DEPARTMENT OF DEFENSE
Office of the Secretary
32 CFR Part 170
[Docket ID: DoD-2023-OS-0063]
RIN 0790-AL49

Cybersecurity Maturity Model Certification (CMMC) Program

AGENCY: Office of the Department of Defense Chief Information Officer (CIO), Department of Defense (DoD).

ACTION: Final rule.

SUMMARY: With this final rule, DoD establishes the Cybersecurity Maturity Model Certification (CMMC) Program in order to verify contractors have implemented required security measures necessary to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The mechanisms discussed in this rule will allow the Department to confirm a defense contractor or subcontractor has implemented the security requirements for a specified CMMC level and is maintaining that status (meaning level and assessment type) across the contract period of performance. This rule will be updated as needed, using the appropriate rulemaking process, to address evolving cybersecurity standards, requirements, threats, and other relevant changes.

DATES: This rule is effective on [INSERT 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. The incorporation by reference of certain material listed in this rule is approved by the Director of the Federal Register as of [INSERT 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

FOR FURTHER INFORMATION CONTACT: Ms. Diane Knight, Office of the DoD CIO at osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil or 202–770–9100.

SUPPLEMENTARY INFORMATION:

History of the Program

The beginnings of CMMC start with the November 2010, Executive Order (E.O.) 13556,[1] *Controlled Unclassified Information*. The intent of this Order was to "establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls." Prior to this E.O., more than 100 different markings for this information existed across the executive branch. This ad hoc, agency-specific approach created inefficiency and confusion, led to a patchwork system that failed to adequately safeguard information requiring protection, and unnecessarily restricted information-sharing.

As a result, the E.O. established the CUI Program to standardize the way the executive branch handles information requiring safeguarding or dissemination controls (excluding information that is classified under E.O. 13526, Classified National Security Information[2] or any predecessor or successor order; or the Atomic Energy Act of 1954[3], as amended).

In 2019, DoD announced the development of CMMC in order to move away from a "self-attestation" model of security. It was first conceived by the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) to secure the Defense Industrial Base (DIB) sector against evolving cybersecurity threats. In September 2020, DoD published the 48 CFR CMMC interim final rule, *Defense Federal Acquisition Regulation Supplement (DFARS): Assessing Contractor Implementation of Cybersecurity Requirements* (DFARS Case 2019-D041 85 FR 48513, September 9, 2020)[4], which implemented the DoD's vision for the initial CMMC Program and outlined the basic features of the framework (tiered model of practices and processes, required assessments, and implementation through contracts) to protect FCI and CUI. The 48 CFR CMMC interim final rule became effective on 30 November 2020,

---

[1] www.federalregister.gov/citation/75-FR-68675 (November 4, 2010)
[2] www.federalregister.gov/citation/75-FR-707 (December 29, 2009)
[3] www.govinfo.gov/link/uscode/42/2011, et seq
[4] www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplementassessing-contractor-implementation-of

establishing a five-year phase-in period. In response to approximately 750 public comments on the 48 CFR CMMC interim final rule, in March 2021, the Department initiated an internal review of CMMC's implementation.

In November 2021, the Department announced the revised CMMC Program, an updated program structure and requirements designed to achieve the primary goals of the internal review:

- Safeguard sensitive information to enable and protect the warfighter
- Enforce DIB cybersecurity standards to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Perpetuate a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

The revised CMMC Program has three key features:

- **Tiered Model**: CMMC requires companies entrusted with Federal contract information and controlled unclassified information to implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also describes the process for requiring protection of information flowed down to subcontractors.
- **Assessment Requirement:** CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.
- **Phased Implementation:** Once CMMC rules become effective, certain DoD contractors handling FCI and CUI will be required to achieve a particular CMMC level as a condition of contract award. CMMC requirements will be implemented using a 4-phase implementation plan over a three-year period.

Current Status of the CMMC Program

Separate from this rulemaking, DoD has a proposed acquisition rule (48 CFR part 204 CMMC Acquisition rule) to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to address procurement related considerations and requirements related to this program rule (32 CFR part 170 CMMC Program rule). The 48 CFR part 204 CMMC Acquisition rule also partially implements a section of the National Defense Authorization Act for Fiscal Year 2020 directing the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. defense industrial base.[5] The 48 CFR part 204 CMMC Acquisition rule, when finalized, will allow DoD to require a specific CMMC level in a solicitation or contract. When CMMC requirements are applied to a solicitation, Contracting officers will not make award, exercise an option, or extend the period of performance on a contract, if the offeror or contractor does not have the passing results of a current certification assessment or self-assessment for the required CMMC level, and an affirmation of continuous compliance with the security requirements in the Supplier Performance Risk System (SPRS)[6] for all information systems that process, store, or transmit FCI or CUI during contract performance. Furthermore, the appropriate CMMC certification requirements will flow down to subcontractors at all tiers when the subcontractor processes, stores, or transmits FCI or CUI. It should be noted the Department may include CMMC requirements on contracts awarded prior to 48 CFR part 204 CMMC Acquisition rule becoming effective, but doing so will require bilateral contract modification after negotiations.

To date, the DoD has relied on offeror representation that the security requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*" have been met, as described by 48 CFR 252.204-7008. In some instances, the DoD has verified contractor implementation of NIST SP 800-171 through assessment by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). As part of this responsibility, DCMA DIBCAC assesses DIB companies to ensure they are meeting contractually required cybersecurity standards and to ensure contractors have

[5] www.federalregister.gov/documents/2024/08/15/2024-18110/defense-federal-acquisition-regulation-supplementassessing-contractor-implementation-of

[6] www.sprs.csd.disa.mil/ under OMB control number 0750-0004

the ability to protect CUI for government contracts they are awarded. DCMA DIBCAC conducts NIST SP 800-171 assessments in support of 48 CFR 252.204-7012 (DFARS clause 252.204-7012), *Safeguarding Covered Defense Information and Cyber Incident Reporting*[7], and 48 CFR 252.204-7020 (DFARS clause 252.204-7020), *NIST SP 800-171 DoD Assessment Requirements*[8]. The DCMA DIBCAC prioritization process is designed to adjust as DoD's cyber priorities evolve based on ongoing threats. DCMA DIBCAC collects and analyzes data on DoD contractors to include:

- Mission critical programs, technologies, and infrastructure and the contractors (prime or lower tier) that support DoD capabilities.
- Cyber threats, vulnerabilities, or incidents.
- DoD Leadership requests.

To date, DCMA DIBCAC has assessed 357 entities including DoD's major prime contractors. In accordance with NIST SP 800-171, titled "*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*," Revision 2, February 2020 (includes updates as of January 28, 2021) (NIST SP 800-171 R2), contractors must describe in a System Security Plan (SSP)[9] how the security requirements are met or how the organizations plan to meet the requirements and address known and anticipated threats. In the event companies cannot establish full compliance, they must develop plans of action that describe how unimplemented security requirements will be met and how any planned mitigations will be implemented. Although an explicit time limit for mitigation is not specified in NIST SP 800-171 R2, contractors that fail to reasonably comply with applicable requirements may be subject to standard contractual remedies. The CMMC Program's assessment phase-in plan, as described in § 170.3, does not preclude entities from immediately seeking a CMMC certification assessment prior to the 48 CFR part 204 CMMC Acquisition rule being finalized and the clause being added to new or existing DoD contracts.

The Department estimates 8350 medium and large entities will be required to meet CMMC Level 2 C3PAO assessment requirements as a condition of contract award. CMMC Level 2 requirements will apply to all contractors that process, store, or transmit CUI, and will provide DoD with a means to assess that CUI safeguarding requirements prescribed in 32 CFR part 2002 have been met. DoD estimates 135 CMMC Third-Party Assessment Organization (C3PAO)-led certification assessments will be completed in the first year, 673 C3PAO certification assessments in year 2, 2,252 C3PAO certification assessments in year 3, and 4,452 C3PAO certification assessments in year four.

Any DoD component can request DCMA DIBCAC to initiate an assessment and these requests will take priority in the assessment scheduling process. Once identified for assessment, DCMA DIBCAC determines the assessment date and notifies the company to begin the preassessment process. Typically, planning and scheduling takes place 3 to 6 months in advance of a DCMA DIBCAC assessment to allow DCMA DIBCAC and the DIB company time to prepare, however, DoD's identified priorities may expedite the execution of an assessment. As discussed in more detail in the regulatory text, assessment results are reported to DoD, including key stakeholders via SPRS and made available to the DIB company. Please see the DCMA DIBCAC website at www.dcma.mil/DIBCAC/ that includes links to the pre-assessment documents; a publicly releasable version of the assessment database; FAQs; an informational video; a link to Procurement Integrated Enterprise Environment (PIEE), the primary enterprise procure-to-pay application for the DoD; a link to SPRS where assessment scores are posted; and links to other reference materials.

---

[7] www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting

[8] www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements

[9] Required since November 2016, NIST SP 800-171 R2 security requirement 3.12.4 states organizations must "develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems."

As discussed in more detail later in the regulatory text, all requirements that are scored as NOT MET are identified in a Plan of Action and Milestones (POA&M) to meet the CMMC requirement. Organizations Seeking Assessment (OSAs) satisfy the CMMC requirements needed for contract award by successfully meeting all 110 security requirements of NIST SP 800-171 R2 or by receiving a Conditional CMMC Status when achieving the minimum passing score of 80 percent and only including permittable NOT MET requirements as described in § 170.21 on the POA&M. All requirements that were scored "NOT MET" and placed on the POA&M must be remedied within 180 days of receiving their Conditional CMMC Status. Proper implementation of these requirements must be verified by a second assessment, called a POA&M closeout assessment. If the POA&M closeout assessment finds that all requirements have been met, then the OSA will achieve a CMMC Status of Final Level 2 (Self) or Final Level 2 (C3PAO) as applicable. However, if the POA&M closeout assessment does not validate all requirements have been met by the end of the 180 days, then the CMMC Status of Conditional Level 2 (Self) or Conditional Level 2 (C3PAO) will expire and at this point, standard contractual remedies will apply for any current contract.

DoD has created a series of guidance documents to assist organizations in better understanding the CMMC Program and the assessment process and scope for each CMMC level. These guidance documents are available on the DoD CMMC website at https://dodcio.defense.gov/CMMC/Documentation/ and on the DoD Open Government website at https://open.defense.gov/Regulatory-Program/Guidance-Documents/. The CMMC Program has also been incorporated in the Department's 2024 Defense Industrial Base Cybersecurity Strategy.[10] The strategy requires the Department to coordinate and collaborate across components to identify and close gaps in protecting DoD networks, supply chains, and other critical resources. Other prongs of the Department's cybersecurity strategy are described in the Department's National Industrial Security Program Operating Manual (NISPOM) which address implementation of the Security Executive Agent Directive (SEAD) 3[11][11][12] procedures for the protection and reproduction of classified information; controlled unclassified information (CUI); National Interest Determination (NID) requirements for cleared contractors operating under a Special Security Agreement for Foreign Ownership, Control, or Influence; and eligibility determinations for personnel security clearance processes and requirements[13].

Overview of Revised CMMC Program

Current Requirements for Defense Contractors and Subcontractors

Currently, Federal contracts (including defense contracts) involving the transfer of FCI to a non-Government organization follow the requirements specified in 48 CFR 52.204-21 (Federal Acquisition Regulation (FAR) clause 52.204-21), *Basic Safeguarding of Covered Contractor Information Systems*[14]. FAR clause 52.204-21 requires compliance with 15 security requirements, FAR clause 52.204-21 (b)(1), items (i) through (xv). These requirements are the minimum necessary for any entity wishing to receive FCI from the US Government (USG).

Defense contracts involving the development or transfer of CUI to a non-Government organization require applicable requirements of DFARS clause 252.204-7012[15]. This clause requires defense contractors to provide adequate security on all covered contractor information systems by implementing the 110 security requirements specified in NIST SP 800-171. This clause includes additional requirements; for example, defense contractors must confirm that any Cloud Service Providers (CSPs) used by the contractor to handle CUI meet Federal Risk and Authorization Management Program (FedRAMP) Moderate Baseline or the equivalent requirements. It also requires defense contractors to flow down all the requirements to their

---

[10] https://media.defense.gov/2024/Mar/28/2003424523/-1/-

[11] /1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF

[12] www.govinfo.gov/content/pkg/FR-2020-12-21/pdf/2020-27698.pdf)

[13] www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/32-CFR-Part-117-NISPOM-Rule/

[14] www.acquisition.gov/far/52.204-21

[15] www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incidentreporting

subcontractors who process, store, or transmit CUI. The CMMC Program currently does not include any requirements for contractors operating systems on behalf of the DoD.

To comply with DFARS clause 252.204-7012, contractors are required to develop a SSP[16] detailing the policies and procedures their organization has in place to comply with NIST SP 800-171. The SSP serves as a foundational document for the required NIST SP 800-171 selfassessment. To comply with 48 CFR 252.204-7019 (DFARS provision 252.204-7019) and DFARS clause 252.204-7020, self-assessment scores must be submitted[17]. The highest score is 110, meaning all 110 NIST SP 800-171 security requirements have been fully implemented. If a contractor's Supplier Performance Risk System (SPRS) score is less than 110, indicating security gaps exist, then the contractor must create a plan of action[18] identifying security tasks that still need to be accomplished. In essence, an SSP describes the cybersecurity plan the contractor has in place to protect CUI. The SSP needs to address each NIST SP 800-171 security requirement and explain how the requirement is implemented. This can be through policy, technology, or a combination of both.

In November 2020, the DoD released its 48 CFR CMMC interim final rule, the *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements*[19] (DFARS Case 2019-D041, 85 FR 61505, November 30, 2020). The goal of this rule was to increase compliance with its cybersecurity regulations and improve security throughout the DIB. This rule introduced one new provision and two new clauses – DFARS provision 252.204-7019, DFARS clause 252.204-7020, and 48 CFR 252.204-7021 (DFARS clause 252.204-7021).

- DFARS provision 252.204-7019 complements DFARS clause 252.204-7012 by requiring contractors to have a NIST SP 800-171 assessment (basic, medium, or high) according to NIST SP 800-171 DoD Assessment Methodology[20]. Assessment scores must be reported to the Department via SPRS. SPRS scores must be submitted by the time of contract award and not be more than three years old.
- DFARS clause 252.204-7020 notifies contractors that DoD reserves the right to conduct a higher-level assessment of contractors' cybersecurity compliance, and contractors must give DoD assessors full access to their facilities, systems, and personnel. Further, DFARS clause 252.204-7020 complements DFARS clause 252.204-7012's flow down requirements by holding contractors responsible for confirming their subcontractors have SPRS scores on file prior to awarding them contracts.
- DFARS clause 252.204-7021 paves the way for rollout of the CMMC Program. Once CMMC is implemented, the required CMMC Level and assessment type will be specified in the solicitation and resulting contract. Contractors handling FCI or CUI will be required to meet the CMMC requirement specified in the contract. DFARS clause 252.204-7021 also stipulates contractors will be responsible for flowing down the CMMC requirements to their subcontractors.

CFR part 170 **Additional Requirements for Defense Contractors and Subcontractors Discussed in This Final Rule**

When this 32 CFR part 170 CMMC Program rule and the complementary 48 CFR part 204 CMMC Acquisition rule are finalized and following a phased implementation plan,

---

[16] Required since November 2016, NIST SP 800-171 R2 security requirement 3.12.4 states organizations must "develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems."

[17] www.sprs.csd.disa.mil/ under OMB control number 0750-0004

[18] The plan of action requirement described under DFARS clause 252.204-7020 is different from a Plan of Action and Milestones (POA&M) requirement in CMMC as plans of action do not require milestones.

[19] www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplementassessing-contractor-implementation-of

[20] www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version1.2.1-6.24.2020.pdf

solicitations and resulting defense contracts involving the processing, storing, or transmitting of FCI or CUI on a non-Federal system will, unless waived, have a CMMC level and assessment type requirement that a contractor must meet to be eligible for a contract award. The four phases of the implementation plan add CMMC level requirements incrementally, starting in Phase 1 with self-assessments, and ending in Phase 4, which represents full implementation of program requirements. The DoD elected to base the phase-in plan on the level and type of assessment to provide time to train the necessary number of assessors, and to allow companies time to understand and implement CMMC requirements. Details of each phase are addressed in § 170.3(e). In Phases 2 and 3, DoD will implement CMMC Level 2 and Level 3 certification requirements, respectively. At full implementation (Phase 4), DoD will include CMMC requirements in all applicable DoD contracts and option periods on contracts awarded after the beginning of Phase 4.

Table 1 defines the requirements for each CMMC level and assessment type.

Table 1—CMMC Level and Assessment Requirements

CMMC Status	Source & Number of Security Reqts.	Assessment Reqts.	Plan of Action & Milestones (POA&M) Reqts.	Affirmation Reqts.
Level 1 (Self)	• 15 required by FAR clause 52.204-21	• Conducted by Organization Seeking Assessment (OSA) annually • Results entered into SPRS (or its successor capability)	• Not permitted	• After each assessment • Entered into SPRS

Level 2 (Self)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by OSA every 3 years • Results entered into SPRS (or its successor capability) • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS (or its successor capability)
Level 2 (C3PAO)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by C3PAO every 3 years • Results entered into CMMC Enterprise Mission Assurance Support Service	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days	• After each assessment and annually thereafter • Assessment will lapse

		(eMASS) (or its successor capability) • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	upon failure to annually affirm • Entered into SPRS (or its successor capability)
Level 3 (DIBCAC)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 • 24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to § 170.14(c)(4)	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment • Conducted by Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every 3 years • Results entered into CMMC eMASS (or its successor capability)	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Level 2 (C3PAO) affirmation must also continue to be completed annually • Entered into SPRS (or its

		• CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4		successor capability)

Program Walkthrough – Contractor Perspective

This section will provide a simplified walkthrough of the CMMC Program from the perspective of an Organization Seeking Assessment (OSA) seeking to comply with program requirements.

CMMC Level Selection

An OSA will select the CMMC level it desires to attain. Once the CMMC Program is implemented, a DoD solicitation will specify the minimum CMMC Status required to be eligible for award. One of four CMMC Statuses will be specified:

- Level 1 (Self) is a self-assessment to secure FCI processed, stored, or transmitted in the course of fulfilling the contract. The OSA must comply with the 15 security requirements set by FAR clause 52.204-21. All 15 requirements must be met in full—no exceptions are allowed.
- Level 2 (Self) is a self-assessment to secure CUI processed, stored, or transmitted in the course of fulfilling the contract. The OSA must comply with the 110 Level 2 security requirements derived from NIST SP 800-171 R2.
- Level 2 (C3PAO) differs from Level 2 (Self) in the method of verifying compliance. OSAs must hire a C3PAO to conduct an assessment of the OSA's compliance with the 110 security requirements of NIST SP 800-171 R2. OSAs can shop for C3PAOs on the CMMC Accreditation Body (AB) Marketplace.
- Level 3 (DIBCAC) is a government assessment of 24 additional requirements derived from NIST SP 800-172, titled "*Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*," February 2021 (NIST SP 800-172 Feb2021). The OSA must ensure that they have already achieved a CMMC Status of Final Level 2 (C3PAO) before seeking CMMC Status of Final Level 3 (DIBCAC). Once this is done, an OSA should then initiate a Level 3 certification assessment by emailing a request to Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) point of contact found at www.dcma.mil/DIBCAC, being sure to include the Level 2 (C3PAO) certification unique identifier in the email. **Scoping**

In order to achieve a specified CMMC Status, OSAs must first identify which information systems, including systems or services provided by External Service Providers (ESPs), will process, store, or transmit FCI, for Level 1 (Self), and CUI for all other CMMC Statuses. These information systems constitute the scope of the assessment.

Within these information systems, for Level 2 and Level 3 the assets should be further broken down into asset categories: Contractor Risk Managed Assets (Level 2), Security Protection Assets (Level 2 and 3), and Specialized Assets (Level 2 and 3). For Level 1 all assets, with the exclusion of Specialized Assets, are simply identified as either in-scope or out-of-scope based on whether they process, store, or transmit FCI. Definitions and treatment of these categories as they relate to assessment scoping, treatment of ESPs, and treatment of assets which cannot be secured due to their inherent design, can be found at § 170.19.

Assessment and Affirmation

a. OSAs that meet all 15 Level 1 requirements have achieved CMMC Status of Final Level 1 (Self). The OSA must submit an affirmation of compliance with FAR clause 52.204-21 requirements in SPRS. At this point, OSAs have satisfied the CMMC requirements needed for award of contracts requiring a CMMC Status of Final Level 1 (Self). To maintain a CMMC

Status of Final Level 1 (Self), this entire process must be repeated in full on an annual basis, including both self-assessment and affirmation.

b. For Level 2 assessments, if all 110 requirements are satisfied, the assessment score will be 110 and the OSA will have achieved a CMMC Status of Final Level 2 (Self) or Final Level 2 (C3PAO) as applicable and is eligible for contract award as long as all other contractual requirements are met.

Not all requirements must immediately be MET to be eligible for contract award. If the minimum score is achieved on the assessment (equal to 80% of the maximum score) and certain critical requirements are met, OSAs will achieve a CMMC Status of Conditional Level 2 (Self) or Conditional Level 2 (C3PAO) as applicable. All NOT MET requirements must be noted in an assessment Plan of Action and Milestones (POA&M). At this point the OSA will have satisfied the CMMC requirements needed for contract award OSAs must have met all 110 security requirements of NIST SP 800-171 R2 within 180 days of receiving their Conditional CMMC Status, which must be verified with a second assessment, called a POA&M closeout assessment. If the POA&M closeout assessment finds that all requirements have been met, then the OSA will achieve a CMMC Status of Final Level 2 (Self) or Final Level 2 (C3PAO) as applicable. However, if a POA&M closeout assessment does not find that all requirements have been met by the end of 180 days, then the CMMC Status of Conditional Level 2 (Self) or Conditional Level 2 (C3PAO) will expire. At this point, standard contractual remedies will apply.

The OSA should submit an affirmation into SPRS after achieving a CMMC Status of Conditional Level 2 (Self) or CMMC Status of Conditional Level 2 (C3PAO) as applicable. OSAs should submit an affirmation once a CMMC Status of Final Level 2 (Self) or Final Level 2 (C3PAO) as applicable is achieved. Being eligible for contracts subject to CMMC Level 2 (Self) also indicates eligibility for contracts subject to Level 1 (Self), and being eligible for contracts subject to CMMC Level 2 (C3PAO) also indicates eligibility for contracts subject to Level 1 (Self) and Level 2 (Self), assuming all other contractual requirements are met. OSAs must reaffirm in SPRS their compliance with CMMC Level 2 requirements annually but need only conduct a new assessment every three years. These deadlines are based on the CMMC Status Date of the Conditional Status if a POA&M was required or the Final Status if the assessment resulted in a score of 110. CMMC Status date is not based on the date of a POA&M closeout assessment.

c. For Level 3 assessments, OSAs should note that asset categories are assessed against security requirements differently than they are at Level 2. In particular, Contractor Risk Managed Assets identified in a Level 2 scope are treated as CUI Assets if they reside within a Level 3 scope. Definitions and treatment of these assets at Level 3 as they relate to scoping of the assessment, in addition to treatment of ESPs, are described in § 170.19(d).

During the course of assessment, DCMA DIBCAC will focus on assessing compliance with all 24 selected requirements derived from NIST SP 800-172 Feb2021, but limited checks may be performed on the 110 requirements from NIST SP 800-171 R2. If DCMA DIBCAC identifies that all 24 requirements from NIST SP 800-172 Feb2021 are satisfied, the OSA will have achieved a CMMC Status of Final Level 3 (DIBCAC) and is eligible for contract award as long as all other contractual requirements are met. Not all requirements must immediately be MET to be eligible for contract award. If the minimum score is achieved on the assessment (equal to 80% of the maximum score of 24) and certain critical requirements are met, OSAs will achieve a CMMC Status of Conditional Level 3 (DIBCAC), and all NOT MET requirements must be noted in a POA&M. At this point the OSA will have satisfied the CMMC requirements needed for contract award.

OSAs must have met all 24 selected security requirements of NIST SP 800-172 Feb2021 within 180 days of receiving their Conditional CMMC Status, which must be verified with a POA&M closeout assessment by DCMA DIBCAC. If the POA&M closeout assessment finds that all requirements have been met, then the OSA will achieve a CMMC Status of Final Level 3 (DIBCAC). However, if a POA&M closeout assessment does not find that all requirements have

been met by the end of 180 days, then the CMMC Status of Conditional Level 3 (DIBCAC) will expire. At this point, standard contractual remedies will apply.

The OSA should submit an affirmation into SPRS after achieving a CMMC Status of Conditional Level 3 (DIBCAC) if applicable and once a CMMC Status of Final Level 3 (DIBCAC) is achieved. Being eligible for contracts subject to CMMC Level 3 (DIBCAC) also indicates eligibility for contracts subject to Level 1 (Self), Level 2 (Self), and Level 2 (C3PAO), assuming all other contractual requirements are met. To maintain CMMC Level 3 (DIBCAC) status, an OSA must undergo both a Level 2 certification assessment *and* a Level 3 certification assessment every three years and separately affirm compliance with Level 2 and Level 3 requirements in SPRS annually. These deadlines are based on the CMMC Status Date of the Conditional certification if applicable or the CMMC Status Date of the Final determination. CMMC Status Date is not based on the date of a POA&M closeout assessment.

Flow-down

If the OSA employs subcontractors to fulfill the contract, those subcontractors must also have a minimum CMMC Status as shown in table 2.

Table 2 – Minimum Flow-down Requirements

Table 2—Minimum Flowdown Requirements Prime Contractor Requirement	Minimum Subcontractor Requirement If the subcontractor will process, store, or transmit	
	FCI	CUI
Level 1 (Self)	Level 1(Self)	N/A
Level 2 (Self)	Level 1(Self)	Level 2 (Self)
Level 2 (C3PAO)	Level 1(Self)	Level 2(C3PAO)
Level 3 (DIBCAC)	Level 1(Self)	Level 2(C3PAO)

Summary of Provisions Contained in This Rule

Section 170.1 Purpose

Section 170.1 addresses the purpose of this rule. It describes the CMMC Program and establishes policy for requiring the protection of FCI and CUI that is processed, stored, or transmitted on defense contractor and subcontractor information systems. The security standards utilized in the CMMC Program are from the FAR clause 52.204-21; DFARS clause 252.2047012 that implements NIST SP 800-171 R2; and selected requirements from the NIST SP 800-172 Feb2021, as applicable. The purpose of the CMMC Program is for contractors and subcontractors to demonstrate that FCI and CUI being processed, stored, or transmitted is adequately safeguarded through the methodology provided in the rule.

Section 170.2 Incorporation by Reference

Section 170.2 addresses the standards and guidelines that are incorporated by reference. The Director of the Federal Register under 5 U.S.C. § 552(a) and 1 CFR part 51 approves any materials that are incorporated by reference. Materials that are incorporated by reference in this rule are reasonably available. Information on how to access the documents is detailed in § 170.2. Materials that are incorporated by reference in this rule are from the NIST (see § 170.2(a)), the Committee on National Security Systems (see § 170.2(b)), and the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) (see § 170.2(c)) which may require payment of a fee.

Note: While the ISO/IEC standards are issued jointly, they are available from the ISO Secretariat (see § 170.2(c)).

The American National Standards Institute (ANSI) IBR Portal provides access to standards that have been incorporated by reference in the U.S. Code of Federal Regulations at https://ibr.ansi.org. These standards incorporated by the U.S. government in rulemakings are offered at no cost in "read only" format and are presented for online reading. There are no print or download options. All users will be required to install the FileOpen plug-in and accept an online end user license agreement prior to accessing any standards.

The materials that are incorporated by reference are summarized below.

(a)Federal Information Processing Standard (FIPS) Publication (PUB) 200 (FIPS PUB 200), titled “Minimum Security Requirements for Federal Information and Information Systems,” is the second of two security standards mandated by the Federal Information Security Management Act (FISMA). It specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum-security requirements. This standard promotes the development, implementation, and operation of more secure information systems within the Federal Government by establishing minimum levels of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements. This document is incorporated by reference as a source for definitions.

(b) FIPS PUB 201-3, titled “Personal Identity Verification (PIV) of Federal Employees and Contractors,” establishes a standard for a PIV system that meets the control and security objectives of Homeland Security Presidential Directive-12. It is based on secure and reliable forms of identity credentials issued by the Federal Government to its employees and contractors. These credentials are used by mechanisms that authenticate individuals who require access to federally controlled facilities, information systems, and applications. This Standard addresses requirements for initial identity proofing, infrastructure to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials. This document is incorporated by reference as a source for definitions.

(c)NIST SP 800-37, titled “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” Revision 2 (NIST SP 800-37 R2), describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels. The RMF also promotes near real-time risk management and ongoing information system and common control authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make efficient, cost-effective, risk management decisions about the systems supporting their missions and business functions; and incorporates security and privacy into the system development life cycle. Executing the RMF tasks links essential risk management processes at the system level to risk management processes at the organization level. In addition, it establishes responsibility and accountability for the controls implemented within an organization’s information systems and inherited by those systems. This document is incorporated by reference as a source for definitions.

(d) NIST SP 800-39, titled “Managing Information Security Risk: Organization, Mission, and Information System View,” March 2011 (NIST SP 800-39 Mar2011), provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of Federal information systems. NIST SP 800-39 Mar2011 provides a structured, yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines. The guidance provided in this publication is not intended to replace or subsume other risk-related activities, programs, processes, or approaches that organizations have implemented or intend to implement addressing areas of risk management covered by other legislation, directives, policies, programmatic initiatives, or mission/business requirements. Rather, the risk management guidance described herein is complementary to and should be used as part of a more comprehensive Enterprise Risk Management (ERM) program. This document is incorporated by reference as a source for definitions.

(e)NIST SP 800-53, titled “Security and Privacy Controls for Information Systems and Organizations,” Revision 5 (NIST SP 800-53 R5), provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalog addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy. This document is incorporated by reference as a source for definitions.

(f) NIST SP 800-82r3, titled “Guide to Operational Technology (OT) Security,” September 2023 (NIST SP 800-82r3), provides guidance on how to secure ICS, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. This document is incorporated by reference as a source for definitions.

(g) NIST SP 800-115, titled “Technical Guide to Information Security Testing and Assessment,” September 2008 (NIST SP 800-115 Sept2008), assists organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies. The guide provides practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures. These can be used for several purposes, such as finding vulnerabilities in a system or network and verifying compliance with a policy or other requirements. The guide is not intended to present a comprehensive information security testing and examination program but rather an overview of key elements of technical security testing and examination, with an emphasis on specific technical techniques, the benefits and limitations of each, and recommendations for their use. This document is incorporated by reference as a source for definitions.

(h) NIST SP 800-160, Volume 2, titled “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,” Revision 1, December 2021 (NIST SP 800-160 V2R1), focuses on cyber resiliency engineering—an emerging specialty systems engineering discipline applied in conjunction with systems security engineering and resilience engineering to develop survivable, trustworthy secure systems. Cyber resiliency engineering intends to architect, design, develop, implement, maintain, and sustain the trustworthiness of systems with the capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources. From a risk management perspective, cyber resiliency is intended to help reduce the mission, business, organizational, enterprise, or sector risk of depending on cyber resources. This document is incorporated by reference as a source for definitions.

(i) NIST SP 800-171, titled “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” Revision 2, February 2020 (includes updates as of January 28, 2021) (NIST SP 800-171 R2), provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a Federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI

prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by Federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This document is incorporated by reference as a foundational source for definitions and security requirements.

(j) NIST SP 800-171A, titled "Assessing Security Requirements for Controlled Unclassified Information," June 2018 (NIST SP 800-171A Jun2018), provides Federal and non-Federal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST SP 800-171 R2. The assessment procedures are flexible and can be customized to the needs of the organizations and the assessors conducting the assessments. Security assessments can be conducted as self-assessments; independent, third-party assessments; or government-sponsored assessments and can be applied with various degrees of rigor, based on customer-defined depth and coverage attributes. The findings and evidence produced during the security assessments can facilitate risk-based decisions by organizations related to the CUI requirements. This document is incorporated by reference as a foundational source for definitions and assessment.

(k) NIST SP 800-172, titled "Enhanced Security Requirements for Protecting Controlled
Unclassified Information: A Supplement to NIST Special Publication 800-171," February 2021 (NIST SP 800-172 Feb2021), provides Federal agencies with recommended enhanced security requirements for protecting the confidentiality of CUI: (1) when the information is resident in nonfederal systems and organizations; (2) when the nonfederal organization is not collecting or maintaining information on behalf of a Federal agency or using or operating a system on behalf of an agency; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI Registry. The enhanced requirements apply only to components of nonfederal systems that process, store, or transmit CUI or that provide security protection for such components when the designated CUI is associated with a critical program or high value asset. The enhanced requirements supplement the basic and derived security requirements in NIST SP 800-171 R2 and are intended for use by Federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This document is incorporated by reference as a foundational source for security requirements.

(l) NIST SP 800-172A, titled "Assessing Enhanced Security Requirements for Controlled Unclassified Information," March 2022 (NIST SP 800-172A Mar2022), provides Federal agencies and nonfederal organizations with assessment procedures that can be used to carry out assessments of the requirements in NIST SP 800-172 Feb2021. The assessment procedures are flexible and can be tailored to the needs of organizations and assessors. Assessments can be conducted as (1) self-assessments; (2) independent, third-party assessments; or (3) governmentsponsored assessments. The assessments can be conducted with varying degrees of rigor based on customer-defined depth and coverage attributes. The findings and evidence produced during the assessments can be used to facilitate risk-based decisions by organizations related to the CUI enhanced security requirements. This document is incorporated by reference as a foundational source for definitions and assessment.

(m) ISO/IEC 17011:2017(E), titled "Conformity assessment – Requirements for accreditation bodies accrediting conformity assessment bodies," Second edition, November 2017 (ISO/IEC 17011:2017(E)), specifies requirements for the competence, consistent operation and impartiality of accreditation bodies assessing and accrediting conformity assessment bodies. This document is incorporated by reference as a source for requirements on the CMMC Ecosystem.

(n) ISO/IEC 17020:2012(E), titled "Conformity assessment – Requirement for the operation of various types of bodies performing inspection," Second edition, March 1, 2012

(ISO/IEC 17020:2012(E)), specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities. It applies to inspection bodies of type A, B or C, as defined in ISO/IEC 17020:2012(E), and it applies to any stage of inspection." This document is incorporated by reference as a source for requirements on the
CMMC Ecosystem.

(o) ISO/IEC 17024:2012(E), titled "Conformity assessment – General requirements for bodies operating certification of persons," Second edition, July 1, 2012 (ISO/IEC 17024:2012(E)), contains principles and requirements for a body certifying persons against specific requirements and includes the development and maintenance of a certification scheme for persons." This document is incorporated by reference as a source for requirements on the CMMC Ecosystem.

Section 170.3 Applicability

Section 170.3 identifies entities to which the rule applies and how the Department intends to implement the rule. The rule applies to defense contractors and subcontractors that will process, store, or transmit FCI or CUI in performance of a DoD contract, and private-sector businesses or other entities that are specified in Subpart C. This rule does not apply to Federal information systems operated by contractors and subcontractors in support of the Government. CMMC Program requirements apply to DoD solicitations and contracts requiring defense contractors and subcontractors to process, store, or transmit FCI or CUI. Exceptions to the applicability of this rule are addressed in § 170.3(c)(1) and (2). Department Program Managers or requiring activities will determine which CMMC Level and assessment type will apply to a contract or procurement. Applicability of the required CMMC Level and assessment type to subcontractors is addressed in § 170.23.

Section 170.3 addresses the four-phased implementation plan of the CMMC Program requirements in solicitations and contracts. Phase 1 begins on the effective date of this CMMC 32 CFR part 170 CMMC Program rule or the complementary 48 CFR part 204 CMMC Acquisition rule, whichever occurs later. More information regarding Phase 1 can be found in § 170.3(e)(1). Phase 2 begins one calendar year after the start date of Phase 1. More information regarding Phase 2 can be found in § 170.3(e)(2). Phase 3 begins one calendar year after the start date of Phase 2. More information regarding Phase 3 can be found in § 170.3(e)(3). Phase 4, or full implementation, begins one calendar year after the start date of Phase 3. More information regarding Phase 4 can be found in § 170.3(e)(4).

Section 170.4 Acronyms and Definitions

Section 170.4 includes acronyms and definitions used in the rule text and can be used as a reference while reading the text and tables. CMMC introduces new terms and associated definitions, and customizes definitions for existing terms, as applied to the CMMC Program. CMMC-custom terms and definitions are clearly marked to distinguish from terms sourced externally. CMMC also utilizes terms created by other authoritative sources, including NIST. Terms from other authoritative sources are also listed in § 170.4 and are properly sourced.

The Department developed the following CMMC-custom terms to enhance understanding of the requirements and elements of the CMMC Program:

- Accreditation
- Accreditation Body
- Affirming Official
- Assessment
- Level 1 self-assessment
- Level 2 self-assessment
- Level 2 certification assessment
- Level 3 certification assessment
- POA&M closeout self-assessment
- POA&M closeout certification assessment
- Assessment Findings Report

- Assessment Team
- Asset Categories
- Authorized
- Cloud Service Provider
- CMMC Assessment and Certification Ecosystem
- CMMC Assessment Scope
- CMMC Assessor and Instructor Certification Organization (CAICO)
- CMMC instantiation of eMASS
- CMMC Status
- Final Level 1 (Self)
- Conditional Level 2 (Self)
- Final Level 2 (Self)
- Conditional Level 2 (C3PAO)
- Final Level 2 (C3PAO)
- Conditional Level 3 (DIBCAC)
- Final Level 3 (DIBCAC)
- CMMC Status Date
- CMMC Third-Party Assessment Organization (C3PAO)
- Contractor Risk Managed Assets
- Controlled Unclassified Information (CUI) Assets
- Enduring Exception
- External Service Provider (ESP)
- Operational plan of action
- Organization-defined
- Organization Seeking Assessment (OSA)
- Organization Seeking Certification (OSC)
- Out-of-Scope Assets
- Periodically
- Process, store, or transmit
- Restricted Information Systems
- Security Protection Assets
- Security Protection Data
- Specialized Assets
- Temporary Deficiency
- Test Equipment.

Section 170.5 Policy

Section 170.5 addresses the policy underlying the rule. The protection of FCI and CUI on defense contractor information systems is crucial to the continuity of the missions and functions of the DoD. To that end, this rule requires that contractors and subcontractors implement the specified security requirements for the applicable CMMC Level. For CMMC Level 3, the selected security requirements are defined in NIST SP 800-172 Feb2021 with the applicable DoD Organization-Defined Parameters (ODPs) defined in table 1 to § 170.14(c)(4).

Program Managers and requiring activities identify the applicable CMMC Level and assessment type. Factors used to determine which CMMC Level and assessment type will be applied are included but not limited to the list found in § 170.5(b)(1-5). CMMC Program requirements will flow down to subcontractors, as applicable (see § 170.23). A DoD Service Acquisition Executive or a Component Acquisition Executive may elect to waive inclusion of CMMC Program requirements in a solicitation or contract.

Section 170.5 addresses that the CMMC Program does not alter the requirements imposed on contractors and subcontractors in FAR clause 52.204-21, DFARS clause 252.204-7012, or any other applicable safeguarding of information requirement. The CMMC Program verifies implementation of security requirements in FAR clause 52.204-21, NIST SP 800-171 R2, and selected security requirements in NIST SP 800-172 Feb2021, as applicable.

Section 170.6 CMMC PMO

Section 170.6 addresses the CMMC Program Management Office (PMO) functions that are performed within the Department of Defense Chief Information Officer (DoD CIO).

Section 170.7 DCMA DIBCAC

Section 170.7 addresses how DCMA DIBCAC will support the CMMC Program by conducting CMMC Level 2 certification assessments of the Accreditation Body and C3PAOs; conducting CMMC Level 3 certification assessments for OSCs; and recording results, issuing certificates, tracking appeals, and retaining records as required.

Section 170.8 Accreditation Body

Section 170.8 addresses the roles and responsibilities of the Accreditation Body, as well as requirements that the Accreditation Body must meet. The Accreditation Body must be US-based and be and remain a member in good standing with the Inter-American Accreditation Cooperation (IAAC) and become an International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA) signatory, with a signatory status scope of ISO/IEC 17020:2012(E) and be compliant with ISO/IEC 17011:2017(E)[21]. There is only one Accreditation Body for the DoD CMMC Program at any given time, and its primary mission is to authorize and accredit the C3PAOs. The Accreditation Body authorizes and accredits C3PAOs in accordance with the requirements in section 170.8(b).

The Accreditation Body also oversees the CAICO to ensure compliance with ISO/IEC 17024:2012(E)[22] and to ensure all training products, instruction, and testing materials are of high quality.

Section 170.8 addresses specific requirements for the Accreditation Body with regards to national security background checks, foreign ownership, reporting, information protection, and appeals. The Accreditation Body will also develop policies for Conflict of Interest (CoI), Code of Professional Conduct (CoPC), and Ethics that comply with all ISO/IEC 17011:2017(E) and DoD requirements. These policies will apply to the Accreditation Body as well as to all other individuals, entities, and groups within the CMMC Ecosystem. The information systems used by the Accreditation Body to process CMMC information have to meet all of the security requirements for CMMC Level 2 and will be assessed by DCMA's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

Section 170.9 CMMC Third-Party Assessment Organizations (C3PAOs)

Section 170.9 addresses the roles, responsibilities, and requirements for C3PAOs, which are the organizations that perform CMMC Level 2 certification assessments for OSCs. The C3PAOs will submit assessment data into the CMMC instantiation of government owned and operated system called eMASS[23], a CMMC instance of the Enterprise Mission Assurance Support Service. C3PAOs issue Certificates of CMMC Status, in accordance with the requirements in § 170.17 of this part.

Section 170.9 addresses detailed requirements for C3PAOs with regards to national security background checks, foreign ownership, reporting, records management, information protection, quality assurance, and appeals. The information systems used by C3PAOs to process Level 2 certification assessment information have to meet all of the security requirements for CMMC Level 2 and will be assessed by DCMA DIBCAC. C3PAOs need to comply with ISO/IEC 17020:2012(E), as well as with the Accreditation Body's policies for CoI, CoPC, and Ethics.

Prior to a C3PAO being compliant with ISO/IEC 17020:2012(E), the C3PAO may be authorized but not accredited. After a C3PAO is compliant with ISO/IEC 17020:2012(E), the C3PAO may be accredited.

Section 170.10 CMMC Assessor and Instructor Certification Organization (CAICO)

Section 170.10 addresses the roles, responsibilities, and requirements for the CAICO, the organization that trains, tests, designates Provisional Instructors (PIs), and certifies CMMC

---

[21] www.iso.org/standard/67198.html

[22] www.iso.org/standard/52993.html

[23] This system is accessible only to authorized users.

Certified Professionals (CCPs), CMMC Certified Assessors (CCAs), CMMC Certified Instructors (CCIs). There is only one CAICO for the DoD CMMC Program at any given time. The CAICO must comply with ISO/IEC 17024:2012(E), as well as with the Accreditation Body's policies for CoI, CoPC, and Ethics. Section 170.10 addresses detailed requirements for the CAICO with regards to certification examinations, quality assurance, appeals, records management, reporting, separation of duties, and information protection.

Section 170.11 CMMC Certified Assessor (CCA)

Section 170.11 addresses the roles and responsibilities of a CMMC Certified Assessor (CCA) who conduct Level 2 certification assessments. In order to be a CCA, a candidate must first be a CCP, must adhere to the requirements set forth in § 170.10, § 170.8(b)(17), and complete a Tier 3 background investigation or equivalent. The required cybersecurity experience for different CCA roles is addressed in § 170.11(b)(6) and (10). Section 170.11 addresses CCA requirements with respect to security breaches; completion of a Tier 3 background investigation or equivalent; reporting; sharing assessment information; and permitted use of C3PAO equipment, devices, and services.

Section 170.12 CMMC Instructor

Section 170.12 addresses the roles and responsibilities of a CMMC Provisional Instructor (PI) and CMMC Certified Instructor (CCI) to teach CMMC assessor candidates. Candidate PIs and CCIs are trained and tested per the requirements set forth in § 170.12(c). Section 170.12(c) also provides candidate PIs and CCIs with the requirements to obtain and maintain designation or certification (as applicable), compliance with Accreditation Body policies, work activity exclusions, confidentiality expectations, non-disclosure clause, non-public training related information, forbidden consulting services, and reporting requirements.

Section 170.13 CMMC Certified Professional (CCP)

Section 170.13 addresses the roles and responsibilities of a CMMC Certified Professional (CCP) required to provide advice, consulting, and recommendations to clients. The CAICO trains and tests candidate CCPs per the requirements set forth in § 170.13(b) with CCP certification issued upon successful completion. A CCP can participate on CMMC Level 2 certification assessments with CCA oversight, however CCAs are responsible for making final assessment determinations for a CMMC Status of Conditional or Final Level 2 (C3PAO). A list of CCP requirements is provided for obtaining and maintaining certification, compliance with Accreditation Body policies, completion of a Tier 3 background investigation or equivalent, sharing assessment specific information, and reporting requirements.

Section 170.14 CMMC Model

Section 170.14 addresses the structure, security requirement contents, organization, sourcing, and numbering of the security requirements that comprise the CMMC Model. It also provides an overview of the assessment process. The CMMC Model consists of three (3) levels, each containing security requirements taken directly from existing regulations and guidelines. Firstly, § 170.14(2) defines CMMC Level 1 as the 15 security requirements listed in the FAR clause 52.204-21(b)(1). Secondly, § 170.14(3) defines CMMC Level 2 as the 110 security requirements from the NIST SP 800-171 R2. Lastly, § 170.14(4) defines CMMC Level 3 as 24 selected security requirements from the NIST SP 800-172 Feb2021.

The CMMC security requirements are organized into domains following the approach taken in NIST SP 800-171 R2. The numbering of the CMMC security requirements, addressed in § 170.14(c)(1), is of the form DD.L#-REQ where the 'DD' is the two-letter domain abbreviation, the 'L#' is the CMMC Level, and the 'REQ' is based directly on the numbering in the source. Assessment criteria for these security requirements, as described in § 170.14(d), is based on security requirement assessment guidance provided in NIST SP 800-171A Jun2018 and NIST SP 800-172A Mar2022.

Section 170.15 CMMC Level 1 Self-Assessment and Affirmation Requirements

Section 170.15 addresses how an OSA will achieve and maintain compliance with the CMMC Status of Level 1 (Self). The OSA must successfully implement the security requirements listed in § 170.14(c)(2) within their Level 1 CMMC Assessment Scope as described

in § 170.19(b). Successful implementation requires meeting all objectives defined in NIST SP 800-171A Jun2018 for the corresponding CMMC Level 1 security requirements as outlined in the mapping table 1 to § 170.15(c)(1)(i).

After implementation, the OSA must perform a Level 1 self-assessment to verify the implementation and score themselves using the scoring methodology provided in § 170.24. All objectives must be met in order for a security requirement to be considered fully implemented; no security requirements may be placed on a POA&M for Level 1. The OSA must then input their results into SPRS as described in § 170.15(a)(1)(i) and submit an affirmation as described in § 170.22.

In order to be eligible for a contract with a requirement for the CMMC Status of Level 1 (Self), the OSA must have achieved a CMMC Status of Final Level 1 (Self) and have submitted an affirmation. These activities must be completed annually.

Section 170.16 CMMC Level 2 Self-Assessment and Affirmation Requirements

Section 170.16 addresses how an OSA will achieve and maintain compliance with the CMMC Status of Level 2 (Self). The OSA must successfully implement the security requirements listed in § 170.14(c)(3) within its Level 2 CMMC Assessment Scope as described in § 170.19(c). Successful implementation requires meeting all objectives defined in NIST SP 800-171A Jun2018 for the corresponding CMMC Level 2 security requirements. Requirements for ESPs and CSPs that process, store, transmit CUI are provided in § 170.16(c)(2) and (3).

After implementation, the OSA must perform a Level 2 self-assessment to verify the implementation and score themselves using the scoring methodology provided in § 170.24. All objectives must be met in order for a security requirement to be considered fully implemented; in some cases, if not all objectives are met, some security requirements may be placed on a POA&M as provided for in § 170.21. If the minimum score has been achieved and some security requirements are in a POA&M, the OSA has achieved the CMMC Status of Conditional Level 2 (Self); if all requirements are MET as defined in § 170.24(b), the OSA has achieved a CMMC Status of Final Level 2 (Self). For Conditional Level 2 (Self), a POA&M closeout must be conducted within 180 days as described in § 170.21(b) or the Conditional Level 2 (Self) CMMC Status will expire.

After a Level 2 self-assessment, as well as after a POA&M closeout, the OSA must input their results into SPRS as described in § 170.16(a)(1)(i) and submit an affirmation as described in § 170.22.

In order to be eligible for a contract with a requirement for the CMMC Status of Level 2 (Self), the OSA must have achieved the CMMC Status of either Conditional Level 2 (Self) or Final Level 2 (Self) and have submitted an affirmation. The Level 2 self-assessment must be completed every three years and the affirmation must be completed annually following the Final CMMC Status Date.

Section 170.17 CMMC Level 2 Certification Assessment and Affirmation Requirements

Section 170.17 addresses how an OSC will achieve and maintain compliance with the CMMC Status of Level 2 (C3PAO). The OSC must successfully implement the security requirements listed in § 170.14(c)(3) within its Level 2 CMMC Assessment Scope as described in § 170.19(c). Successful implementation requires meeting all objectives defined in NIST SP 800-171A Jun2018 for the corresponding CMMC Level 2 security requirements. Requirements for ESPs and CSPs that process, store, transmit CUI are provided in § 170.17(c)(5) and (6).

After implementation, the OSC must hire a C3PAO to perform an assessment to verify the implementation. The C3PAO will score the OSC using the scoring methodology provided in § 170.24. All objectives must be met in order for a security requirement to be considered fully implemented; in some cases, if not all objectives are met, some security requirements may be placed on a POA&M as defined in § 170.21. If the minimum score has been achieved and some security requirements are in a POA&M, the OSC has achieved the CMMC Status of Conditional Level 2 (C3PAO); if all requirements are MET as defined in § 170.24(b), the OSC has achieved the CMMC Status of Final Level 2 (C3PAO). For Conditional Level 2 (C3PAO),

a POA&M closeout must be conducted within 180 days as described in § 170.21(b) or the Conditional Level 2 (C3PAO) CMMC Status will expire.

After a Level 2 certification assessment, as well as after a POA&M closeout, the C3PAO will input the OSC's results into the CMMC instantiation of eMASS as described in § 170.17(a)(1)(i). After a Level 2 certification assessment, as well as after a POA&M closeout, the OSC must submit an affirmation as described in § 170.22.

In order to be eligible for a contract with a requirement for the CMMC Status of Level 2 (C3PAO), the OSC must have achieved the CMMC Status of either Conditional Level 2 (C3PAO) or Final Level 2 (C3PAO) and have submitted an affirmation. The Level 2 certification assessment must be completed every three years and the affirmation must be completed annually following the Final CMMC Status Date.

Section 170.18 CMMC Level 3 Certification Assessment and Affirmation Requirements

Section 170.18 addresses how an OSC will achieve and maintain compliance with the CMMC Status of Level 3 (DIBCAC). The OSC must have achieved the CMMC Status of Final Level 2 (C3PAO) for information systems within the Level 3 CMMC Assessment Scope as a prerequisite to undergo a Level 3 certification assessment. The OSC must successfully implement the security requirements listed in § 170.14(c)(4) and table 1 to § 170.14(c)(4) within its Level 3 CMMC Assessment Scope as described in § 170.19(d). Successful implementation requires meeting all objectives defined in NIST SP 800-172A Mar2022 for the corresponding CMMC Level 3 security requirements. Requirements for ESPs and CSPs that process, store, transmit CUI are provided in § 170.18(c)(5) and (6).

After implementation, the OSC must contact DCMA DIBCAC to perform an assessment to verify the implementation. DCMA DIBCAC will score the OSC using the scoring methodology provided in § 170.24. All objectives must be met in order for a security requirement to be considered fully implemented; in some cases, if not all objectives are met, some security requirements may be placed on a POA&M as defined in § 170.21. If the minimum score has been achieved and some security requirements are in a POA&M, the OSC has achieved the CMMC Status of Conditional Level 3 (DIBCAC); if all requirements are MET as defined in § 170.24(b), the OSC has achieved the CMMC Status of Final Level 3 (DIBCAC). For Conditional Level 3 (DIBCAC), a POA&M closeout must be conducted within 180 days as described in § 170.21(b) or the Conditional Level 3 (DIBCAC) CMMC Status will expire.

After a Level 3 certification assessment, as well as after a POA&M closeout, DCMA DIBCAC will input the OSC's results into the CMMC instantiation of eMASS as described in § 170.18(a)(1)(i). After a Level 3 certification assessment, as well as after a POA&M closeout, the OSC must submit an affirmation as described in § 170.22.

In order to be eligible for a contract with a requirement for the CMMC Status of Level 3 (DIBCAC), the OSC must have achieved the CMMC Status of either Conditional Level 3 (DIBCAC) or Final Level 3 (DIBCAC) and have submitted an affirmation. The Level 3 certification assessment must be completed every three years and the affirmation must be completed annually following the Final CMMC Status Date.

Section 170.19 CMMC Scoping

Section 170.19 addresses the requirements for the scoping of each CMMC Level and determines which assets are included in a given assessment and the degree to which each is assessed. The CMMC Assessment Scope is specified prior to any CMMC assessment, based on the CMMC Level being assessed. The Level 2 CMMC Assessment Scope may also be affected by any intent to achieve a CMMC Level 3 Certification Assessment, as detailed in § 170.19(e).

Scoping for CMMC Level 1, as detailed in § 170.19(b), consists of all assets that process, store, or transmit FCI. These assets are fully assessed against the applicable CMMC security requirements identified in § 170.14(c)(2) and following the procedures in § 170.15(c). All other assets are out-of-scope and are not considered in the assessment.

Scoping for CMMC Level 2, as detailed in § 170.19(c), consists of all assets that process, store, or transmit CUI, and all assets that provide security protections for these assets. These assets are fully assessed against the applicable CMMC security requirements identified in §

170.14(c)(3) and following the Level 2 self-assessment procedures in § 170.16(c) or the Level 2 certification assessment procedures in § 170.17(c). In addition, Contractor Risk Managed Assets, which are assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place, are documented and are subject to a limited check that may result in the identification of a deficiency, as addressed in table 3 to § 170.19(c)(1). Finally, Specialized Assets, which are assets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment, are documented but are not assessed against other CMMC security requirements, as addressed in table 3 to § 170.19(c)(1). All other assets are out-of-scope and are not considered in the assessment.

Scoping for CMMC Level 3, as detailed in § 170.19(d), consists of all assets that can (whether intended to or not) or do process, store, or transmit CUI, and all assets that provide security protections for these assets. The CMMC Level 3 Assessment Scope also includes all Specialized Assets but allows an intermediary device to provide the capability for the Specialized Asset to meet one or more CMMC security requirements, as needed. These assets (or the applicable intermediary device, in the case of Specialized Assets) are fully assessed against the applicable CMMC security requirements identified in § 170.14(c)(4) and following the procedures in § 170.18(c). All other assets are out-of-scope and are not considered in the assessment.

If an OSA utilizes an ESP, including a Cloud Service Provider (CSP), that does not process, store, or transmit CUI, the ESP does not require its own CMMC assessment. The services provided by the ESP are assessed as part of the OSC's assessment as Security Protection Assets.

Section 170.20 Standards Acceptance

Section 170.20 addresses how OSCs that, prior to the effective date of this rule, have achieved a perfect score on a DCMA DIBCAC High Assessment with the same scope as a Level 2 CMMC Assessment Scope, will be given a CMMC Status of Level 2 (C3PAO).

Section 170.21 Plan of Action and Milestones Requirements

Section 170.21 addresses rules for having a POA&M for the purposes of a CMMC assessment and satisfying contract eligibility requirements for CMMC. All POA&Ms must be closed within 180 days of the Conditional CMMC Status Date. To satisfy CMMC Level 1 requirements, a POA&M is not allowed. To satisfy CMMC Level 2 requirements, a POA&M is allowed. Section 170.21 details the overall minimum score that must be achieved and identifies the Level 2 security requirements that cannot have a POA&M and must be fully met at the time of the assessment. To satisfy CMMC Level 3 requirements, a POA&M is allowed. Section 170.21 details the overall minimum score that must be achieved and identifies the Level 3 security requirements that cannot have a POA&M and must be fully met at the time of the assessment. Section 170.21 also established rules for closing POA&Ms.

Section 170.22 Affirmation

Section 170.22 addresses that the OSA's Affirming Official must affirm, in SPRS, compliance with the CMMC Status: upon completion of any self-assessment, certification assessment, or POA&M closeout assessment (as applicable), and annually following a Final CMMC Status Date.

Section 170.23 Application to Subcontractors

Section 170.23 addresses flow down of CMMC requirements from the prime contractor to the subcontractors in the supply chain. Prime contractors shall comply and shall require subcontractor compliance throughout the supply chain at all tiers with the applicable CMMC Level for each subcontract as addressed in § 170.23(a).

Section 170.24 CMMC Scoring Methodology

Section 170.24 addresses the assessment finding types MET, NOT MET, and NOT APPLICABLE (N/A) in the context of CMMC assessments, and the CMMC Scoring

Methodology used to measure the implementation status of security requirements for CMMC Level 2 and CMMC Level 3. Scoring is not calculated for CMMC Level 1 since all requirements must be MET at the time of assessment.

For CMMC Level 2, the maximum score is the total number of Level 2 security requirements and is the starting value for assessment scoring. Any security requirement that has one or more NOT MET objectives reduces the current score by the value of the specific security requirement. Values for each CMMC Level 2 requirement are enumerated in § 170.24(c)(2)(i)(B).

For CMMC Level 3, the maximum score is the total number of Level 3 security requirements and is the starting value for assessment scoring. Any security requirement that has one or more NOT MET objectives reduces the current score by the value of the specific security requirement. CMMC Level 3 does not use varying values; the value for each requirement is one (1), as described in § 170.24(c)(3).

Appendix A to Part 170: Guidance

Appendix A lists the guidance documents that are available to support defense contractors and the CMMC Ecosystem in the implementation and assessment of CMMC requirements.

Discussion of Public Comments and Resulting Changes

The Department of Defense published the proposed rule, on December 26, 2023 (88 FR 89058). Approximately 361 public submissions were received in response to the publication. Some comments were beyond the scope of the CMMC Program and are described but not addressed in this final rule. The majority of comments received were relevant and are summarized in the discussion and analysis section here. Additional comments were received in response to the CMMC supplemental documents published concurrently with the rule; the discussion and analysis of those comments is located at www.regulations.gov. Some comments received lacked relevance to the rule's content, which is limited to specific CMMC program requirements codified in the 32 CFR part 170 CMMC Program rule, responses for those comments are not provided.

Any contractual requirements related to the CMMC Program rule will be implemented in the DFARS, as needed, which may result in revisions to the DFARS clause 252.204-7021, CMMC Requirements. DoD will address comments regarding the DFARS clause 252.204-7021 in a separate 48 CFR part 204CMMC Acquisition rulemaking.

1. Extension of the Public Comment Period

Comment: DoD received requests from industry associations for an extension of the 60-day public comment period on the CMMC Proposed Rule that the Office of the Federal Register published on 26 December 2023. The length of extensions requested ranged from 30-60 days. Commenters argued that the proposed rule was initially published following a holiday, or more time was needed for associations to fully review member comments about the CMMC Proposed Rule prior to submitting. In addition, they argued that other rules pertaining to cyber incident reporting obligations and security of Federal Information Systems had also been published for public comment, which created a need for additional review time.

Response: The DoD CIO denied requests for an extension of the 60-day public comment period. The DoD provided regular communication to the public through the DoD CMMC website and updates in the semiannual Unified Agenda in preparation for publication of the CMMC Proposed Rule to initiate the 60-day public comment period. The Department has an urgent need to improve DIB cybersecurity by further enforcing compliance with security requirements that were to be implemented by the DIB "as soon as possible but not later than December 2017." ***2.***

The CUI Program

a. CUI Program Guidance

Comment: Many comments were submitted related to the NARA CUI policies or the DoD CUI Program, and while relevant for understanding CMMC requirements, those are separate policies or programs beyond the scope of the CMMC program or this rule. However, several comments recommended that the CMMC rule be revised to address them.

Twenty-two comments requested the government provide more guidance, preferably within RFPs or contracts, to better identify what will be considered CUI for that contract, and how it should be appropriately marked. One comment specifically noted a need for contractual instructions on whether data created in performance of a contract rises to the level of CUI. Another person asked when is does information created or possessed by a contractor become CUI. One comment asked whether digital or physical items derived from CUI are treated as CUI while another asked what specific information qualifies as CUI for OT and IoT assets. Another comment asked whether FCI and or CUI created or provided under a non-DoD agency contract, but which is also used in support of a DoD contract, would be subject to the applicable CMMC level requirement. Another comment noted that DoD focuses too narrowly on data security aspects of major system acquisition and largely fails to address securing data generated by operational and/or maintenance operations, such as invoices and bills of lading for operational support purchases.

One comment stated there was a need for CUI policy guidance for the entire Federal Government. Another comment inferred, incorrectly, that the CMMC Accreditation Body makes determinations about what is and what is not CUI and stated that the Government should make those determinations. Another comment stated that to better address the needs of contractors tasked with safeguarding CUI, NARA should initiate a public comment period to reevaluate its CUI Registry. The comment also noted that NARA should identify when a CUI designation automatically applies to contractor-created information and revise the CUI Registry to stipulate that a specific basis in statute (or a contract) is required for information to be considered CUI. Another comment recommended a study be conducted on protections for systems and data at Confidential and higher classification levels and should assess whether NARA's CUI protection requirements (32 CFR part 2002) have yielded any real benefits in protecting critical data. Another comment stated that the CUI program is a costly proposition whose security value is questionable given data can still be compromised, even over systems with a CMMC assessment. The comment stated that if data is to be controlled for Critical Items, then the existing system used for CONFIDENTIAL information should suffice. Finally, another comment suggested that CUI information should be under the control of the Federal Government and access granted only to appropriately trained, and qualified contractors through a portal.

Response: Neither the CUI program (established in EO 13556) nor the safeguarding requirements codified in its implementing directives are changed by virtue of the compliance assessment framework established by this rule.

CMMC requirements apply to prime contractors and subcontractors throughout the supply chain at all tiers that will process, store, or transmit any FCI or CUI on contractor information systems in the performance of the DoD contract or subcontract, irrespective of the origin of the information.

The executive branch's CUI Program is codified in 32 CFR part 2002 and establishes policy for designating, handling, and decontrolling information that qualifies as CUI. The definition of CUI and general requirements for its safeguarding are included in 32 CFR 2002.4 and 2002.14, respectively. 32 CFR 2002.14(h)(2) specifically requires agencies to use NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems. At the time of award, the DoD may have no visibility into whether the awardee will choose to further disseminate DoD's CUI, but DFARS clause 252.204-7012 and DFARS clause 252.204-7021 require the prime contractor to flow down the information security requirement to any subcontractor with which the CUI will be shared. Decisions regarding which DoD information must be shared to support completion of subcontractor tasks is between the prime contractor and the subcontractors. The DoD encourages prime contractors to work with subcontractors to lessen the burden of flowing down CUI. The DoD declines to adopt alternatives such as policy-based solutions that lack a rigorous assessment component or require sharing CUI only through DoD-hosted secure platforms. Suggested alternatives to implementing NIST SP 800-171 and identifying what data is CUI are beyond the scope of the CMMC Program and this rule.

b. FCI and CUI Definitions

Comment: Five comments stated that what DoD considers CUI is not well defined. Another comment stated that companies should be provided a reference list of what the DoD considers CUI. Another recommended DoD use existing mechanisms like the DD Form 254 architecture to clearly define the scope of CUI on a contract-by-contract basis. Seven comments recommended the CMMC rule mandate a Security Classification Guide (SCG) or similar document.

Nine comments stated there was too much confusion and ambiguity regarding FCI and CUI and that the government needed to provide clear and standardized FCI and CUI definitions that are tailored to the specific requirements of the CMMC rule. One comment recommended rule edits to address this perceived ambiguity. One comment requested clarification and examples of differences between CUI Basic and Specialized CUI.

Response: Federal Contract Information is defined in FAR clause 52.204-21, which also provides the security requirements applicable for basic safeguarding of such information. The DoD has no authority to modify definitions established in the FAR for application to all executive branch agencies. This rule makes no change to the definition or handling of CUI.

c. Marking Requirements

Comment: Twenty-three comments expressed concern with or requested clarification regarding CUI marking. Twelve comments specifically noted concern with CUI markings being applied to too many documents, in part because CUI was an ambiguous concept. They requested the DoD encourage personnel to mark documents as CUI only when appropriate and provide better guidance for managing flow-down clauses. Another comment noted that many small businesses are currently subject to NIST SP 800-171 requirements through DFARS contract clause flow-down and cannot say with certainty that they have CUI in their possession. The comment further noted that small businesses regularly receive mismarked data. One comment stated there is an increased use of automatic CUI marking on DoD communications, seemingly without regard to content. One comment stated that the rule fails to outline a mechanism for reporting government mishandling, and that contractors should use a reporting system to minimize their own risk and liability. One comment requested the rule be edited to prevent Program Managers or requesting activities from assigning a CMMC Level 3 requirement unless they have high confidence that 80+ percent of CUI and/or FCI under the relevant contract has complete CUI markings. Another comment stated that the Federal government should develop a marking schema to communicate information safeguarding requirements, while yet another stated that DoD must publish a training module for contracting officers so that they are properly classifying documents prior to finalization of this rule.

One comment stated CUI across the DoD is diverse and what may be CUI for one system may not be for another. The comment then questioned how this proposed rule and SPRS would accommodate these facts without assuming and mandating that all defense contractor information systems meet the same architecture, security, and cybersecurity standards.

Response: The CMMC Program will not provide CUI guidance materials to industry as it is outside the scope of this CMMC rule. Relevant information regarding what to do when there are questions regarding appropriate marking of CUI may be found at 32 CFR 2002.50 - Challenges to designation of information as CUI. The DoD declined to incorporate suggested edits to the CMMC Level 3 requirements regarding confidence in proper CUI and/or FCI markings.

The DoD's role as data owner is documented in the CUI Program implementing policies and the requirements of 32 CFR part 2002. DoDI 5200.48, states: The authorized holder of a document or material is responsible for determining, at the time of creation, whether information in a document or material falls into a CUI category. If so, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly. DoD Manual 5200.01 outlines DoD's Information Security Program and includes Volume 2, Marking of Information. The DoD declines to incorporate by reference those documents describing the Department's data governance role because the content is beyond the scope of CMMC requirements. The DoD issued policy guidance to its program managers regarding programmatic indicators to consider

when selecting CMMC requirements. Program managers have a vested interested in knowing whether a contractor can comply with these existing requirements to adequately safeguard CUI.

The DoD elected not to make any recommended edits to the CMMC Program related to FCI or CUI marking requirements or provide clarifying examples of the differences between Basic CUI and Specified CUI, as these are beyond the scope of this rule. Mishandling of information by the government is beyond the scope of this rule. DCMA DIBCAC processes, stores, and transmits all data on DoD-approved networks. DoD's adherence to NARA's CUI Program policies is beyond the scope of this rule.

d. **Applicability and Governance of CUI Requirements**

Comment: In addition, one utilities sector representative submitted a lengthy analysis of data types often generated by electric or other utilities, with regulatory references and rationale for why such data would not likely be subject to DoD's CUI safeguarding requirements or CMMC compliance assessments. Such rationale included the fact that some Government-Private CUI categories, such as DoD Critical Infrastructure Information, require explicit designation in that category which (according to the commenter) has not occurred in the electricity subsector. One contractor requested that CMMC clarify requirements around U.S. persons and foreign dissemination of CUI for both contractors, subcontractors' employees, and contingent workers. Two comments suggested it would be appropriate to reference data governance in §170.1 and the DoD's role as the data owner of FCI and CUI across the ecosystem. Another comment stated the classification efforts must themselves be audited.

Response: The quantity of FCI and CUI a defense contractor possesses, including copies of the same material, is irrelevant to the CMMC assessment required. All copies of FCI or CUI related to the DoD contract must be safeguarded. The CMMC Program is not intended to validate compliance with cybersecurity requirements of non-DoD agencies' contracts. The requirements for sharing of CUI with non-US persons is beyond the scope of this rule.

The CMMC program provides a mechanism to assess contractor compliance with applicable security requirements for the safeguarding of FCI or CUI. CMMC program requirements make no change to existing policies for information security requirements implemented by DoD. Policies for CUI and creation of program documentation, to include Security Classification Guides, are separate from this rule. Discussion in this rule regarding DoD programs providing CUI training and the implementation of EO 13556 are beyond the scope of this rule.

CMMC program requirements are applicable when DoD requires processing, storing, or transmitting of either FCI or CUI on a non-Federal contractor owned information system in the performance of a contract between DoD and the contractor. The DoD does not manage nor is it involved in data exchanges between contractors and subcontractors.

3. Other DoD Policies and Programs

Many comments dealt with DoD policies and programs that, while relevant for understanding CMMC requirements, are still entirely separate programs or policies that are not within the scope of the CMMC program. However, several commenters recommended that the rule be revised to address them. Key topics among such comments include:

a. Adaptive Acquisition Framework

Comment: One commenter misunderstood CMMC program purpose and thought the requirements applied to systems and capabilities acquired or developed for DoD's use, using formal policies of the Defense Acquisition System. Based on this misinterpretation, this commenter made dozens of recommendations related to integration of CMMC assessment and program requirements with other existing DoD acquisition frameworks and suggested relying on the assessors that complete TRAs, in place of implementing the CMMC program. One of their comments also proposed establishing a single responsible office for CUI and SCRM, hosting CUI material within a single, separate secure and existing cloud-based data warehouse and including hardware and software approving authorities as part of the proposed rule for GFE. The commentor also stated the role of the Office of Small Business Programs (OSBP) needs to flow down to the Small Business Administration military service offices. The commentor also asked how to reconcile CMMC against the DoDI 8582.01 requirement stating a DoD Component

should not specify the content and format of plans of action that address deficiencies or specifying the parameters of security controls.

This commenter also recommended creation of a MIL-Standard in lieu of aligning cybersecurity requirements to existing NIST standards, and linkage of CMMC requirements to procedures related to Approval to Operate (which applies to DoD systems. This commenter suggested that the CMMC PMO be made responsible to provide system scans to check for Software Bills of Material as part of DoD's response to Executive Order 14028 regarding Supply Chain Risk Management. The commenter further requested a DoD-level working group outline how DoD program offices might identify which components are mission or safety critical or which associated production processes should be identified as CTI. That commenter recommended this rule be held in abeyance until AT&L [sic] has reviewed and provided their insight into the impacts of CMMC on existing DoD acquisition documentation and deliverables. Yet another comment recommended that "this proposed DFARS ruling" be vetted through "AT&L, ASD and OUSD" [sic] as a minimum to determine if changes would be required in the Program Protection Improvement Plan and System Security Plan. Lastly, this commenter recommended the DoD engage with NDIA and ISO/IEC to develop alternate standards for securing data and supply chains.

Response: CMMC Program requirements apply to contractor-owned information systems that process, store, or transmit FCI and CUI and do not apply to systems developed or acquired for DoD through the formal Defense Acquisition System (DAS). Therefore, integrating the CMMC assessment process and internal DAS processes (including technical reviews prior to RFP development) is not appropriate and is beyond the scope of this rule. Note that CMMC applicability is broader than just the Major Defense Acquisition Programs.
DoD's organizational alignment of responsibilities (between OSBP and SBA military offices) for assisting small businesses or establishing new offices within OSD is beyond the scope of this rule. Due to national security concerns, DoD declines the recommendation to further delay implementation of the CMMC Program. Each passing day in delay of implementing the security requirements for safeguarding DoD FCI and CUI increases the risk for exfiltration of non-public information on unsecured nonfederal systems that may result in the loss of DoD's technological advantages in its warfighting capabilities and programs.

Discussions regarding acquisition strategies and frameworks are beyond the scope of this CMMC rule. The CMMC Program does not alleviate or supersede any existing requirements of the Adaptive Acquisition Framework, nor does it alter any statutory or regulatory requirement for acquisition program documentation or deliverables. Note that CMMC Program requirements do not apply to systems delivered to DoD. DoD Instructions for required acquisition program documentation are beyond the scope of this rule. CMMC assessment certifications are not integrated into System Security Plans (SSPs).

The role of System Engineering and associated processes within the DoD acquisition process is beyond the scope of this rule. ITRA assessments provide a view of program technical risk and are not well-suited to the assessment of contractor owned information systems against standards for safeguarding CUI. CMMC Program requirements do not clash with Program Office responsibilities, but instead provide Program Manager's with a mechanism for validating that contractors are compliant with the rules for protecting DoD CUI.

b. FedRAMP Program and FedRAMP Equivalency

Comment: Many commenters took issue with the requirements for FedRAMP Moderate Equivalency, as referenced in DFARS clause 252.204-7012 and defined in a separate DoD policy memo. Some merely highlighted discrepancies or highlighted concerns about their ability to meet the FedRAMP Moderate Equivalency requirements. Others recommended revisions to that policy, or to the DFARS clause 252.204-7012 clause, or both. Some recommended the FedRAMP Moderate Equivalency policy memo be incorporated into the DFARS clause 252.2047012 clause. Other suggestions ranged from eliminating equivalency to meet requirements, allowing 3PAO attestation to equivalency, requiring all FedRAMP Moderate Equivalency candidates to be assessed by the same C3PAO or allowing equivalency to be

established through other industry certifications or third-party security assessments, i.e., SOC, ISO/IEC 27001. One commenter requested that applications hosted on a FedRAMP Moderate environment only need to meet the CMMC level of the data the application will process. Another suggested that all Cloud Service Providers be required to meet the same CMMC requirement as the OSCs they support. One commenter recommended expanding the scope of CMMC Program to include assessing other security requirements in DFARS clause 252.204-7012, to include the use of FedRAMP Moderate cloud environment. Comments also expressed that it is unreasonable to expect any cloud provider to share security documentation with a customer or C3PAO since they limit dissemination of this information due to operational security needs. Another commenter noted that the proposed rule does not cover all types of information that contractors may handle, such as classified information, export-controlled information, or proprietary information and they recommended the DoD clarify applicability of the CMMC program for these types of information.

Response: Although some commercially based Cloud Service Offerings (CSOs) may experience limitations in trying to support the Defense Industrial Base with the FedRAMP Moderate equivalent requirement, the DoD is not willing to assume all the risk of non-FedRAMP Moderate Equivalent CSOs when the CSO is used to process, store, or transmit CUI. If the offering does not process, store, or transmit CUI, then FedRAMP certification is not required. Although the DoD considered acceptance of the ISO/IEC 27001 certification, it chose the NIST cybersecurity requirement to meet FedRAMP Moderate baseline equivalency standard to stay aligned with the FedRAMP Moderate baseline which is based on NIST standards versus ISO/IEC standards.

The rule was updated to require FedRAMP moderate or FedRAMP moderate equivalency in accordance with DoD Policy. CMMC Program Requirements make no change to existing policies for information security requirements implemented by DoD. Comments related to applications hosted on a FedRAMP Moderate environment are outside the scope of this rule. The requirements for CSPs that process, store, or transmit CUI are set by DFARS clause 252.204-7012 and the DoD CIO policy memo on FedRAMP Moderate equivalency. These requirements are beyond the scope of this rule. ESPs that are not CSPs will be required to meet the CMMC requirements and be assessed as part of the scope of an acquiring OSA. ESPs that are not a CSP may voluntarily request a C3PAO assessment if they decide it would be to their advantage.

c. Other DoD Programs and Policies

Comment: One commenter expressed dissatisfaction with results obtained from previously submitted FOIA requests related to development of the CMMC program.

Two commenters asked if there was a mechanism to update FAR clause 52.204-21 to address evolving threats and recommended the Department specifically identify the frequency and identify accountable parties to review and update FAR security requirements. Another commenter cited responses visible on the DoD CIO's Frequently Asked Questions (FAQ) web site and criticized both the utility of the information (given that does not constitute formal policy) and the frequency with which the information is updated. Similarly, one commenter asked for more frequent updates to FAQs on the DoD Procurement Toolbox URL.

One commenter asserted that the Federal Government sometimes contracts for support to perform sensitive tasks and permits access to "highly classified" information that should only be accessed by Federal employees.

One commenter requested NIST develop a simplified inspection standard for organizations with less than 20 employees.

One commenter asked about the transfer of CMMC Program oversight from OUSD(A&S) to DoD CIO.

A comment cited the utility of free cybersecurity related services that DoD agencies offer, such as security alerts and vulnerability scanning, and encouraged expansion of those programs.

One person suggested that DoD's Zero-Trust approach would provide a higher level of security for CUI data than the CMMC program.

One commenter stated the Department should develop clear, flexible guidelines and alternative pathways for global companies to achieve CMMC compliance without relying on enclave architectures and recommended that this approach rely on Zero Trust principals.

One comment noted that under FAR clause 52.204-21, FCI does not include simple transactional information (STI) and asked if certain data would be considered STI and therefore not subject to CMMC.

One comment stated that conflicting regulatory guidance exists between the content of E.O. 15028, NIST SP 800-218, NIST SP 800-171 R2, and NIST SP 800-171 Revision 3.

Response: One comment lacked clarity and failed to clearly articulate any relevance to the content of this rule, so no response can be provided.

SPRS will be used for reporting CMMC Status of all contractors, regardless of which service issued the contract. Publication of this rule follows completion of OMB's formal rulemaking process, which includes both DoD internal coordination (including the USD(A&S) and USD(R&E)) and Interagency coordination.

CMMC is consistent with Section 3.4 of DoDI 8582.01, Validation and Compliance. CMMC does not specify the content and format of plans of action beyond what is specified in NIST SP 800-171 R2, which is required under DoDI 8582.01.

Clinger Cohen Act requirements, which apply to DoD's IT investments, are not relevant to CMMC Program requirements, which apply to contractor-owned information systems. The classification marking of existing DoD documentation is beyond the scope of this rule, as is engagement with INCOSE and ISO/IEC certification organizations.

Executive Orders state mandatory requirements for the Executive Branch and have the effect of law. EO 14028 - "Improving the Nation's Cybersecurity" (issued May 12, 2021) requires agencies to enhance cybersecurity and software supply chain integrity. NIST SP 800-171 R2 and NIST SP 800-218 are guidelines, not regulations. NIST SP 800-171 Revision 3 is not currently applicable to this rule.

Recommendations to add or modify requirements specified in NIST documentation should be submitted in response to NIST requests for public comment on the applicable guidelines. Federal and DoD requirements for delivery of software bills of material of secure software development are beyond the scope of this rule, which is limited to the assessment of compliance with requirements for adequate protection of FCI and CUI. Federal Contract Information is defined in FAR clause 52.204-21, which also provides the security requirements applicable for basic safeguarding of such information. The Department has no authority to modify definitions established in the FAR for application to all executive branch agencies. Any data that meets the definition of FCI, is subject to CMMC Level 1. It is beyond the scope of the CMMC rule to render decisions on specific elements of data.

The OUSD(A&S) was not replaced by the DoD CIO, rather, CMMC Program management oversight has been realigned from the OUSD(A&S) to the Office of the DoD CIO for better integration with the Department's other DIB cybersecurity related initiatives. Comments pertaining to DoD's organizational structure are not relevant to the content of this rule. DoD's processing of FOIA requests is also not within the scope of this rule. The DoD declines to respond to speculative or editorial comments about private citizens or outside entities, all of which are beyond the scope of this rule. Likewise, the DoD will not comment here on other DoD cybersecurity related programs, such as Zero Trust.

Some comments expressed appreciation for cybersecurity related services that DoD provides free of charge, including protected DNS, vulnerability scanning, and security alerts, but these programs are outside the CMMC program. The government cannot comment on specific implementation or documentation choices of an OSA. Comments on alternate risk mitigation strategies such as product monitoring or software testing are not within the scope of this rule text.

d. DoD Policies Supporting CMMC Implementation

Comment: Some comments addressed the DoD's internal policies and training efforts to prepare the Government workforce for CMMC program implementation. For example, some

commenters opined that the rule's focus on contactor responsibilities misses the true risk that lies further up obscure supply chains. Another commenter recommended DoD work with contractors in each sector to provide clear guidance on the types of data that the Department would consider CTI. One commenter requested DoD acknowledge that human factors influence DIB cybersecurity while another stated DoD should provide uniform web-based training at no cost to ensure applicable training requirements are satisfactorily met. Another asked whether DoD PMs would receive CMMC related training prior to implementation. Another comment asked whether specific risk mitigating approaches, such as product monitoring or software testing might suffice to manage supply chain risk considering lack of visibility into the origins of 3rd and 4th tier components.

One commenter perceived the CMMC requirement for Program Managers to identify the level of assessment requirement appropriate for a solicitation as removing the contract award decision from the USD(A&S). One commenter stated more information about procedures for implementing CMMC into government-wide contracts is needed. Another commenter expressed a need to use a basic contract that is unclassified, and any CUI would be contained in a separate appendix to allow sub-contractors to plan with their Prime to access the information on the Prime's network and avoid requirements for their own CMMC certification.

Another comment recommended revisions to describe that medium assurance certificates for incident reporting are a DFARS clause 252.204-7012 requirement, independent of CMMC program requirements.

Two commenters criticized the DFARS clause 252.204-7020 requirement to allow "full access" to contractor facilities, systems, and personnel for the purposes of DIBCAC assessment, or for damage assessment following incident, and recommended that the CMMC program not include or rely on this authority.

Another commenter recommended that, prior to issuing a final rule on CMMC, DoD work with other relevant agencies to integrate and harmonize the numerous regulatory changes that impact contractors' capacity to safeguard data and systems. One commenter suggested rule publication be delayed until DoD articulates the benefit expected from contractor compliance with the rule.

Response: All recommendations to revise other Government-wide or DoD policies and programs are beyond the scope of the CMMC rule.

CMMC Program Requirements make no change to existing policies for information security requirements implemented by DoD. Policies for CUI and creation of program documentation, to include Security Classification Guides and FedRAMP equivalency are separate from this rule. Relevant policies include DoDI 5200.48 "Controlled Unclassified Information" and DoD Manual 5200.45 "Instructions for Developing Security Classification Guides" for example[24]. Some comments received lacked relevance to the rule's content, which is limited to specific CMMC program requirements. Changes to FAR and DFARS requirements are beyond the scope of this rule, as are the contents and updating of DoD's FAQ and Procurement Toolbox web pages.

CMMC program requirements do not result in any change to which DoD organization makes the contract award. Recommendations to adopt standard DoD contracting procedures (i.e., to exclude CUI information in the basic award) are not within the scope of this rule, which outlines program requirements. The DoD limits the burden of CMMC compliance by requiring annual affirmations rather than annual assessments. Affirmations required for the CMMC program indicate that a DoD contractor has achieved and intends to maintain compliance with the applicable DoD information security requirements.

The CMMC program is designed only to validate implementation of the information security standards in FAR clause 52.204-21, NIST SP 800-171 R2, and a selected subset of NIST SP 800-172 Feb2021. This rule does not address the other DFARS clause 252.204-7012 requirements for cyber incident reporting. The CMMC assessment framework will not alter, alleviate, or

[24] DoD Issuances (www.esd.whs.mil/DD/DoD-Issuances)

replace the cyber incident reporting aspects of DFARS clause 252.204-7012, which will remain effective where applicable. Classified information is managed differently from CUI, and different safeguarding regulations apply to these different categories of information (each of which are defined in 32 CFR part 2002). CMMC Program requirements are aligned to the requirements for safeguarding of CUI and are unrelated to the requirements for safeguarding classified information. "Export Controlled" is a category of CUI. To the extent that a company generates information it considers proprietary, but which is explicitly excluded from the definition of CUI (see 32 CFR part 2002), no CMMC requirements would apply.

As the CMMC program requirements make no change to existing policies for information security requirements implemented by DoD, dialogues with industry to identify CUI is outside the scope of this 32 CFR part 170 CMMC Program rule. Several existing requirements directly address the human factors of cybersecurity, particularly those in the Awareness and Training, Personnel Security, and Physical Protection domains. Additional training and education on the topics of CUI safeguarding requirements, cybersecurity hygiene, and other useful topics may be found at:

www.archives.gov/cui/training.html https://securityawareness.usalearning.gov/
https://business.defense.gov/Resources/Be-Cyber-Smart/

OSAs may develop their own policies to validate completion of training. Developing and providing cyber security awareness training is not within the scope of the CMMC Program. DoD program managers will receive training.

In support of 32 CFR part 170 CMMC Program final rule, DoD issued guidance to reiterate the most appropriate information safeguarding requirements for DoD information and the associated CMMC assessment requirement for any given solicitation. Irrespective of CMMC Program assessment requirements, when CUI is processed, stored, or transmitted on contractor owned information systems, those systems are subject to the security requirements of NIST SP 800-171, due to the applicability of DFARS clause 252.204-7012. Program Managers have a vested interested in knowing whether a contractor can comply with these existing requirements to adequately safeguard DoD CUI.

Applicability of and compliance with DFARS clause 252.204-7020 is beyond the scope of the CMMC Program. Implementation of the CMMC Program does not require or rely upon DFARS clause 252.204-7020. The existing assessments described in DFARS clause 252.2047020 are entirely different than those described in this rule. This rule contains no cyber incident reporting requirements. Concerns related to a CISA rule pertaining to cyber incident reporting are beyond the scope of this rule and should have been submitted instead to the relevant docket for that rule. The DoD has declined the recommendation to address certificate requirements for the cyber incident reporting requirements of DFARS clause 252.204-7012 in this rule. The DoD is unable to comment on, balance with, or modify contractual or regulatory requirements to comply with any other agency's future requirements.

The preamble of this rule articulates how contractor compliance with CMMC will contribute to counteracting the cyber security threat. Implementation of the CMMC Program will help protect DoD’s FCI and CUI that is processed, stored, and transmitted on non-Federal information systems of defense contractors and subcontractors. Adequately securing that information as required, down to the smallest, most vulnerable innovative companies, helps mitigate the security risks that result from the significant loss of FCI and CUI, including intellectual property and proprietary data. Hence the implementation of the DoD CMMC Program is vital, practical, and in the public interest. Working with NIST and other regulatory authorities to align standards is beyond the scope of this rule.

4. DFARS Requirements

Comment: Two commenters recommended the DoD fully implement CMMC requirements to standardize contract requirements to avoid proliferation of unique contract clauses across the Department. One comment suggested the rule should state explicitly that CMMC requirements do not apply to other agencies and advise DoD contractors to seek legal guidance before complying with CMMC requirements if other agency requirements also apply.

In addition, several commenters thought the 32 CFR part 170 CMMC Program rule requirements lacked sufficient information about the associated 48 CFR part 204 CMMC Acquisition rule requirements to implement them. One person erroneously identified the DFARS clause 252.204-7021 as part of the 32 CFR part 170 CMMC Program rule, and one person asked what additional rulemaking is needed to implement CMMC requirements. Another person recommended close coordination and synchronization between the two rules. One comment recommended the contract clauses be simplified to be "stand alone", rather than requiring cognizance of the 32 CFR part 170 CMMC Program rule content.

One commenter asked whether contractors must meet CMMC requirements during the solicitation phase, or to view RFPs that contain CUI. Another asked how DoD plans to integrate CMMC requirements into DoD's Adaptive Acquisition Framework. One contractor disagreed with CMMC's pre-award approach, and worried it could create a need to become compliant in anticipation of future solicitations. This commenter posited that any information designated as CUI after contract award will create a "chicken and egg" dilemma for CMMC compliance. Other comments asked whether conditional certifications would be weighted differently than final certifications in the proposal evaluation and award process and suggested that DoD provide 6 months advance notice for all solicitations containing a CMMC requirement.

Some comments urged the DoD to describe how DoD will identify CUI in solicitations and when CUI markings should apply in CSP or ESP scenarios. They also requested modification of DoD contracting procedures to provide criteria for identifying CUI information in each contract award along with the corresponding CMMC assessment level. One commenter inquired about the difference between implementing security requirements and assessing compliance. Some comments pertained to other DFARS contractual requirements, rather than CMMC requirements. For example, some recommended changing DFARS clause 252.204-7012 to remove the definition of Covered Defense Information and to deviate from a requirement to comply with the NIST SP 800-171 version current at the time of solicitation. In addition, they asked about cost allowability for time and materials or cost type contracts. Some comments posited that costs for reassessment or recertification should be explicitly identified as reimbursable in the 48 CFR part 204 CMMC Acquisition rule, while one similar comment suggested that CMMC level 3 certification costs should be allowable when CMMC level 3 requirements are initially implemented.

One comment addressed cyber incident reporting timelines for cloud service providers and recommended that the DoD's FedRAMP moderate equivalency policy be revised to align with DFARS clause 252.204-7012 timelines. Another asked whether the rule inadvertently omitted requirements to assess compliance with DFARS clause 252.204-7012 cyber incident requirements.

Other commenters asked for the CMMC contract clause verbiage, as was subsequently published in the related 48 CFR part 204 CMMC Acquisition rule. For example, some people asked whether CMMC requirements would be levied in ID/IQ contract awards versus task order awards, and GSA schedules. They asserted that adding CMMC clauses in GSA schedules might inadvertently allow contracting officers to include them in non-DoD issued task orders. Another opined that ID/IQ contracting procedures might necessitate changing the CMMC level needed for the base contract after its initial award, based on the needs of a task order. One commenter incorrectly inferred that a single Program Manager would make the CMMC level and type determination for every task order issued against an ID/IQ. In addition, two comments suggested that the DoD communicate with every current DoD contractor to identify which CMMC level would apply to their existing contracts.

One company identified their specific DoD contract and asked whether it would be cancelled absent CMMC compliance. Another asked whether a current DFARS clause 252.204-7020 selfassessment score could be submitted to meet a CMMC level 2 self-assessment requirement. They also recommended elimination of the DFARS clause 252.204-7020 requirements when CMMC is implemented.

One commenter speculated about whether DoD's CMMC contract clauses can be applied to

DoD contractors that also make and sell the same product to other US Government agencies. They noted that export licenses do not restrict companies from providing product data to other parties and posited that this might conflict with CMMC requirements. One person asked about the potential for conflicts between CMMC clauses and the Berry amendment and suggested that Berry amendment compliance take precedence over CMMC clauses.

Response: Some comments received lacked relevance to the rule's content, which is limited to specific CMMC program requirements. Changes to FAR and DFARS requirements are out of scope of the 32 CFR part 170 CMMC Program rule, as contractual changes would occur under the 48 CFR part 204 CMMC Acquisition rule. This rule does not discuss the Berry Amendment. The rule does not address recovery of assessment costs because it does not make any change to 48 CFR 31.201-2.

This 32 CFR part 170 CMMC Program rule is not an acquisition regulation, however, a CMMC Conditional Certification meets the CMMC program certification requirements. Any comments related to contract requirements should be directed to the related 48 CFR part 204 CMMC Acquisition rule.

CMMC requirements apply to contracts that include FAR clause 52.204-21 or DFARS clause 252.204-7012 and result in processing, storing, or transmitting of FCI or CUI on a contractor owned information system. The CMMC program is not a verification program for compliance with all requirements of DFARS clause 252.204-7012, rather, its purpose is to ensure compliance with FAR clause 52.204-21, NIST SP 800-171 R2, and NIST 800-172 Feb2021 when applicable. The DoD does not provide detailed instruction on how to implement specific solutions to meet security requirements identified in the FAR clause or applicable NIST requirements, which is determined by the OSA. Any deviation from or change to the DFARS clause 252.204-7012 clause is beyond the scope of this rule.

Each of the teams responsible for developing these two CMMC rules has reviewed both documents.

There are no CMMC requirements for reviewing FCI or CUI solicitation material. Recommendations to adopt standard contracting procedures for award of DoD contracts (i.e., to exclude CUI information in the basic award) are out the scope of this 32 CFR part 170 CMMC Program rule. In support of the 32 CFR part 170 CMMC Program final rule, DoD issued policy guidance to its program managers and acquisition workforce to identify the appropriate CMMC requirement in solicitations and contracts. The CMMC assessment level required does not change based on acquisition lifecycle phase and is based on whether FCI and CUI are processed, stored, or transmitted on contractor owned information systems used in the performance of a contract.

Discussion of DoD's willingness to provide advance notice of CMMC requirements or to remove the PM's discretion to include the CMMC level that best suits program requirements is a 48 CFR part 204 CMMC Acquisition rule matter and outside the scope of this rule. The CMMC Level will be identified in the solicitation. Once attained, a CMMC self-assessment or certification can be used in support of any number of proposals and solicitations.

5. Litigation and False Claims

Comment: Some commenters expressed concern that CMMC implementation would result in increased litigation by DIB companies or pursuit of False Claims Act penalties by DoD against DIB companies. One commenter erroneously believed that Mexico would participate in oversight of the CMMC ecosystem, and that "a flood of litigation" may result from DIB companies losing contracts due to non-compliance with CMMC requirements. One commenter suggested that DoD should absolve contractors from False Claims Act prosecution when differences are found between C3PAO assessment results and a previously submitted contractor self-assessment, due to potentially valid reasons for the differing outcomes. Another suggested that DoD establish protections from regulatory and legal liability related to cyber incidents when the affected contractor has complied with relevant CMMC Program requirements.

Response: The DoD lacks the authority to change the False Claims Act, which is a Federal law that imposes liability persons and companies who defraud or knowingly submit false claims to the government. Comments related to Safe Harbor provisions are outside the scope of this rule.

Comments about potential industry litigation are also beyond the scope of the final rule and the recommendations provided were not appropriate for inclusion in this rule. Nothing in the rule prevents frivolous private lawsuits, but the rule does provide that the CMMC AB maintain an appeals process. The DoD has faithfully followed the formal rulemaking process, to include completion of the public comment period. Implementation of the CMMC program will be carried out objectively and in accordance with the tenets of the final rule. No foreign actors have any role in DoD's administration of the program.

6. DoD Metrics

Comment: Several commenters inquired about the types of metrics the DoD plans to use to monitor progress toward the DIB cybersecurity objectives that the CMMC program was designed to meet. One asked whether DoD's metrics would include testing, and another recommended they capture changes in the population of DoD contractors caused by cost impacts of CMMC implementation. Others referenced a December 2021 GAO Report that critiqued DoD's earlier attempts to implement the CMMC program. Specifically, they cited the GAO's finding that, at that time, DoD had not defined how it would analyze data to measure performance.

A comment recommended the DoD identify responses to other GAO findings, which dealt with improvements to communications with industry and metrics for program management. Another comment asked whether management alignment within OSD, budget, and staffing of the CMMC program office are adequate.

Two comments asked how many current contract awardees had received notification or identification of CUI to be provided in performance of their contracts, and asked which CMMC level would theoretically apply to those contracts. Another asked the DoD to provide DIBCAC assessment results data as a more relevant justification for the CMMC program than the 2019 DoDIG report on DIB Cybersecurity.

Response: DoD's response to the referenced GAO and DoD IG reports are beyond the scope of this rule. Likewise, the DoD does not comment on analysis methods supporting the DoD IG's conclusions. Publishing DIBCAC assessments results is also beyond the scope of this rule, as are CMMC Program effectiveness metrics and return on investment calculations. The DoD is establishing CMMC assessment requirements as part of a comprehensive effort to verify that underlying information security requirements are met, as required, for all contractor owned information systems that process, store, or transmit CUI or FCI in the performance of a DoD Contract. DoD's calculation of ROI for the security controls that CMMC will assess, and cost elasticity of the DIB are also beyond the scope of this rule.

7. Phased Implementation of the Program

Comment: Many comments asked for additional explanation of DoD's expected start and progression through phases of the CMMC implementation plan. Several asked that the phase-in plan be extended. One commenter asked whether contracts that would otherwise be associated with CMMC Level 3 would include a CMMC Level 2 requirement if issued prior to Phase 4 of the plan. Another misread the phase-in plan to mean that self-assessments would no longer be permitted at Full Implementation. One comment asked if the USG would be revisiting acquisition timelines to add more time for due diligence to ensure all entities meet CMMC requirements or have a POA&M in place.

Some commenters observed that DoD's intended dates for CMMC implementation, as published in an earlier 48 CFR CMMC interim final rule, are unachievable and must be changed via another CMMC DFARS rule. Some commenters were confused by the differences between the dates of implementation phases in the rule, and the seven years described in cost estimates as necessary to complete implementation. Another commenter asked why the rule only applies to DoD.

Some commenters suggested changes to prioritize different kinds of contracts, programs, or companies earlier or later in the implementation plan, rather than basing the phase-in on assessment type. For example, one suggested capping the number of contracts with CMMC requirements each year. Another suggested phasing in by increasing the numerical assessment score required for compliance, with additional time permitted for POA&M close-out beyond the current limit of 180 days. Another suggested reversing the phase-in to begin with CMMC Level 3. Several commenters requested extension of the phase-in plan to allow more time. One speculated that "tens of thousands" of contractors would require certification in less than 18 months. One commenter suggested the DoD modify the timing of implementation for CMMC levels 2 and 3, and that DoD consider allowing sufficient time to develop a robust CMMC ecosystem and demonstrate the CMMC model before full implementation.

Flexibility in the implementation plan that allows Program Managers and requiring activities to include CMMC requirements earlier in the plan than will be mandated by policy also generated questions and comments. Some commenters asked whether this could result in the DoD applying CMMC requirements to previously awarded contracts or asked that the rule specify they will apply only to new contracts. Another asked about opportunities to renegotiate the contract ceiling price if CMMC assessments are required for option period exercise. One commenter asked that the rule be revised to exclude these flexibilities to result in an "on/off" approach to implementation.

Another commenter asked what mechanisms the DoD would have to change the pace of implementation or monitor the contracts that include CMMC requirements.

Response: The DoD lacks the authority to implement CMMC as a Federal-wide program. The 48 CFR part 204 CMMC Acquisition rule for CMMC will be updated to align with this 32 CFR part 170 CMMC Program rule and will modify DFARS clause 252.204-7021. CMMC Phase 1 implementation will commence when both the 32 CFR part 170 CMMC Program rule and the 48 CFR part 204 CMMC Acquisition rule are in effect. Some commenters may have overlooked that § 170.3(e) states Phase 1 begins on the effective date of this 32 CFR part 170 CMMC Program rule or the complementary 48 CFR part 204 CMMC Acquisition rule, whichever occurs later. The implementation plan describes when CMMC level requirements will appear in solicitations, it does not define a timeframe by which all contractors must be certified. During the first phases of the plan, a majority of CMMC requirements will be for selfassessment.

In response to public comments, the DoD has updated the rule to extend Phase 1 by 6 months, with appropriate adjustments to later phases. DoD is not conducting Pilots in the updated CMMC implementation plan. The phased implementation plan described in § 170.3(e) is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements. DoD has updated the rule to add an additional six months to the Phase 1 timeline. Phase 2 will start one calendar year after the start of Phase 1.

The DoD's objective timeline to begin implementing the CMMC requirements has been, and remains, FY2025. The implementation period will consist of four (4) phases, 1 through 4, and is intended to address any CMMC assessment ramp-up issues, provide the time needed to train the necessary number of assessors, and to allow companies time to understand and implement CMMC requirements. It is estimated that full implementation of CMMC by all defense contractors will occur over seven years, given the number of DoD solicitations contractors respond to and are awarded each year.

The four phases add CMMC level requirements incrementally, starting in Phase 1 with Level 1 and Level 2 Self-assessments, and ending with Phase 4 for Full Implementation, as addressed in § 170.3(e)(4). By Phase 3, all CMMC Levels 1, 2, and 3 will be included in some DoD solicitations and contracts, but Level 3 requirements may be identified for implementation as option period requirements rather than for initial contract award. In Phase 4, DoD will include CMMC requirements in all applicable DoD contracts and option periods on contracts awarded after the beginning of Phase 4. As addressed in § 170.18(a), receipt of a CMMC Level 2 Final

CMMC Status for information systems within the Level 3 CMMC Assessment Scope is a prerequisite for a CMMC Level 3 certification assessment.

CMMC self-assessment requirements build on the existing DFARS clause 252.204-7020 requirement for basic safeguarding of CUI. CMMC Level 3 requires advanced implementation, and the phase-in period provides additional time for OSC to achieve the higher standard. In phase 4, which is full implementation, CMMC requirements must apply to new contracts and option year awards. The DoD may choose to negotiate modifications adding CMMC requirements to contracts awarded prior to CMMC implementation, as needed. No changes to this rule are needed to reflect existing contract administration processes. Questions on specific contracting matters, including contract costs and funding, are outside of the scope of this rule.

With the implementation of the final 32 CFR part 170 CMMC Program rule and 48 CFR part 204 CMMC Acquisition rule, prospective DoD contractors and subcontractors should be actively preparing for DoD contract opportunities that will include CMMC Program requirements when performance will require the contractor or subcontractor to process, store, or transmit FCI or CUI. The respective phases of the implementation plan provide adequate time to complete CMMC requirements and DoD program requirements and timelines will dictate the programs that may warrant CMMC Level 3 requirements during the phased implementation of CMMC.

DoD considered many alternatives before deciding upon the current CMMC implementation plan. The phased implementation plan is based on CMMC assessment level and type, which DoD believes to be a fair approach for all prospective offerors. Defining the phase-in based on contract type, company size standard, or other potential bases could lead to unfair advantage. Program Managers will have discretion to include CMMC Status requirements or rely upon existing DFARS clause 252.204-7012 requirements, in accordance with DoD policy. The DoD will monitor the Program Managers' exercise of this discretion to ensure a smooth phase-in period. The decision to rely upon CMMC self-assessment in lieu of certification assessment is a Government risk-based decision based upon the nature of the effort to be performed and CUI to be shared. Note that section § 170.20 Standards acceptance states OSCs that completed a DCMA DIBCAC High Assessment with a score of 110 and aligned with CMMC Level 2 Scoping, will receive Final CMMC Status for a Level 2 certification assessment.

As noted by one commenter, self-assessments against NIST SP 800-171 are already required, and verifying compliance with applicable security requirements is necessary for the protection of DoD CUI. For all CMMC independent assessments (i.e., Level 2 or 3), DoD policy guides Program Managers in appropriately including these requirements in DoD solicitations. DoD systems that support the procurement process can identify the number of contracts issued that include any specific clause. Such metrics for the CMMC Program are not within the scope of this rule.

The seven-year timespan reflects the DoD's estimate for all defense contractors to achieve CMMC compliance. The implementation plan ramps up CMMC assessment requirements over 4 phases, such that the ecosystem will reach maximum capacity by year four. One commenter referenced the response to a specific comment to the 2020 CMMC rule. Those earlier questions about the 2020 rule publication are no longer relevant due to changes made in the more recent 2023 rule publication. DoD estimates acknowledge that contractors with existing contracts may not receive another contract award or even submit another proposal immediately.

The DoD has developed CMMC to increase consistency of implementation of NIST SP 800171 R2 and NIST SP 800-172 Feb2021. Specifically, this rule provides extensive information on scoring methodology, in an effort to improve self-assessments. The use of independent C3PAOs further enforces consistency for those companies that need to meet a CMMC Level 2 certification requirement. The DoD has considered the suggestions and declines to modify the phase-in periods based on total score required, or other criteria, which would not provide the desired improvements in DIB cybersecurity.

The DoD notes the commenter's concern that self-assessments go away after Phase 4.

Requirements from earlier phases continue as each additional phase is implemented. When applicable, self-assessments will still be allowed, as appropriate, in Phase 4. This rule describes flow down requirements to subcontractors. This rule makes no change to 48 CFR 252.204-7008.

8. Commercially available off-the-shelf (COTS) Procurements

Comment: One comment suggested the definition of COTS should be more explicitly defined or the model outlined in § 170.2 should encompass COTS products. Two comments questioned the exemption of CMMC requirements for contracts or subcontracts exclusively for commercial off-the-shelf (COTS) items. Others questioned applicability of CMMC requirements to COTS procurements and/or purchases at or below the micro-purchase threshold. Finally, one commenter questioned the validity of a COTS exclusion, stating that no COTS components are exempt from DoD's certification requirements from DISA or NSA.

Response: The term Commercially available off-the-shelf (COTS) is defined in FAR part 2.101. Some comments pertained to content of the 48 CFR part 204 CMMC Acquisition rule, including applicability of CMMC clauses to COTS procurements and/or those below the micropurchase threshold. Such comments are not within the scope of this CMMC 32 CFR part 170 CMMC Program rule, which outlines program requirements and not acquisition procedures. CMMC requirements do not apply to contracts and subcontracts that are exclusively for the delivery of COTS products to a DoD buyer. The exemption does not apply to a contractor's use of COTS products within its information systems that process, store, or transmit CUI. CMMC assessments are conducted on contractor owned information systems to ascertain compliance with the designated FAR, DFARS, and NIST requirements.

9. Specific Product Recommendations

Comment: One managed service provider expressed concern that the specific tools they use to provide services might be considered Security Protection Assets or generate Security Protection Data in the context of CMMC assessment requirements, which might result in clients electing to use their own tools and products in lieu of the managed service provider. This commenter attached a list of more than a dozen commercial product and tools they use as examples associated with this concern. One commenter used their public comment submission to submit materials marketing services their company can provide, while another commenter suggested the rule direct readers to a website listing all software, tools, and applications deemed "safe and cost effective" by virtue of CMMC assessment.

Another commenter asserted that all companies need access to cybersecurity solutions from DHS/CISA and grants to assist them in buying Zero Trust technologies to protect CUI. Similarly, some commenters recommended various other cybersecurity tools, programs, or technologies that could be used to meet CMMC security requirement and provide threat intelligence to DIB companies. Such recommendations included portals used in conjunction with perimeter and privileged access management systems. One commenter proposed delaying implementation of the CMMC rule until all DoD contractors' system architectures could be analyzed for possible implementation of Virtual Machines, or Blockchain for secure data transmission, or hosting of all CUI on DoD hosted platforms.

Response: The government cannot comment on specific products or vendors, including marketing materials submitted via public comment. However, companies that act as ESPs should note this rule does not require CMMC assessment or certification of ESPs that do not process, store, or transmit CUI. Services provided by an ESP are in the OSA's assessment scope.

Comments pertaining to solutions available from other Federal agencies or expressing a desire for grants to obtain Zero Trust solutions or other cybersecurity solutions are also beyond the scope of the CMMC rule. A wide range of technologies may be used to implement CMMC requirements. DoD will not comment on specific OSA technology choices. The Department declines the recommendation to review the system architectures of all DoD contractors. The DoD did not modify the rule to identify a repository of "safe and cost effective" software, applications, and tools because a CMMC assessment does not evaluate commercial products or services for those characteristics and the government does not provide product endorsements.

10. Applicability

a. Systems Operated on Behalf of DoD and National Security Systems

Comment: The DoD received questions about whether CMMC requirements apply to information systems that are designated as National Security Systems, Defense Business Systems, or systems operated on the DoD's behalf. In concert with those questions, one person recommended adding NIST SP 800-53 R5 requirements to the rule for such systems. The commenter further recommended expanding applicability of the rule to include contractor-owned systems that directly affect DoD NSS. Two commenters recommend edits to clarify that CMMC requirements do not apply to NSS or to government systems operated by contractors on the DoD's behalf.

One commenter asked if a Cloud Service Provider that stores CUI would have to be at Impact Level 4 in accordance with the DISA Cloud Computing Security Requirements Guide.

Response: The CMMC assessment requirements apply in conjunction with FAR clause 52.204-21 and DFARS clause 252.204-7012 requirements and provide a mechanism for verifying compliance with the security requirements for safeguarding FCI or CUI (e.g., NIST SP 800-171) levied by those clauses.

The CMMC Program does not alter any additional security requirements that may be applicable to contractor-owned information systems that may also meet the criteria for designation as NSS.

There is no conflict between the CMMC rule and the DISA Cloud SRG, which applies to contractor information systems that are part of Information Technology (IT) services or systems operated on behalf of the Government. The CMMC rule does not apply to those systems (§ 170.3(b)). The DoD declines to modify the rule because the applicability section already states this rule applies to contractor-owned information systems.

b. Infrastructure Entities

Comment: Many commenters had concerns about CMMC's potential impact to the energy and electric industries, Internet Service Providers (ISPs) and small, disadvantaged businesses looking to contract with the DoD, especially given dependencies on appropriate marking of Controlled Unclassified Information (CUI).

Another commenter referenced Executive Order 13175, "Consultation and Coordination with Indian Tribal Governments" and requested information on CMMC impact to and potential exemptions for Native American and small disadvantaged contractors. Another commenter stated that some small businesses may stop providing cost estimating services to Federal agencies due to "threatened penalties" under CMMC requirements.

One commenter recommended adding the definition of the defense industrial base (DIB), and referenced the Cybersecurity and Infrastructure Security Agency definition, which explicitly excludes commercial infrastructure providers from their definition of the Defense Industrial Base Sector. One commenter stated the lack of clarity around requirements for electric cooperatives under the CMMC framework is causing concern about unanticipated cost impacts for these smaller entities. The commenter requested that DoD provide contractors the ability to recover unanticipated costs incurred to achieve CMMC certification.

Another commenter asked about potential CMMC exemptions for telecommunications providers, specifically for end user encryption. The commenter stated the DoD needs to impose CUI encryption requirements on the relevant contractors and not telecommunications network providers, who have no control over whether a user encrypts information it sends over those networks. The commenter also noted that definitions of "common carrier" vary across Federal Government and suggested the DoD should create a blanket exemption for contracts involving commercial communications networks that are not "purpose-built" to transmit sensitive government data. Another commenter suggested the CMMC Rule should further clarify that encryption must be configured such that the common carrier does not have access to the decryption key(s).

Several commenters requested clarity around CUI, citing general confusion among industry about which CUI is subject to the CMMC Program. Some commenters interpreted the rule as proposing to apply to all CUI information, rather than just information handled by the contractor

"in support of a defense contract" and asserted that this would be an expansion beyond the current DFARS clause 252.204-7012 requirements. They further suggested this broad definition could result in companies applying costly controls to all apparent CUI, regardless of its association with DoD, to avoid penalties under the False Claims Act. They recommended clearly stating that CUI provided to contractors by non-DoD agencies should be subject to the requirements of those agencies and not the CMMC Program.

A commenter said the electric industry will experience increased costs as electric utilities comb through vast amounts of data across the electric grid to determine all potential CUI, even if that CUI is not specifically subject to a DoD contract. One commenter stated that guidance DoD has provided for electric utilities to identify CUI in the past is insufficient and suggested that use of Security Classifications Guides could help by minimizing the need for CMMC compliance. In addition, they speculated that inclusion of CMMC requirements could create requirements after award which might require adjustments to contract price. Another commenter stated energy companies servicing military customers must develop governance programs around data protection years in advance, with significant investments. The commenter is concerned that CMMC requires these companies to make these large investments prior to knowing if a proposed contract may contain CUI and without adequate guidance about what data is considered CUI.

Response: This rule has no disproportionate impact on Native American-owned businesses. Once identified as a requirement, the CMMC Level will apply uniformly to all prospective competitors. DoD must enforce safeguarding requirements uniformly across the Defense Industrial Base for all contractors and subcontractors who process, store, or transmit CUI. The value of information (and impact of its loss) does not diminish when the information moves to DoD contractors and DoD subcontractors, regardless of their status as Native American or small disadvantaged businesses.

The CMMC Program rule does not include "threatened penalties." If a requirement of a DoD contract is not met, then standard contractual and other remedies applicable to that contract may apply.

CMMC Program requirements make no change to existing policies for information security requirements implemented by DoD. Policies for CUI and creation of program documentation, to include Security Classification Guides, are separate from this rule.

Section 170.4(b) of the rule states Defense Industrial Base (DIB) is defined in 32 CFR part 236, which addresses DoD and DIB Cyber Security Activities. Section 236.2 includes the DoD approved definition for DIB.

The CMMC Program applies only to DoD contracts that include the DFARS clause 252.2047021 and under which FCI or CUI is processed, stored, or transmitted on contractor information systems.

This includes CUI outside the category of the Defense Organizational Index Group. Contracts for the provision of electricity or other utilities which do not contain FAR clause 52.204-21 or DFARS clause 252.204-7012 and which do not require the processing, storing, or transmitting of FCI or CUI on contractor owned information systems will not require CMMC assessment. The CMMC rule makes no change to FAR cost allowability or cost accounting standards. The 32 CFR part 170 CMMC Program rule has been updated to add "in performance of the DoD contract" to § 170.3, and the 48 CFR part 204 CMMC Acquisition rule will provide the contractual direction.

A common carrier's information system is not within the contractor's CMMC Assessment Scope if CUI is properly encrypted during transport across the common carrier's information system. A common carrier who is a DoD contractor or subcontractor is responsible for complying with the CMMC requirements in their contracts. CUI encryption requirements already apply to the OSA, not the telecommunications network provider. The lack of adequate encryption on the part of the OSA would not trigger application of CMMC requirements to the common carrier's network. The term "common carrier" appears in the comment section to a previous rule making process. Its definition and use are taken from CNSSI 4009. Efforts to define it or related terms by other agencies are outside the scope of the CMMC Program.

Commenter scenarios where a common carrier would be privy to an OSA's encryption keys are unrealistic. DoD declines to provide additional guidance.

CMMC Program requirements make no change to existing policies for information security requirements implemented by DoD. Policies for CUI and creation of program documentation, to include Security Classification Guides, are separate from this rule. Relevant policies include DoDI 5200.48 "Controlled Unclassified Information" and DoD Manual 5200.45 "Instructions for Developing Security Classification Guides". CMMC Program requirements will be identified as solicitation requirements. Contractors will be required to meet the stated CMMC requirements, when applicable, at or above the level identified. For this reason, it is up to each DIB organization to determine which CMMC level they should attain.

Questions regarding specific contractual matters are outside of the scope of this rule and may be addressed by the 48 CFR part 204 CMMC Acquisition rule. The CMMC program will be implemented as a pre-award requirement.

c. Joint Ventures

Comment: Two commenters requested clarification as to whether CMMC requirements will apply to companies engaged in Joint Ventures.

Response: CMMC program requirements are applicable when DoD requires processing, storing, or transmitting of either FCI or CUI in the performance of a contract between DoD and the respective contractor. CMMC Program requirements will apply to information systems associated with 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. The identity of an offeror or contractor as a joint venture does not in and of itself define the scope of the network to be assessed.

d. Fundamental Research Efforts

Comment: One commenter recommended that both the sharing of CUI and the decision to apply a CMMC compliance assessment should only be considered for contracts of sufficient contract value and performance period to make the expense of safeguarding CUI worthwhile. This commenter asserted that small businesses are selected for SBIR contract award not based on ability to protect information, but instead on the unique product or service they offer.

Some commenters expressed concern that CMMC could result in state-funded universities incurring costs to comply with CMMC level 2, while even the costs for implementing required FCI safeguarding requirements is a significant financial burden. These commenters speculated that applying FCI or CUI markings to fundamental research information negatively impact academic institutions by requiring them to remove such data from the public domain. This commenter cited DFARS clause 252.204-7000 as rationale to modify the CMMC rule to exclude fundamental research.

One commenter requested that when contracting for fundamental research, the Government include a CMMC requirement based only on whether information shared is currently FCI or CUI, and not whether the effort might lead to development of FCI or CUI. Another commenter requested that DoD issue policies clearly describing how to recognize or identify circumstances that could result in fundamental research becoming FCI or CUI such that it would require being processed, stored, or transmitted on CMMC compliant information systems. The commenter expressed concern that absent such policies, research institutions may house all DoD-related project activities in CUI enclaves “out of an abundance of caution”, thereby unnecessarily expanding CUI applicability at significant cost. They asked that DoD Instruction 5200.48, “Controlled Unclassified Information,” and a related DoD policy memorandum “Clarifying Guidance for Marking and Handling Controlled Technical Information in accordance with Department of Defense Instruction 5200.48, ‘Controlled Unclassified Information” be incorporated into the rule by reference.

One commenter questioned whether and how CMMC requirements may apply to noncontract efforts, including grants, or efforts conducted under Other Transactional Authorities.

Response: One of the main purposes of the CMMC Program is to ensure that DoD contracts that require contractors to safeguard CUI will be awarded to contractors with the ability to protect that information. All contractor-owned information systems that process, store, or transmit CUI are subject to the requirements of NIST SP 800-171 when DFARS clause 252.2047012 is included in the contract. This is the case whether or not the contractor is engaged in fundamental research.

To the extent that universities are solely engaged in fundamental research that only includes information intended for public release and does not include FCI or CUI, no CMMC requirement is likely to apply. When a research institution does process, store, or transmit FCI, the information should be adequately safeguarded in accordance with the FAR clause 52.204-21, if applied. When a research institution does process, store, or transmit CUI, the information should be adequately safeguarded in accordance with the DFARS clause 252.204-7012, if applied. That clause makes the contractor owned information system subject to NIST SP 800-171, which includes requirements for Awareness and Training (AT) and Physical Protection (PE). The CMMC Program provides a means to verify compliance.

DoD's CUI program policies already address responsibilities for identifying and marking information, including procedures for changing markings. The DoD declined to incorporate all the references associated with marking and handling CUI. The DoD instructions and policy guidance are authoritative and incorporating them into the CMMC regulation is beyond the scope of this rule. DoD declines to update the preamble to exclude the possibility that information may be designated CUI over the course of time. According to A&S memo dated 31 March 2021, titled Clarifying Guidance for Marking and Handling Controlled Technical Information in accordance with Department of Defense Instruction 5200.48, "Controlled Unclassified Information," "Information related to RDT&E-funded research efforts, other than fundamental research, do not always qualify as CUI." This implies that some DoD fundamental research may qualify as CUI. When the DoD does determine that research meets the definition of CUI, safeguarding requirements of DFARS clause 252.204-7012 will apply regardless of whether the contractor's work is fundamental research. In such instances, CMMC assessment requirements may also be applied. Contractors should work closely with Government Program Managers to ensure a proper understanding of the data being developed and the appropriate markings and safeguarding.

Questions regarding the application of CMMC requirements to specific transactions, including grants and OTAs, are outside of the scope of this 32 CFR part 170 CMMC Program rule.

e. DoD Waiver of CMMC Applicability

Comment: Several questions were submitted about waiver procedures for CMMC requirements. For example, someone asked which DoD person or office has authority to approve waiver requests. Others also requested insight to the specific criteria for waiver approval. One commenter submitted preferred rewording of the rule section that describes waivers while another suggested self-assessment should be required even when certification is waived.

Response: DoD internal policies, procedures, and approval requirements will govern the process for DoD to waive inclusion of the CMMC requirement in the solicitation. Once applicable to a solicitation, there is no process for OSAs to seek waivers of CMMC requirements from the DoD CIO. In accordance with § 170.5(d), a limited waiver authority is provided to the Acquisition Executive with acquisition oversight for the program in question. These officials may issue supplemental guidance dictating specific coordination requirements for waiver requests. Recommended administrative changes have been incorporated into § 170.5(d) to add clarity.

11. Determination of Applicable Assessment Type

a. Process for Level Determination

Comment: Multiple comments asked how DoD will determine the CMMC level to include in solicitations. Multiple comments inquired about the criteria DoD will use to determine when to require a CMMC Level 2 self-assessment, CMMC Level 2 certification, or CMMC Level 3

certification assessment. Multiple comments asked specifically about when CMMC Level 2 selfassessment will be required versus CMMC Level 2 Certification. One comment requested more information on which companies may "self-attest".

One comment requested § 170.5(a) be modified to prevent CMMC level 2 or 3 being assigned for contracts where only FCI is exchanged. One comment emphasized that requirement(s) for Contractor certification levels must be the same as stated throughout this proposed ruling. Two comments recommended providing contracting officers with interim guidance to ensure consistency in applying CMMC requirements. One comment requested the detailed guidance ensure CMMC requirements are selected based on risk, and that certification is not required by default.

Some commenters objected to the wording of one criterion for level selection as "potential for and impacts from exploitation of information security deficiencies". One asserted this equates to a sub-CONFIDENTIAL security classification. One comment expressed that all information systems that process CUI should have the same level of "program criticality, information sensitivity, and the severity of cyber threat" since CUI is Unclassified Information which is a "handling caveat".

Multiple comments requested a clearer description of what contracts require CMMC Level 3 Certification, one of which requested a definition of what constitutes a "priority program" that might require CMMC Level 3. One comment requested that acquisition processes first analyze the CUI for a proposed effort using published factors for aligning CUI to high value assets before setting CMMC levels. They asserted use of such published factors would improve accuracy of CUI marking.

Response: Pre-award contracting procedures and processes for CMMC assessment requirements will be addressed in the 48 CFR part 204 CMMC Acquisition rule. CMMC is a pre-award requirement. As stated in the Applicability section summary of the CMMC rule (§ 170.3), once CMMC is implemented in the 48 CFR part 204 CMMC Acquisition rule, DoD will specify the required CMMC Level in the solicitation and the resulting contract.

DoD's policies and procedures for the length of time allowed for proposal submission in response to any solicitation are beyond the scope of this rule. PMs typically consider the totality of the requirement when deciding how much time to allow for proposal submission or whether to seek industry input through Request for Information to inform solicitation details. Note that once attained, companies may reference a CMMC Status as part of any number of proposals to various solicitations with that level of CMMC requirement if the same assessment scope is used.

The type and sensitivity of information to be utilized during the contract, FCI or CUI, determines the requirements in the solicitation, which then informs the CMMC level required. CMMC level 1 requirements are designed to be applied when FAR clause 52.204-21 security requirements apply to the contract, whereas CMMC level 2 and 3 requirements are designed for the protection of CUI information, and to be applied when DFARS clause 252.204-7012 also applies.

When CMMC Program requirements are effective, the DoD will begin including CMMC assessment requirements in solicitations as described in § 170.3 Applicability. DoD solicitations will specify which requirements will apply to the contract award. Prior to issuance of a solicitation, DoD will determine the appropriate CMMC level and type of assessment needed to ensure adequate safeguarding of the DoD program information to be shared in performance of the contract. Identification of the CMMC level and assessment type will be part of the DoD's requirement definition process. As addressed in § 170.18(a) of this rule, a CMMC Level 2 Final CMMC Status is a prerequisite for CMMC Level 3 assessment and must be achieved for information systems within the Level 3 Assessment Scope.

Identification of priority programs is a function of the requirements definition process for any DoD effort. The DoD will issue policy guidance to Program Managers to clarify which programmatic indicators should be considered for selecting the most appropriate information safeguarding requirement and associated CMMC assessment requirement for any given

solicitation. Once identified as a requirement, the CMMC Status required will apply uniformly to all prospective competitors.

b. Who Determines the CMMC Level

Comment: Two comments asked who, within the Department, determines the CMMC level required for a contract. One comment suggested that DoD should require senior-level approval to include CMMC Level 3 Certification requirements in solicitations to limit unnecessary application. One comment inquired about when and how CMMC levels change during the program office's Agile Acquisition Framework lifecycle.

Response: Based on DoD decision criteria that include the type and sensitivity of program information to be shared, Program Managers will identify and coordinate as appropriate the CMMC requirement in the solicitation. Internal policies for implementation of CMMC requirements by DoD's acquisition community have been developed, and work will continue as needed to integrate CMMC policies into relevant acquisition policies, guidebooks, and training materials. The DoD intends that requiring activities will determine when compliance should be assessed through CMMC Level 3 as part of the ordinary acquisition planning and requirements generation process.

The CMMC assessment level required does not change based on acquisition lifecycle phase, but based on whether FCI and CUI are processed, stored, or transmitted on contractor owned information systems. All contractor-owned information systems that process, store, or transmit CUI are subject to the requirements of NIST SP 800-171 when DFARS clause 252.204-7012 is included in the contract.

c. CMMC Level 3 Determination

Comment: Multiple comments requested further clarification about which types or categories of CUI require enhanced protection against Advanced Persistent Threats (APTs) at CMMC Level 3 and whether the CMMC level would be based on the Program or the data. Two comments expressed concern or asked how DoD Components will avoid assigning CMMC Level 3 requirements to too many contracts. One comment recommended that DoD modify its criteria for CMMC Level 3 to consider factors such as Acquisition Program Category.

Response: CMMC levels do not correspond to CUI levels as the CMMC Program requirements make changes to neither the CUI Program, categories of CUI, nor existing DoD policies for information security requirements. The CMMC Flow down requirement is defined in § 170.23.

The Requiring Activity knows the type and sensitivity of information that will be shared with or developed by the awarded contractor and selects the CMMC Level required to protect the information according to DoD guidance.

The DoD declines to modify CMMC Level 3 selection criteria as described in the commenters recommended alternatives, which have no bearing on DoD's need for increased confidence in a contractor's ability to safeguard certain CUI against Advanced Persistent Threats. The value of information, and impact of its loss, does not diminish based on the total number or dollar value of contracts held by the awardee, or acquisition program category. The DoD reserves the right to decide when compliance should be assessed by the Government through CMMC Level 3 certification. The DoD defines the work requirements to be solicited for any given program contract.

d. Environments Processing Both FCI and CUI

Comment: Two commentors recommended the elimination of separate assessments when the FCI and CUI environments are the same. One of these comments requested clarification regarding the scenario of an OSC having one assessment scope environment for both FCI and CUI that meets Level 2 requirements.

Response: CMMC Level 2 is required when CUI will be processed, stored, or transmitted on contractor information systems. Successful completion of a CMMC Level 2 self-assessment or CMMC Level 2 certification assessment will suffice to meet the CMMC Level 1 requirement for FCI if/when the scope is identical. The CMMC Level 2 Scoping Guide reflects this language.

e. Recommendations and Scenarios

Comment: One comment recommended removing CMMC Level 2 self-assessment, changing the CUI Program, or creating a new type of CUI to distinguish between CMMC Level 2 self-assessment and CMMC Level 2 Certification. Another comment noted that the requirements for CMMC Level 2 certification assessment are almost identical to requirements for CMMC Level 2 self-assessment. One comment expressed concern that DoD's designation of CMMC Level 2 self-assessment and certification assessment runs contrary to FCI (FAR requirements) and the CUI Program. One comment asked if the designation of information as FCI or CUI changes the scope of CMMC.

One comment asked for clarification on which contracts will have sensitive unclassified DoD information but will not require CMMC assessment. One comment recommended removing the option for CMMC Level 2 self-assessments to reduce complexity. One comment posed multiple questions about what DoD will do if contracting officers assign CMMC Level 2 or CMMC Level 3 Certification requirements at a rate substantially higher than projected.

Response: The DoD CIO looked at CUI from a risk-based perspective and determined that different approaches to assessments could be implemented to address risk and help lower the burden for the DIB. The security requirements for a CMMC Level 2 self-assessment and a CMMC Level 2 certification assessment are the same, the only difference in these assessments is whether it is performed by the OSA or by an independent C3PAO.

The decision to rely upon self-assessment in lieu of certification assessment is a Government risk-based decision based upon the nature of the effort to be performed and CUI to be shared. The size of the company with access to the CUI is not a basis for this determination. The value of information (and impact of its loss) does not diminish when the information moves to contractors of smaller size. The DoD declines to modify the rule to include its internal decision process.

To select a CMMC Level for a procurement, Program Managers and requiring activities will identify the applicable CMMC Level using the factors included in § 170.5(b)(1) through (5). The DoD did agree with one comment to rephrase § 170.5(b)(4) to delete a reference to the "potential for" impact from exploitation of information security deficiencies, which likely cannot be effectively determined. The DoD does not agree that the wording equates to a subCONFIDENTIAL classification and declines to delete that criterion. § 170.5(b)(3) is appropriately worded in that it states Program Managers will consider the listed criteria in selecting a CMMC requirement level. It does not have the effect of "transforming FCI into CUI". The DoD reserves the right to define the criteria for selection of the CMMC assessment requirement, just as it defines all other requirements for inclusion in a solicitation.

The Department remains committed to implementing the CMMC program to require compliance assessment against applicable security requirements in all DoD contracts involving FCI or CUI. Some such contracts will require only a CMMC self-assessment, while others will require a certification assessment. The commenter misinterprets that some contracts that do require processing of FCI or CUI will not require CMMC assessment of either kind, without approval of a waiver.

The DoD declines to remove self-assessments from the rule. Self-assessments allow the acquiring organization to balance the cost and complexity of assessment with the risk to the information being shared with the OSA.

Supporting guidance for CMMC implementation will be updated, as necessary. DoD has options to mitigate implementation issues such as waivers and other contractual remedies. DoD's estimate for the number of contractor's requiring CMMC Level 1 and cost estimates represent derived estimates based on internal expertise and public feedback in accordance with OMB Circular A-4.

12. Flow-Down / Applicability to Sub Contractors

a. Applicability and Compliance

Comment: Several comments requested clarification about the applicability of CMMC requirements to subcontractors and how to correctly flow down requirements. Some asked

whether prime contractors would have flexibility to flow down a lower CMMC level than required for the prime contract. Three comments expressed confusion about the type of Level 2 assessment required for subcontractors when supporting a prime that is required to meet CMMC Level 3 requirements. Two asked about the impact to flow-down when contractors hold multiple contracts. A couple comments requested clarity on how to determine the correct CMMC level to flow down.

Some comments asked what factors would result in flow-down of a particular CMMC requirement level, or whether affirmations submitted by primes would require knowledge of subcontractor compliance status.

Other comments asked what tools would be available to assist contractors in checking subcontractor compliance with CMMC requirements or suggested that SPRS should be made available for this purpose. One suggested that without this transparency, CMMC compliance would become a meaningless effort to "check the box" without actual steps to secure their systems. Another simply asked if they would have their own SPRS and eMASS access, or access through their prime. Some asked what action meets the rule's requirement to "require subcontractor compliance", i.e., does simply including the CMMC clause in subcontracts meet that requirement.

One comment objected to the definition of subcontractor used in the rule, which they stated was overly broad and would result in application of CMMC requirements to too many businesses. Some comments suggested the flow-down requirement apply only to one sub-tier, while another requested advance notice of solicitations that plan to include CMMC requirements. One comment suggested that CUI be treated more like classified information, meaning to limit sharing of CUI with subcontractors. Some comments asked whether prime contractors are responsible for verifying subcontractor compliance with DFARS clause 252.204-7012, as C3PAOs do during an assessment. Two comments recommended rephrasing the flow-down section, with one specifically asking to clarify it is required only when FCI or CUI will be processed, stored, or transmitted in the performance of any particular prime contract. Another suggested edits for clarity or for consistency with DFARS clause 252.204-7012.

Response: It is up to each OSA to protect FCI and CUI and to determine the assessment boundary, policies, and procedures necessary to do that. Section 170.23 specifically addresses the CMMC requirements that apply to subcontractors that will process, store, or transmit FCI or CUI. Section 170.23 addresses flow down of CMMC requirements from the prime contractor to the subcontractors in the supply chain. Prime contractors are responsible for complying with contract terms and conditions, including the requirement to flow down applicable CMMC requirements to subcontractors. The DoD modified § 170.23(a)(3) to clarify that when a subcontractor will process, store, or transmit CUI in performance of the subcontract and the Prime contractor has, for the associated prime contract, a requirement of Level 2 certification assessment, then CMMC Level 2 certification assessment is the minimum requirement for the subcontractor. Requirements for External Service Providers are defined in § 170.4; not all companies that provide services to an OSA are considered ESPs.

As in other contexts, the Government may specify additional guidance in the solicitation. CMMC assessments will be identified as pre-award requirements. Subcontractors at each tier are responsible for submitting their own assessment and affirmation information in SPRS. CMMC self-assessments and certifications will be reflected in SPRS, including an indicator of the currency of the credentials. Contracting Officers and Program Managers need not review any assessment artifacts, only the resulting scores and certificate validity period.

Work arrangements between the prime and subcontractor are beyond the scope of this rule, however, if CUI is flowed down and will be processed, stored, or transmitted on subcontractor information systems in the performance of a DoD contract then CMMC requirements also flow down as described in § 170.23. The DoD will not track progress toward certification but will implement CMMC as a pre-award requirement. An OSA's pursuit of a C3PAO assessment is a business decision to be made by each contractor considering the contract opportunities it wishes to pursue.

The DoD disagrees with one commenter's assertion that CMMC requirement will flow down "regardless of what work they do", because it does not acknowledge the point that flow-down requirements are for subcontractors who process, store, or transmit CUI. The text of § 170.23, clearly conditions the flow-down to those cases when a subcontractor will process, store, or transmit FCI or CUI. The prime contractor's responsibility is to flow down CMMC assessment requirements as described in § 170.23 and to ensure that FCI and CUI are not further disseminated to subcontractors that do not meet the CMMC requirement indicated in § 170.23. Likewise, subcontractors must also flow down CMMC requirements and ensure that FCI and CUI are not further disseminated to subcontractors that do not meet the CMMC requirement indicated in § 170.23. Section 170.23 has been revised to make this clearer. DoD declines to accept the recommendation to treat CUI like classified data. Classified information is managed differently from CUI, and different safeguarding regulations apply to these different categories of information (each of which are defined in 32 CFR part 2002).

This rule makes no change to CUI policies for marking of data, and CMMC levels are not CUI categories in the DoD CUI registry. Primes and their subcontractors must understand flowdown requirements based on § 170.23, which clearly identifies requirements that apply when subcontractors will process, store, or transmit CUI in performance of the subcontract and the Prime contractor has a requirement of Level 3 certification assessment (i.e., CMMC Level 2 certification assessment is the minimum requirement for the subcontractor). In addition, the rule has been revised to make clear that the requirement applies in the performance of a subcontract when the relevant prime contract has a CMMC requirement. The rationale for the minimum level 2 certification flow-down requirement is that the DoD made a risk-based decision not to mandate flow down of the level 3 requirement unless explicit guidance is provided to do so. As stated in § 170.23(a)(3), when a Prime contractor has a requirement of Level 2 certification, any CUI that is flowed down for a subcontractor to process, store, or transmit in performance of the subcontract will also carry a minimum requirement of Level 2 certification assessment. CMMC Program requirements will be identified as solicitation and contract requirements, and contractors will be required to meet the stated CMMC requirements, when applicable, at or above the level identified. One commenter misinterpreted a response to a prior public comment. The quoted content says that contractors and subcontractors each must verify (through CMMC assessment) that all applicable security requirements of NIST SP 800-171 required via DFARS clause 252.204-7012 have been implemented. Contractors are not required to assess subcontractor implementation of the requirements of NIST SP 800-171. The prime contractor's responsibility is to flow down CMMC assessment requirements as described in § 170.23 and also to refrain from disseminating FCI or CUI to subcontractors that have not indicated meeting the CMMC level described in that section for the type of information to be shared. Likewise, subcontractors must also flow down CMMC requirements or refrain from disseminating FCI or CUI. The DoD does not provide SPRS access or other tools for contractors to identify the CMMC status or other companies. The DoD expects that defense contractors will share information about CMMC status with other DIB members to facilitate effective teaming arrangements when bidding for DoD contracts.

Prime contractors will not be granted access to subcontractor's information in SPRS. However, prime contractors should communicate early and often with prospective subcontractors to confirm current CMMC status, including whether the level matches that required. This interaction does not involve the government and is beyond the scope of this rule.

This rule follows the format and includes all sections required in OMB guidelines for formal rulemaking. The DoD lacks authority to modify the template or omit required sections, which results in some repetition.

DIB contractors are responsible for submitting their Level 1 and Level 2 self-assessments and will access SPRS to enter the results. DIB contractors do not have access to CMMC eMASS, as that system is used to support certification assessments only.

CMMC Program requirements are designed to require completion of an assessment and an annual affirmation. The purpose of the annual affirmation addressed in § 170.22 is to validate to

the DoD that the contractor is actively maintaining its CMMC level status, which is more than a checkbox exercise.

One commenter misinterpreted the quoted definition of subcontractor, which makes clear that term includes only those entities providing supplies, materials, equipment, or services under a subcontract in connection with the prime contract. DFARS clause 252.204-7012 and FAR clause 52.204-21 also flow-down the requirement to safeguard information. CMMC program requirements will be flowed down similarly, therefore there is no anticipated expansion of scope. The cost estimates included in the published rule include costs for both existing DIB members and new entrants (or newly covered entities).

The DoD modified the Overview summary of CMMC 2.0 to read "The DFARS clause 252.204-7012 also requires defense contractors to include this clause in all subcontracts that will require the subcontractor to process, store, or transmit CUI." The DoD declined additional edits in this location that requested reframing the criteria Program Managers will use select CMMC requirements to address Levels 2 and 3 only. The DoD may apply CMMC Level 2 or 3 requirements when there is anticipation of the need for the contactor or subcontractors to process, store, or transmit CUI during the performance of a contract.

b. Prime and Subcontractor Relationships

Comment: Many requested specific examples of when a prime contractor should flow down its CMMC requirements to a subcontractor or ESP, and how to determine the appropriate CMMC level to flow down. For example, one comment asked whether the subcontract document would require safeguarding, necessitating flow-down of the CMMC requirement. Some comments expressed concern that flow-down requirements are not sufficiently clear to prevent prime contractors from unnecessarily sharing CUI and applying CMMC requirements to lower tier suppliers. Another thought that the flow-down requirements will drastically expand the scope of the program and drive cost increases for the DIB.

Several comments suggested strategies for minimizing the burden of security implementation on lower tier subcontractors, such as requiring prime contractors to provide access to CUI on prime contractor systems, or prohibiting prime contractors from unnecessarily sharing CUI information that would necessitate a CMMC requirement. One asked whether the prime contractor has a responsibility to check which CMMC level the subcontractor has flowed down to the next tier. One comment referenced industry activities aimed at gauging subcontractor preparedness for CMMC and expressed concern with anecdotal evidence that primes will not issue orders until the subcontractor has submitted CMMC scores into SPRS.

Response: One commentor correctly interpreted § 170.23(a)(3) as meaning that CMMC level 2 Certification requirements (not self-assessments) flow down for subcontractors that will handle CUI when the Prime contract specifies a CMMC Level 2 Certification requirement.

At the time of award, the DoD may have no visibility into whether the awardee will choose to further disseminate DoD's CUI, but DFARS clause 252.204-7012 and DFARS clause 252.204-7021 require that the prime contractor flow down the information security requirement to any subcontractor with which the CUI will be shared. Decisions regarding the DoD information that must be shared to support completion of subcontractor tasks, will take place between the prime contractor and the subcontractors chosen to complete the specific tasks. The DoD encourages prime contractors to work with its subcontractors to flow down CUI with the required security and the least burden. The DoD declines to revise the rule to address responsibilities for derivative marking of CUI because this rule makes no change to DFARS clause 252.204-7012 or DoD's CUI policies regarding marking of CUI, including creation of information.

The specific contractual language is part of the 48 CFR part 204 CMMC Acquisition rule and beyond the scope of this 32 CFR part 170 CMMC Program rule. This rule describes DoD's intent for CMMC Program requirements, which include that all prime and subcontractors at all tiers that process, store, or transmit CUI in the performance of a DoD contract (or sub-contract) are required to demonstrate compliance with the contract requirements (i.e., FAR clause 52.20421 or DFARS clause 252.204-7012) for adequately safeguarding FCI or CUI.

CMMC flow-down requirements are designed to apply consistent assessment requirements to all subcontractors, regardless of company size, who are required to adequately safeguard CUI. The DoD cannot dictate DIB business practices and encourages prime contractors to carefully consider the necessity of sharing CUI information and work with subcontractors to flow down CUI only when deemed appropriate.

Likewise, the criteria by which contractors select CSPs for support or the availability of GFE for any particular contract are beyond the scope of this rule. The DoD declines to limit CMMC program requirements to the first-tier subcontractor, as suggested by the commenter. When a contractor or subcontractor responds to multiple solicitations, that contractor should complete the highest assessment level among them for the assessment scope defined for use in performance of the contracts. The contractor may also elect to structure its environment to meet differing CMMC requirements based on the contract(s) in question.

Contractual remedies for non-compliance are a 48 CFR part 204 CMMC Acquisition rule matter and beyond the scope of this rule.

c. Requirements

Comment: Some comments objected to CMMC Level 2 certification assessment being identified as the minimum flow-down from prime contractors with a CMMC Level 3 requirement. They asked how the more sensitive data associated with a Level 3 requirement would be tracked. Three asked whether CMMC Level 2 certification assessment must be flowed down as the CMMC requirement when the prime contract requires a higher level, and the subcontract is for limited scope. One comment complained that the rule does not actively encourage primes to flow down Level 2 self-assessment requirements instead of certification requirements.

One comment suggested the Department is impermissibly attempting to make sensitivity determinations of other agencies' CUI and FCI through the implementation of this rule.

Another comment requested affirmation that contractors remain responsible for determining whether information that they create (derived from CUI) retains its CUI identity when sharing that information with lower tier suppliers, and for determining any associated CMMC flow-down requirement.

Response: DoD will issue guidance to Program Managers to reiterate the most appropriate information safeguarding requirements for DoD information and the associated CMMC assessment requirement for any given solicitation. CMMC program requirements will be identified in the solicitation, and contractors will be required to meet the stated CMMC requirements, when applicable, at or above the level identified by the time of contract award. CMMC requirements flow down from primes to subcontractors, as described in section § 170.23.

The DoD declined to provide forecasts of upcoming DoD solicitations with CMMC assessment requirements. Given that FAR clause 52.204-21 was effective in 2016 and DFARS clause 252.204-7012 was effective in 2017, OSAs have had over seven years to implement NIST SP 800-171 R2 requirements and close out POA&Ms. DoD contracts that require OSAs to process, store, or transmit CUI and include DFARS clause 252.204-7020, also require a minimum of a self-assessment against NIST SP 800-171 requirements. That self-assessment includes the same requirements as the CMMC Level 1 and CMMC Level 2 self-assessments.

DoD must enforce CMMC requirements uniformly for all defense contractors and subcontractors, regardless of size, who process, store, or transmit FCI, and CUI, regardless of size. The value of DoD information (and impact of its loss) does not diminish when the information moves to contractors and subcontractors. The DoD cannot dictate business practices but encourages prime contractors to work with its subcontractors to limit the flow down of FCI and CUI. The DoD declines to base CUI safeguarding requirements on contract ceiling value.

This DoD 32 CFR part 170 CMMC Program rule does not impact or supersede 32 CFR part 2002 (the CUI Program) or make exceptions for the categories of CUI or the Designating Agency for the CUI. CMMC requirements apply to DoD contracts that will involve processing, storing, or transmitting of FCI or CUI on any non-Federal information system.

13. The CMMC Ecosystem Roles, Responsibilities and Requirements:

a. Government

Comment: Some comments asked how the Department plans to address complaints and concerns from ecosystem stakeholders and the process by which disputes between OSCs and C3PAOs or the CMMC AB are resolved. Two comments wanted the CMMC PMO to document a process for ecosystem stakeholders to register complaints or use of Service Level Agreements to hold the Department accountable to respond.

Some asked whether the DoD could be subject to litigation challenging DoD's reliance on the CMMC AB's appeals process to resolve disputes between OSCs and C3PAOs. The commenters asserted resolving such disputes may be an inherently governmental function. One commenter noted that transactions between OSCs and C3PAOs for initiating an assessment are beyond the DoD's authority to regulate, since the DoD is not a party to the transaction. They perceived DoD's indirect oversight of C3PAOs through the CMMC AB as creating conflicts of interest and potential legal liabilities. One commenter requested the DoD modify the rule to state the CMMC PMO is responsible for the assessment and monitoring of the CMMC AB, as well as the CMMC AB's performance of its roles.

One commenter noted the ISO/IEC 17011:2017(E) requirements that the CMMC AB must meet and asked why the rule identifies a timeline for compliance instead of requiring immediate accreditation.

One commenter referenced a CMMC-related Request for Information issued prior to CMMC program development to gauge industry's capability to provide the necessary ecosystem accreditation and management functions. They asserted no response was provided to their RFI response.

One comment suggested the CMMC PMO should develop a process to act as the authoritative source for assessment interpretations to ensure consistency. One person asked which DoD office authored the rule. Another noted the realignment of the CMMC PMO from OUSD(A&S) to DoD CIO and asked whether this indicated a lack of OUSD(A&S) involvement in the program. One commenter noted that DoD Program Managers and requiring activities have a role in the CMMC Program and suggested that their responsibilities for marking and managing CUI be added to the rule.

One commenter wanted to require DIBCAC assessors to complete CCP and CCA training and certification exams through a CAICO approved licensed training provider.

Response: DoD agreed with the commenter that the government does not have authority over transactions between the OSC and C3PAO. The roles and responsibilities of the government are set forth in § 170.6. The interaction between the CMMC Accreditation Body and C3PAOs is governed by the requirements of this rule in §§ 170.8 and 170.9, including Conflict of Interest, Code of Professional Conduct, and Ethics policies, as well as ISO/IEC standards.

All DCMA DIBCAC assessors comply with DoD regulations regarding the cybersecurity workforce, to include DoD Directives 8140 and 8570 and other internal training standards. DCMA DIBCAC assessors' credentials for CMMC Levels 2 and 3 exceed the training that CCPs and CCAs complete through Approved Training Providers and include industry certification and a security clearance. Additionally, DCMA DIBCAC assessors must take the CMMC certification examinations.

DoD's contract with the CMMC AB assigned places responsibility for Level 2 assessment interpretation to the CMMC Accreditation Body. The CMMC Accreditation Body publishes assessment procedures and guidance for C3PAO's conducting CMMC Level 2 Certification Assessments. The CMMC AB is required to provide the CMMC PMO with all plans or changes related to its own activities and activities within the CMMC Ecosystem for review prior to implementation and publication. The DCMA DIBCAC is responsible for CMMC Level 3 assessment interpretation and will use the same process that is used for DIBCAC High Assessments.

Management oversight of the CMMC Program was realigned from the OUSD(A&S) to the Office of the DoD CIO for better integration with the Department's other DIB cybersecurity

related initiatives. Comments pertaining to DoD's organizational structure are not relevant to the content of this rule. The DoD CIO is responsible for all matters relating to the DoD information enterprise, including network policy and standards and cybersecurity. In this capacity, the DoD CIO prescribes IT standards, including network and cybersecurity standards. The DoD CIO oversees programs to enhance and supplement DIB company capabilities to safeguard DoD information that resides on or transits DIB unclassified information systems.

The DoD reviewed and assessed whitepapers that were submitted by RFI respondents and determined that no single respondent could meet all the broad facets required to serve as the CMMC Accreditation Body.

§§ 170.8, 170.9, and 170.10 document the roles of the CMMC AB and the CAICO in managing a complaints/appeals process for CCAs, CCPs, and C3PAOs. OSCs concerned about the results of a Level 2 or Level 3 Certification assessment have a route of appeal documented in § 170.9. DoD, as the contracting entity, is not subject to service level agreements. Vendors and prospective vendors can voice concerns with the relevant contracting officer. External organizations may utilize existing DoD procedures to file complaints or concerns against any DoD organization.

This rule establishes requirements for the conduct of assessments, as well as the requirements for handling of disputes, to include an appeals process. In the roles established by this rule, C3PAOs and the CMMC AB execute program requirements as codified in the 32 CFR part 170 CMMC Program rule, with appropriate DoD oversight. For ISO/IEC 17020:2012(E) and ISO/IEC 17011:2017(E) compliance, an appeals process is required. Appeals are addressed in §§ 170.8(b)(16) and 170.9(b)(9), (14), (20), and (21).

The DoD declines to update the rule content of § 170.6 to include a new subsection on DoD PMs and requesting activities and their responsibilities regarding marking CUI as that subject matter is already addressed for the DoD. DoD Instruction 5200.48 on CUI establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with 32 CFR part 2002, CFR for CUI to include 32 CFR 2002.20 Marking CUI; and 48 CFR 252.204-7008 and DFARS clause 252.204-7012. The CMMC Program requirements make no change to existing policies for information security implemented by the DoD.

The DoD declined to modify the rule to further define the existing CMMC PMO oversight responsibilities, identified in § 170.6, which includes the CMMC AB and all other aspects of the program.

b. CMMC- AB

Comment: There were multiple comments regarding the CMMC Accreditation Body (AB). Ten comments were not relevant to the rule text. Multiple commenters asked about mechanisms to monitor the CMMC AB and how the DoD provides oversight. Seven comments provided valuable editorial recommendations that enhanced the existing rule text. Seven comments also raised concerns and asked for clarification about certification of the CMMC AB, its standing with international accreditation bodies and the effects of that standing on the C3PAOs. Two comments sought clarity on the CMMC AB's responsibilities and what resources they will provide to the CMMC ecosystem. One comment suggested incorporation by reference of specific CMMC AB generated artifacts. One comment requested clarity on terms and definitions regarding the CMMC AB.

Response: Some comments received lacked relevance to the rule's content, including the establishment of outside entities. The DoD declines to respond to speculative or editorial comments about private citizens or entities, which are outside the scope of this rule. The DoD declines to respond to requests for documents related to the CMMC AB and the CAICO that lack relevance to the CMMC rule.

The term CMMC Accreditation Body is a generic term for whichever accreditation body is supporting the DoD at a given time. The rule has been updated to remove reference to any specific accreditation body. There is only one Accreditation Body for the DoD CMMC Program at any given time, and its primary mission is to authorize and accredit the C3PAOs. The Accreditation Body does not issue certifications. The current CMMC AB is under a no-cost

contract that has followed normal DoD contracting procedures. The DoD declines to delete the section outlining requirements for the CMMC AB, which are enduring and apply irrespective of which entity the DoD has currently approved to serve in that capacity.

This rule identifies the requirements for the Accreditation Body's role in the CMMC Ecosystem. The DoD has a variety of options available to address the commenter's concern should the current CMMC AB not be able to fulfill this role. These include but are not limited to, contracting with a new/replacement Accreditation Body. And authorized and accredited C3PAOs would be able to continue conducting CMMC assessments.

§ 170.8(b)(6) requires the CMMC AB to complete a CMMC Level 2 assessment conducted by DCMA DIBCAC that must meet all CMMC Final Level 2 certification assessment requirements and will not result in a CMMC Level 2 certification. This requirement for an assessment is based on the potential compilation of sensitive information on the CMMC AB's information systems. After the CMMC AB's successful completion of this Level 2 assessment, the DoD reserves the right to send CUI to the CMMC AB, as appropriate.
Requirements for the CMMC AB, detailed in § 170.8(b) of this rule, include DoD requirements to comply with Conflict of Interest, Code of Professional Conduct and Ethics policies as set forth in the DoD contract with the AB. § 170.8(b)(3) details the ISO/IEC requirements the CMMC AB must meet and the timeline for meeting them. § 170.8(b)(3)(i) and (ii) further detail the requirements for the CMMC AB to authorize and accredit C3PAOs. The CMMC AB is under contract with the DoD and must fully comply with the contract requirements.

The CMMC rule was updated to clarify that the CMMC AB must be a U.S.-based signatory to the International Laboratory Accreditation Cooperation Mutual Recognition Arrangement within 24 months of DoD approval and must operate in accordance with ISO/IEC 17011:2017(E). The rule was also updated to clarify that a disqualifying eligibility determination may result in the CMMC AB losing its authorization or accreditation under the CMMC Program.

All CMMC ecosystem members are required to abide by the appropriate ethics and conflicts of interest policies established by the CMMC AB and CAICO. Rule content pertaining to ethics, quality assurance functions, record keeping, data encryption, security, etc. functions across the ecosystem are tailored to reflect the role each entity fills in the ecosystem. The CMMC AB is not an agency of the Federal government; it is a private sector organization operating under contract with the DoD. As described in § 170.6(a), the Office of the Department of Defense Chief Information Officer (DoD CIO) provides oversight of the CMMC Program and is responsible for establishing CMMC assessment, accreditation, and training requirements as well as developing and updating CMMC Program implementing guidance. The Accreditation Body must be under contract with the DoD. The rule has been modified to include additional CMMC AB oversight responsibilities for the CMMC PMO. The Department declines to incorporate CMMC AB generated artifacts into the rule by reference. The responsibilities of the DoD CIO and CMMC PMO are outlined in § 170.6 and the responsibilities of the Accreditation Body are outlined in § 170.8.

The DoD acknowledges that the CMMC AB may not offer both accreditation services and certification services. DoD declines to make edits to these sections as they are in alignment with the roles and responsibilities of the CMMC AB. The DoD has revised § 170.8(b)(17)(i)(C) in the rule to clarify that the "CMMC activities" which former Accreditation Body members are prohibited from include any or all responsibilities described in Subpart C of this rule.

The rule was updated to indicate that C3PAOs must also meet administrative requirements as determined by the CMMC AB. It was also updated to clarify that the term "independent assessor staff" in § 170.8(b)(4) refers to independent CMMC Certified Assessor staff, and to clarify the meaning of the term "members" at § 170.8(b)(17)(i)(B). DoD declines to modify § 170.8(b)(15) to include the phrase "technical accuracy and alignment with all applicable legal, regulatory, and policy requirements", as this does not result in a substantive change to the requirements as currently specified.

c. C3PAOs

Comment: Clarification was requested regarding C3PAOs' timelines for accreditation and their dependencies on the CMMC AB accreditation process. Some commenters requested additional time. Clarification was also requested on the current disposition of authorized C3PAOs. A few comments asked for simplification and clarification of the difference between the terms "authorized" and "accredited" with the establishment of C3PAOs. One comment requested that the rule be edited to require full compliance before C3PAOs can conduct certifications, and that duplicative language relating to ethics, record keeping, etc., be moved to a central location in the rule. One commentor questioned whether § 170.9(b)(16), which states "Ensure that all CMMC assessment activities are performed on the information system within the CMMC Assessment Scope", applies to all C3PAO personnel or just those involved in the Quality Assurance process.

Other comments objected to the requirement that C3PAOs obtain a CMMC Level 2 certification assessment because the assessment does not result in a Level 2 certification. They asked whether this would require two separate assessments every three years for C3PAOs that also conduct contractor work for DoD. Two comments requested clarification on determining the scope for a CMMC Level 2 assessment of a C3PAO to be used by DIBCAC, and if or when they would be required to obtain a FedRAMP Moderate certification. Also, clarification was requested on whether a C3PAO is permitted to possess OSC CUI and other artifacts during the assessment so long as they are destroyed upon completion of the assessment. One comment suggested that all information collected by the C3PAO be encrypted.

Three comments asked for clarification on what constitutes a C3PAO assessment team and whether it can consist of solely a Lead CCA. One commentor asked whether entities accredited under ISO 17020:2012(E) by another accreditation body, rather than the CMMC AB, meets CMMC C3PAO requirements. A couple of comments asked for clarification on whether a C3PAO could be foreign owned and participate in the current CMMC AB Marketplace.

Response: One commenter misinterpreted several sections of the CMMC rule. By defining the requirements in this rule to become a C3PAO, and defining a scoring methodology, the DoD is providing the authority and guidance necessary for C3PAOs to conduct assessments.

DoD considered many alternatives before deciding upon the current CMMC structure. The DoD has established requirements for a CMMC Accreditation Body, and this accreditation body will administer the CMMC Ecosystem. The appeals process is defined in §§ 170.8(b)(16) and 170.9(b)(9), (14), (20), and (21). The DoD will not assume the workload of directly managing the CMMC ecosystem or the other alternatives suggested. DoD must treat all potential defense contractors and subcontractors fairly. DoD cannot inadvertently create a pathway to a free assessment for an organization by virtue of its dual-purpose as a C3PAO and separately as a defense contractor. Therefore, DoD assesses C3PAOs free of charge, but the assessment does not result in a Certificate of CMMC Status. The C3PAOs determine the people, processes, and technologies that are in-scope for their DIBCAC assessment to become a C3PAO. The need to protect the assessment information is independent of its status as FCI or CUI. Assessment information, such as which requirements are MET or not, as well as the evidence and analysis leading to that result, would provide valuable insights to an adversary if not protected. A C3PAO is not a CSP and therefore would not require a FedRAMP moderate assessment to be a C3PAO. However, if they use a CSP to process, store, or transmit assessment information, then the CSP would require a FedRAMP Moderate, or equivalent, assessment. The CSP assessment results and CRM would be in scope for the C3PAO assessment.

The requirements in § 170.9 apply to both authorized and accredited C3PAOs. The only difference between authorization and accreditation is the status of the CMMC Accreditation Body. Prior to the CMMC AB achieving its full ISO/IEC 17011:2017(E) compliance, the interim term "authorized" is used for C3PAOs. As stated in §§ 170.8(b)(3)(i) and 170.9(b)(1) and (2), currently authorized C3PAOs must achieve and maintain compliance with ISO/IEC 17020:2012(E) within 27 months of authorization. As stated in § 170.9(b)(6), C3PAOs must obtain a Level 2 certification assessment, but this does not result in a CMMC Level 2 certificate.

The DoD declines to modify the rule text related to C3PAO requirements as it does not make a substantive change. Requirements are specified in the rule for each entity within the CMMC ecosystem.

A C3PAO may start preparing for compliance with ISO/IEC 17020:2012(E) before the Accreditation Body achieves compliance with ISO/IEC 17011:2017(E). The 27-month timeline for a C3PAO to achieve and maintain compliance with ISO/IEC 17020:2012(E) begins on the date that the C3PAO is authorized by the Accreditation Body, as addressed in § 170.9(b)(2) C3PAOs authorized by the CMMC AB prior to becoming compliant with ISO/IEC 17020:2012(E) must be accredited by the CMMC AB within 27 months of the C3PAO's initial authorization to meet CMMC program requirements. The accreditation process is not tied to, nor is it impacted by, the DoD's appropriations period.
The rule has been updated to add "authorized" to the definition of a C3PAO. Authorized is defined in § 170.4.

DoD disagrees with the suggestion that certain C3PAO requirements are not needed or redundant. C3PAO's must follow specific requirements for CMMC assessment record retention and disposition, audits, personal information, and CMMC Assessment Scope. Each paragraph number is independent, dependent sub-paragraphs are numbered with lower case Roman numerals. The requirement in § 170.9(b)(16) applies to all C3PAO company personnel participating in the CMMC assessment process.

The size of a C3PAO assessment team is variable based on factors including the scope of the assessment and the arrangements between the OSC and C3PAO. The rule has been updated in § 170.9(b)(12) to clarify that, at a minimum, the assessment team must have a Lead CCA, as defined in § 170.11(b)(10), and one other CCA. A C3PAO is permitted to possess OSC CUI and artifacts during an assessment. CMMC Certified Assessors must use the C3PAO's information technology which has received a CMMC Level 2 certification assessment as stated in § 170.11(b)(7) and any copies of the OSC's original artifacts must be destroyed when the assessment is complete as defined in § 170.9(1).

The DoD has considered the recommendation to require encryption of all information and declines to revise the rule text, since the C3PAO is required in § 170.9(b)(6) to obtain a Level 2 certification assessment conducted by DCMA DIBCAC.

Several foreign or international companies submitted comments expressing interest in the rule section pertaining to C3PAO requirements (§ 170.9(b)) and correctly noted that this section does not preclude otherwise qualified foreign companies from achieving C3PAO accreditation. Also, the DoD does permit 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.

d. CAICO

Comment: Numerous comments requested correction of perceived misstatements, oversights, or erroneous paragraph references in the CAICO responsibilities section. One commenter suggested the level of detail in § 170.10(b) is more appropriate for a statement of work and some paragraphs could be deleted from the rule. They offered preferred rewording to clarify that the CAICO must also comply with AB and ISO/IEC requirements, and further recommended deleting the requirement to provide all documentation in English. In addition, they recommended deleting separation of duties as a requirement, because it is already required under ISO/IEC certification. One commenter conflated CAICO subcontractors with DIB subcontractors and suggested deletion of the rule's restrictions on releasing CMMC-related information. One comment asked whether the Cyber AB and CAICO have documented processes for regular review and updates to their compliance documentation. Lastly, one comment requested duplicative language relating to ethics, record keeping, etc. be moved to a central location in the rule.

A few commenters suggested preferred edits to improve the role of the CAICO. One comment noted that the accreditor for certifying the CAICO should be a U.S.-based signatory to

ILAC or relevant International Accreditation Forum (IAF) in addition to complying with ISO/IEC 17011:2017(E). Two comments noted concerns that having only one CAICO would create an untenable bottleneck should something happen to the single CAICO. One commenter asserted that the CMMC Certified Instructor (CCI) certification requirement is redundant and not cost-effective since instructors will need to be certified as CCPs or CCAs to teach those courses. One comment suggested a grace period of 18-24 months from final rule publication, to allow update of training and examinations, before implementing the CCP and CCA certification requirements. Three comments recommended that Approved Publishing Partner (APP) and Approved Training Providers (ATP) sections be added to Subpart C of the rule. One commenter asked for clarification on what constitutes a CAICO subcontractor and if this includes LTPs and LPPs, and asked why an authorization process for LTPs and LPPs is not included in the rule.

One commenter appreciated that CAICO responsibilities include compliance with relevant ISO/IEC standards, as those are internationally recognized standards.

One commenter provided an attachment containing an image of an article published in the February 2024 issue of National Defense Magazine. The commentor did not provide specific questions or comments regarding the article, they simply submitted an article. DoD declines to comment on the reposting of information being reported in the media.

Response: The DoD declines to comment on the reposting of information being reported in the media. This rule identifies requirements for the CAICO role in the ecosystem. The DoD has a variety of options available to address issues with reliance on a single CAICO. These include but are not limited to working with the CMMC AB to identify a new/replacement CAICO.

The final rule includes a requirement for the Accreditation Body, CAICO, and C3PAOs to adhere to appropriate ISO/IEC standards, which include the current version of the standard for conformity assessment (ISO/IEC 17024:2012(E) located at ISO website: www.iso.org/standard/52993.html).

All CMMC ecosystem members are required inter alia to abide by the appropriate ethics and conflicts of interest policies established by the CMMC AB and CAICO. Rule content pertaining to ethics, quality assurance functions, record keeping, data encryption, security, etc. functions across the ecosystem are tailored to reflect the role each entity fills in the ecosystem. Repeating this content in the section of each ecosystem role serves to emphasize the importance of adherence to these requirements.

DoD disagrees with the commenter's suggestion that certain CAICO requirements are not needed or are redundant. The DoD requirement for documentation in English refers to official information provided to the Accreditation Body or the DoD. The commenter's preferred rewording of § 170.10(b)(3) is unnecessary because there is a separate requirement for the CAICO to meet ISO/IEC standards, and this rule does not codify non-DoD requirements. The DoD declines to remove the requirement in § 170.10(b)(10) to provide status information to the CMMC AB because it is necessary for program management. The rule retains the separation of duties requirement at § 170.10(b)(11), which is more specific than the management of impartiality required under ISO/IEC 17024:2012(E).

The DoD declines to delete certification requirements for CCI. Having the technical background as a CCP or CCA does not ensure all the instructor-unique qualifications necessary to be a CCI are met. The DoD also declines to remove the reference to § 170.10 from § 170.12(b)(1) since it is accurate that the CAICO certifies CCIs.

Section § 170.10(b)(13) ensures that personal information is encrypted and protected in all CAICO information systems and databases and those of any CAICO training support service providers. DoD disagrees with the commentor's statement that training support service providers of the CAICO be allowed to disclose information about CCAs and/or CCPs. § 170.10 references the CAICO requirements. Entities providing training support services to the CAICO are not a part of the assessment process in the ecosystem. It is not up to them to release data on certified persons in the ecosystem. Any metrics regarding certifications will come from the CAICO.

DoD declines to add Approved Publishing Partner (APP) and Approved Training Providers

(ATP), or sections to the rule. The CMMC Program defines the requirements for the ecosystem. Specific requirements for publishing and training guidelines are determined by the CAICO and do not require the oversight of the DoD. The CMMC Rule does not use the term Licensed Training Provider (LTP), as the LTPs are not required to be licensed. The acronym ATP means Approved Training Provider which encompasses the same role in the CMMC Ecosystem. The DoD does not intend to further delay implementation of CMMC to provide an 18 to 24-month grace period from the official release of the rule to build curriculum.

The DoD has reviewed commenter recommendations and revised the rule as follows: The CMMC rule has been updated to state that the CAICO must be accredited by a U.S. based signatory to ILAC or other relevant IAF mutual recognition arrangements and operate in accordance with ISO/IEC 17011:2017(E). The DoD has removed the term "practitioner" from § 170.10(b)(8) for clarity and changed the term subcontractor to training service support provider.

e. CCPs and CCAs

Comment: Some comments requested DoD's response to speculations about market forces, competitiveness of the CMMC Certified Professional (CCP) and CMMC Certified Assessment (CCA) roles and career opportunities, assessor burnout, complexity of CMMC ecosystem, and a limited assessor pool.

Several comments identified administrative changes or preferred rewording or reordering of the CCP and CCA sections of the ecosystem requirements. For example, two commenters objected to repeating the requirement to meet CoPC and COI requirements for each Ecosystem member in § 170.8. Another comment requested deletion of the requirement for all documentation and records to be provided in English.

One commenter recommended revising proficiency and experience requirements for CCPs, CCAs, and Lead CCAs. Another requested clarification on what requirements govern the certification of a CCA and requested the rule allow the CAICO to establish the certification validity period. One comment recommended all additional assessor certification requirements in § 170.11(b)(6)(ii) be removed from the rule, so that only those prerequisite training requirements identified by the CAICO would apply.

Another comment suggested that a requirement prohibiting assessors from use of personally owned IT that is contained in the CCA section at § 170.11 also be added to the C3PAO requirements section at § 170.9. Two commenters objected to the restrictions on CCAs sharing information with people outside the assessment team.

One comment questioned the requirement for a Tier 3 background investigation for CCPs and another suggested the validity period of CCP certification should be determined by the CAICO. Yet another comment suggested changing certification periods from 3 to 4 years for those certified prior to the rule becoming effective. One comment suggested there is insufficient clarity regarding the role CCPs may play in an assessment and another asked whether a CCPs was allowed to review more than just Level 1 requirements. Two other comments recommended updating CCP training to include Level 2 practices. Another comment noted that assessor cannot be robotic and that they must be allowed to evaluate the situation as it pertains to the company being evaluated.

One comment asked for clarification on Lead CCA requirements and requested a reduction in the management experience to 2 years. Two other comments recommended adding IT and cybersecurity experience as relevant skills. One comment also recommended that Lead CCAs have industry-specific knowledge of the industry in which the OSC being assessed participates. Another comment requested clarification whether years of experience are cumulative for the Lead CCA. One comment recommended changing the name of Lead CCA and adding roles and responsibilities requirements. One stated that the rule's CCA prerequisites is too low a skill set and recommended increasing the requirements for both CCAs and Lead CCAs. While another comment noted the rule referenced both DoD Manual 8570 and DoD Manual 8140.03 and one or the either should be used.

One commenter suggested that should sufficient assessors not be available to meet demand, the DoD should provide a delay or "grace period" to meet certification requirements.

Response: The CMMC rule provides detail on anticipated impacts on the DIB in the Impact and Cost Analysis summary of the preamble. Speculation on market forces on roles in the CMMC ecosystem such as CCPs and CCAs are outside of the scope of the CMMC program rulemaking. Likewise, limitations on career opportunities and associated issues such as burn-out or job satisfaction are beyond the scope of the program.

The DoD updated the rule to clarify that CCAs must meet all the requirements set forth in § 170.11(b) and modified the rule in § 170.10(b)(10) to include CMMC Certified Professionals (CCPs). § 170.13(b)(6) was changed to conform to rule text in § 170.11(b)(9) and to clarify with whom information may be shared.

The DoD determined the certification requirements specified in § 170.11(b)(6) meet the needs of ensuring certified assessors have the required depth of cybersecurity knowledge and experience that is beyond what the CMMC-specific training provides.

The DoD disagreed with the comment that the CAICO should determine the length of time a CCP certification is valid. DoD has a significant interest in ensuring the quality of assessors in the CMMC ecosystem and the currency of their training. The DoD does not agree with the assertion that managerial, and personnel related skills are most relevant for success as a Lead Assessor. As written, § 170.11 of the rule requires Lead Assessors to have a balance of technical and managerial expertise. A Lead Assessor also requires assessment or audit experience. The DoD views these skills as the minimum required to adequately provide the technical guidance and managerial oversight of the assessment team. The DoD declined to revise the rule to specify IT and/or Cybersecurity for the required audit experience.

The DoD also disagreed with a recommendation to require Lead CCAs to have industryspecific knowledge of the industry in which the OSC being assessed participates. The DoD found that this requirement would unreasonably restrict C3PAOs from participating in a broad range of assessments and could have a negative effect on the ability of the DIB to schedule CMMC Level 2 certification assessments. The OSC can select a C3PAO with the experience it considers valuable.

The DoD declined a commentor's request to modify the rule to allow the CAICO to determine the requirement for the frequency of CCA/CCP certification. The DoD considers the 3 years certification period a key CMMC program requirement that will be enacted and managed by the CAICO. The DoD also declined to change the rule to extend the certification timeline to 4 years for those earning a certification prior to completion of rulemaking. Additionally, the DoD did not accept the recommendation to remove the requirement for providing documentation in the English language, which applies to all official information that would be provided to the CAICO, CMMC AB, or the DoD.

The DoD disagreed with a commenter's recommendation to remove the second sentence in § 170.11(b)(7) that prohibits individual assessors from using any IT other than that provided to them by the C3PAO that has been contracted to perform that OSA's assessment. This sentence is required to eliminate ambiguity, particularly for C3PAOs that may have implemented a BYOD program or that allow some work roles to use personal devices. The DoD updated the rule to provide additional clarity.

The DoD does not concur with the comment calling for a DoD Manual 8140.03 requirement on CCAs. Assessment teams are required to have a Lead Assessor who must meet the higher level of the DoDM 8140.03 requirements. The rule has been updated to remove reference to DoD Manual 8570.

The experience requirements referenced for the Lead CCA are cumulative. The rule has been updated to move Lead CCA requirements to the end of § 170.11, but not to create a new section.

The DoD disagreed with the commenter's assertion that Assessors are robotic. Assessors will go through CMMC training and will assess each unique CMMC Assessment Scope, as defined by the OSA, against the security requirements. As specified in § 170.13(a) CCPs can participate on CMMC Level 2 certification assessments with CCA oversight where the CCA makes all final decisions. Updates to training are beyond the scope of this rule. Statements made in training

materials produced prior to final adoption of the CMMC rule are beyond the scope of CMMC rulemaking. DoD disagrees with the comment that § 170.13 does not provide sufficient detail regarding the role CCPs may play in an assessment. The requirement in the rule that "with CCA oversight where the CCA makes all final determinations" provides sufficient flexibility to adapt to a wide variety of assessments while ensuring the responsibility for assessment findings rests with the CCA and Lead CCA.

The rule restates COI and CoPC requirements in each ecosystem section because all CMMC ecosystem members are required to abide by the appropriate ethics and conflicts of interest policies established by the CMMC AB and the CAICO. Rule content pertaining to ethics, quality assurance functions, record keeping, data encryption, security, and other functions across the ecosystem are tailored to reflect the role each entity fills in the ecosystem.
DoD CIO, in coordination with OUSD/I&S, evaluated the requirements for the CMMC Ecosystem. Based on the access to sensitive unclassified information, a Tier 3 background investigation that results in determination of national security eligibility is required. § 170.13(a) states that a CCP is eligible to participate in Level 2 certification assessment with CCA oversight and is eligible to become a CCA and will receive additional training and testing per the requirements in § 170.11.

The phased implementation plan described in § 170.3(e) is intended to address ramp-up issues and provide time to train the necessary number of assessors. DoD has updated the rule to add an additional six months to the Phase 1 timeline.

e. CCI

1. Training and Training Materials

Comment: One comment mistook the requirement to "provide all documentation and records in English" as applying to training materials. Four comments expressed concerns about the requirements for confidentiality surrounding training records. These concerns arose primarily from a misinterpretation of the requirement to "keep confidential all information obtained during the performance of CMMC training activities" to mean a requirement to keep the training materials themselves confidential, rather than keeping student records confidential.

Response: The requirement to "provide all documentation and records in English" refers to official information that would be provided to the CMMC Assessor and Instructor Certification Organization (CAICO) or the DoD. The terms do not pertain to all materials used in the delivery of a course. The DoD disagreed with the recommendation to delete the § 170.12(b)(7) requirement for keeping CMMC training records and information confidential. "Training activities" do not include course material. The example in § 170.12(b)(7) (student records) makes clear the type of data covered by the rule.

2. Time Limits and Other Constraints

Comment: One comment recommended that the CAICO, instead of the DoD, determine the frequency of CMMC Certified Instructor (CCI) certification. Another requested clarification on the length of time that a CCI may not provide consulting services. One comment recommended changing the rule to require CCIs to provide updates to the CAICO and the CMMC AB no less than annually, in lieu of "most up to date".

Two comments expressed concern that CCIs are not allowed to provide consulting services to OSCs; one of the comments asserted this would result in reduced quality of training for CMMC Certified Professionals (CCP) and CMMC Certified Assessors (CCA). One comment expressed disagreement with the requirement prohibiting CCIs from exam development and exam proctoring. Another comment recommended a rule update indicating CCIs can teach both CCA and CMMC Certified Professional (CCP) candidates.

Response: The DoD declined a commenter's request to modify the rule to allow the CAICO to determine the requirement for validity period of a CCI certification. The DoD considers the 3year certification period for CCIs as a key CMMC program requirement that is to be enforced by the CAICO.

The DoD modified § 170.12(b)(4) to read "annually" instead of "most up to date" to clarify the reporting requirement.

All CMMC ecosystem members are required to abide by the appropriate ethics and conflicts of interest (COI) policies established by the CMMC AB and CAICO. Rule content pertaining to ethics, quality assurance functions, record keeping, data encryption, security, and other functions across the ecosystem are tailored to reflect the role each entity fills in the ecosystem. The DoD defined COI requirements to reduce the possibility that a CMMC Ecosystem member acting in one capacity may bias, or be biased by, clients that are paying them to perform another CMMC related service. CCIs are not permitted to develop or proctor exams to avoid participating in any activity, practice, or transaction that could result in an actual or perceived conflict of interest.

3. Relationship to CAICO and Other Ecosystem Members

Comment: One comment asked why the rule does not include requirements for LTPs, and another requested additional rule text to clarify the relationship between an ATP and the CAICO in administrative matters of students. One comment recommended not requiring CCIs to provide qualification and training information to the CAICO.

One comment recommended a method for reducing a perceived redundancy in the rule text between ecosystem-related sections. Two comments asserted that a CCI certification is redundant because individuals attempting to become CCIs are already certified as CCPs or CCAs.

One comment asked that a new requirement be added to the rule under § 170.12 to address the transition of Provisional Instructors to CCIs.

Response: The CMMC rule does not use the term Licensed Training Provider (LTP), as training providers are not required to be licensed. The correct term for CMMC training providers is Approved Training Provider (ATP). The CMMC rule contains the requirements to create the training for the CMMC Program. § 170.10 contains the requirements for the CAICO to ensure compliance with ISO/IEC 17024:2012(E) and to ensure all training products, instruction, and testing materials are of high quality.

DoD disagreed with a comment to delete a requirement in the rule for CCIs to update the CAICO regarding qualification, training experience, and other information relating to their competency to teach within the CMMC ecosystem. Viewing and verifying CCI qualifications is an important element of quality assurance in the CAICO's role of training, testing, authorizing, certifying, and recertifying CMMC assessors, instructors, and related individuals.
§ 170.12(b) in the rule was updated to add the requirement for a CCI to be certified at or above the level of training they are delivering. The DoD also modified § 170.12(a)(11) to add CMMC Certified Professional (CCP) candidates.

The DoD declined to remove the certification requirement for CCIs. Although CMMC Certified Assessors have the technical background, that does not imply that they meet all the instructor-unique qualifications necessary to be a CCI.

The DoD modified § 170.12 to include requirements for Provisional Instructors prior to their transition to a CMMC Certified Instructor. Any Provisional Instructor (PI) will be required to achieve certification under the CMMC Certified Instructor (CCI) program within 18 months of the final rule publication. The PI designation ends 18 months after the effective date of the rule.

f. Conflicts of Interest and Code of Professional Conduct

Comment: Many commenters had questions about existing CMMC conflict of interest (CoI) requirements and had suggestions for further protecting the impartiality of the CMMC Program. One commenter requested the Department develop a mechanism to prevent third-party assessment organizations from delaying re-evaluation of NOT MET requirements to create a pipeline of future assessment work. The commenter recommended removing the 10-day reevaluation deadline requirement currently in the CMMC Rule to prevent any conflicts of interest. Another commenter stated that allowing a commercial entity to manage the CMMC 'ecosystem' creates a scenario 'fox watching the henhouse" condition and that fraud and abuse will be rampant.

Some commenters questioned the legality of the current CMMC AB's establishment and alleged unethical behavior by its Board of Directors. They cited the number of resignations among its Board of Directors as evidence of internal politics, conflicts of interests, or ethics

concerns. One commenter suggested the 6-month "cooling off period" between an employee leaving the CMMC AB and supporting other CMMC roles be extended to one year to ensure impartiality within the CMMC Program. Another commenter claimed an informational newsletter offered by the CMMC AB to ecosystem members violates the conflicts of interest requirements. In addition, commenters alleged that the CMMC AB's progress (prior to final rule publication) toward ISO/IEC compliance violates the terms of its contract with DoD, which the DoD should terminate.

Commenters also stated that DoD's no-cost contract with the current CMMC AB has forced them to focus on generating revenue instead of building a CMMC Assessor cadre. One commenter cited publicly available tax filings of the current CMMC AB to substantiate that view. Another commenter noted concerns that the rule permits a timeline for meeting the ISO/IEC requirements, rather than requiring immediate compliance, and suggested that it would be more advantageous to cite different ISO/IEC requirements (for conformity assessment) than those identified in the rule.

One commenter wrote that significant delays in CMMC implementation this far beyond the Department's earlier objectives of 2020 constitute fraud and claimed that DoD representatives directed companies to comply with requirements that have become irrelevant due to changes in program requirements that occurred during rulemaking.

Many commenters stated the Department needs to further clarify existing CoI requirements for CCIs, CCAs, and CCPs in the CMMC Rule text. Specifically, commenters suggested the DoD:

- Revise § 170.12(b)(5) to state that CCIs may serve on an assessment team for a student's company, provided the CCI does not provide consulting to an OSC during delivery of the CMMC Instruction or breach other conflict of interest rules, and add that the CCI must "[b]e a currently certified CCA and conduct at least one certified or mock assessment under the direction of a C3PAO annually."
- Revise § 170.12(b)(6) to allow CCIs to craft exam objectives and content, as CCIs are the "most in tune with issues faced by candidate CCPs and CCAs."
- Strike § 170.12 altogether, because potential CoIs will be rare and can be "managed by existing conflicts of interest mechanisms"; clarify that "while serving as a CMMC instructor" means "limited only to while actively teaching or any time while the person holds the CCI certification"; and that CoI concerns could be addressed by the addition of an Instructor Code of Conduct. One commenter also suggested this section would significantly decrease the available pool of CMMC instructors, as they would be forced to choose between instructing and consulting, which may be a more lucrative option. They also claimed it prevented CCIs who teach CCP/CCA courses at night from providing consulting services during the day.
- Impose a three- or four-year prohibition on ecosystem members from participating in the CMMC assessment process for an assessment in which they previously served as a consultant or "since the OSC last obtained CMMC certification, whichever is most recent."
- Add language to §§ 170.11 and 170.13 to clarify if an individual consults with a defense industrial base company, they are prohibited from participating as a CMMC assessor for that same company.
- Update § 170.8(b)(ii)(17)(ii)(G) and add a time limit to this requirement to ensure a consultant can perform assessments, given an appropriate amount of time has passed.
- Revise § 170.8(b)(17)(ii)(G) to say, "Prohibit CMMC Ecosystem members from participating in the CMMC assessment process for a CMMC assessment in which they previously served as an employee or consultant to prepare the organization for any CMMC assessment," as both an OSC employee and a CCPA/CCP serving as a consultant would face identical CoI.
- Provide more detail on the scope of CCA and CCP conflict of interest disclosure required, particularly around the definition of "process, store, or transmit" in § 170.4(b).
- More narrowly tailor the CoI requirement in § 170.8(b)(17)(i)(D) and more expressly identify the "perceived conflicts of interest" scenarios to help ecosystem members avoid legal risk. -

Rewrite § 170.8(b)(17)(iii)(C) to clarify what constitutes a "satisfactory record of integrity and business ethics."
- Provide more detail in § 170.10(b)(11) on the term “separation of duties,” so CCAs know whether they can volunteer to develop test questions or provide training.

Response Summary: Some comments received lacked relevance to the rule's content, which is limited to specific CMMC Program requirements. The DoD declines to respond to speculative or editorial comments about private citizens or entities, all of which are not within the scope of this rule. Personnel actions taken by the CMMC AB and comments regarding filing of IRS forms are not within the scope of this rule.

§ 170.8(b) of this final rule provides requirements of the CMMC AB. CMMC Program requirements as described in this rule requires the CMMC Accreditation Body and the CAICO to have and abide by ethics and conflicts of interest rules and to have and maintain a Code of Professional Conduct (CoPC). § 170.8(b)(3) describes the ISO/IEC requirements and the timeline in which the CMMC AB needs to meet those requirements. The DoD declines to comment on business decisions made by the current CMMC AB in the performance of its CMMC related roles, responsibilities, and requirements. Based on information currently known to DoD, the CMMC AB is currently performing as defined in this final rule and the terms of the contract. The ANSI National Accreditation Body is performing the function of accrediting the CAICO, which is appropriate given its status as a subsidiary of the CMMC AB.

The DoD defined CMMC Conflict of Interest requirements to reduce the possibility that a member of the CMMC Ecosystem acting in one capacity may bias, or be biased by, clients that are paying them to perform another CMMC related service. The rule text includes ethics requirements for members of the CMMC ecosystem, to include the CMMC AB (§ 170.8). The DoD concurred with some comments and has increased the cooling off period from six months to one year in § 170.8(b)(17)(i)(C).

DoD considered many alternatives before deciding upon the current CMMC structure. The DoD has established requirements for a CMMC Accreditation Body, and this accreditation body will administer the CMMC Ecosystem. The phased CMMC implementation plan provides time to train the necessary number of assessors and, the rule has been updated to add an additional six months to the Phase 1 timeline.

The DoD requires that the Accreditation Body must achieve and maintain compliance with the ISO/IEC 17011:2017(E) standard (the international benchmark used in demonstrating an accreditation body’s impartiality, technical competency, and resources) and the requirements set forth in § 170.8. The CMMC Proposed rule also requires compliance with ISO/IEC 17020:2012(E) for conformity assessments. § 170.12(b)(5) was revised to indicate that a CMMC instructor, subject to the Code of Professional Ethics and Conflict of Interest policies, may serve on an assessment team but cannot consult. CCIs are not permitted to develop or proctor exams to avoid participating in any activity, practice, or transaction that could result in an actual or perceived conflict of interest.

The CAICO is responsible to ensure the separation of duties for individuals volunteering to assist with testing, training, and certification activities. An example of separation of duties is shown in § 170.12(b)(6), which specifies that a CCI cannot be involved in examination activities. DoD modified § 170.8(b)(17)(ii)(G) to add that a consultant is only limited from participation in the assessment process for 36 months. CMMC Ecosystem members do not participate in an assessor capacity on DIBCAC assessments. The DoD declined to add explicit requirements prohibiting ecosystem members from participating in an assessment of an OSC by whom they were previously employed (directly or as a consultant), because the scenario is already covered under § 170.8(b)(17)(ii)(G).

DoD disagreed with the comments that a CMMC Ecosystem member is unable to avoid perceived conflicts of interest. The Accreditation Body is required to provide a CoI policy in § 170.8(b)(17) for CMMC Ecosystem members. The Department expects that a reasonable person subject to the CoI policy should understand how to avoid the appearance of conflicts of interest

and, if unsure, seek clarity from the Accreditation Body. Details of the disclosure requirements are in the Accreditation Body conflict of interest policy.
A satisfactory record of integrity and business ethics is a record that does not indicate derogatory behavior in relation to professional conduct or conflict of interest.

The DoD declined to remove the 10-day re-evaluation deadline in §§ 170.17(c)(2) and 170.18(c)(2) to ensure consistency in the assessment process. The OSC may utilize the appeals process, as necessary. The DoD is required to codify CMMC program requirements through a prescribed and formal rulemaking process. The timeline for CMMC implementation changed due in part to DoD's decision to pause and assess the program, seek opportunities to streamline and ease the burden of its implementation, and respond to public comments. The DoD declines to respond to speculative or editorial comments regarding the actions of private citizens, which are not within the scope of this rule.

g. Ecosystem Eligibility

1. Foreign Ownership

Comment: Two comments noted the rule does not include Foreign Ownership, Control, or Influence (FOCI) requirements for the CAICO. One comment recommended the rule incorporate the definition of the "national technology and industrial base" and exclude those companies from FOCI requirements. The NTIB includes organizations from the United States, the United Kingdom of Great Britain and Northern Ireland, Australia, New Zealand, and Canada that are engaged in research, development, production, integration, services, or information technology activities.

Response: The CAICO has no FOCI requirement because they do not have knowledge of the OSC's network or potential vulnerabilities identified in the assessment process. Per § 170.9(b)(5), the CMMC Program implements the FOCI program that is managed by DCSA. Potential FOCI exemptions are outside the scope of this 32 CFR part 170 CMMC Program rule and must be addressed through international arrangements or agreements.

2. Personnel Security

Comment: There were numerous comments regarding the Tier 3 Personnel Security requirements. Several comments recommended editorial clarification. Multiple comments requested clarification on what "not eligible" meant and what is the "equivalent process". One comment recommended the Tier 3 background investigation be required for all authorized personnel while two comments recommended eliminating the Tier 3 background investigation requirement. Two other comments requested clarification on why a Tier 3 investigation is required when no secret information is handled and there is no clearance granted. Another comment requested clarification on the Tier 3 process. Three comments requested clarity on the citizenship requirements and how the Tier 3 requirement will be enforced for international C3PAO's.

Another comment recommended adding a requirement for CMMC Instructors and Assessors to report to the CAICO within 30 days of conviction, or guilty pleas to certain crimes.

Response: In coordination with the OUSD/I&S, the DoD CIO evaluated requirements for the CMMC Ecosystem. Based on the access to sensitive unclassified information, a Tier 3 background investigation that results in determination of national security eligibility is required as specified in this rule. The concept of "not eligible" in § 170.9(b)(4) is intended to cover those applicants who do not meet the entrance requirements for a DCSA Tier 3 background investigation, it is not an alternative for applicants who do not pass its Tier 3 background investigation. The DCSA maintains a record of all background investigation information in the Personnel Vetting Records system of records, DUSDI 02-DoD, as published in the *Federal Register*. The details of the Tier 3 background investigation are included in this rule to inform the public of the CMMC requirement and that the investigation will not result in a clearance. The DoD declines to remove reference to the Standard Form 86 from the rule. All documentation and records for the background investigation process must be provided in English; rulemaking as a Federal regulation requires this level of detail to ensure clarity of understanding and interpretation. Details about background investigation equivalency is

available from DCSA at www.dcsa.mil/Industrial-Security/International-Programs/SecurityAssurances-for-Personnel-Facilities/. As stated in the 32 CFR part 170 CMMC Program rule, C3PAOs must meet the criteria defined in section § 170.9. If a non-U.S. organization, and its employees, meet all the requirements in § 170.9 and § 170.11, it would not be prohibited from operating as a C3PAO within the U.S. or abroad. The DoD declined to make recommended administrative changes to § 170.9(b)(3), because they did not result in a substantive change.

While a C3PAO may use its own employees to staff an assessment, it also may leverage CCAs and CCPS who are independent contractors, rather than employees of a specific C3PAO. Because these independent CCAs and CCPs may not be covered by the C3PAO's background check requirement, CMMC requires CCAs and CCPs to have their own Type 3 background checks or equivalent.

Section 170.10 has been updated to specify the CAICO must require CMMC Ecosystem members to report to the CAICO, within 30 days, if they are convicted, plead guilty, or plead no contest for certain specified legal matters or criminal activities.

h. ISO/IEC Standards

Comment: Several comments addressed ISO/IEC standards referenced in the proposed rule. Most of these were related to ISO/IEC 17020:2012(E). One commenter wanted to know what the proposed rule meant by "out-of-cycle from ISO/IEC 17020:2012(E)." Another felt the section outlining CMMC AB responsibilities should clarify that the CMMC PMO must approve all C3PAO accreditation requirements established by the Accreditation Body under ISO/IEC 17020:2012(E). One person felt the rule should give C3PAOs more time to achieve compliance with ISO/IEC 17020:2012(E) and one commenter asserted that including a revocation process in the CMMC PMO roles and responsibilities section was inconsistent with ISO/IEC 17020:2012(E) standards because the C3PAO was the certification body.

One comment asserted the requirement in the rule for the CMMC AB to complete the ILAC Peer Review prior to accrediting C3PAOs is too onerous and not consistent with the ISO/IEC process for gaining international recognition as an accreditation body in accordance with ISO/IEC 17011:2017(E).

Response: The rule was updated in § 170.8(a) to clarify responsibilities of the Accreditation Body. DoD agreed with the comment that the requirement to complete the Peer Review prior to accrediting C3PAOs was too onerous and inconsistent with the ISO/IEC process under ISO/IEC 17011:2017(E). The rule has been updated for clarity.

Using the terms of the ISO/IEC 17020:2012(E), the activity of the C3PAO is an "inspection", rather than a "certification". The C3PAO is an inspection body, not a certification body, and is responsible for conducting the Level 2 certification assessment [Inspection]. The rule was revised to delete terms related to granting or revoking certification assessment status. The DoD reserves the right to conduct a DCMA DIBCAC assessment of the OSA, as provided for under the DFARS clause 252.204-7012 and DFARS clause 252.204-7020. DoD declines to extend the period for C3PAOs to achieve compliance with ISO/IEC 17020:2012(E). The Department has determined that 27 months is reasonable and sufficient for a C3PAO to achieve compliance. The rule was also updated in § 170.9(b)(11) to clarify that audit information must be provided upon request.

14. Ecosystem Capacity

Comment: Commenters expressed concern that the demand for third-party assessments amongst the defense industrial base will exceed the capacity of available Certified CMMC Assessors and Certified CMMC Professionals and government assessors which may prevent timely and affordable audits or cause businesses to lose out on DoD contracts. To mitigate the concerns, one commenter suggested delaying phase-in of certification assessment by two years, by relying on self-assessment. One commenter warned of solicitation protests if companies are kept out of a competitive procurement due to a slow CMMC assessment process. Another suggested that insufficient assessors may shrink the market for DoD contractors and compromise assessment quality. Commenters were apprehensive that DoD projections for certification

demand didn't factor in all subcontractors and that the CMMC Accreditation Body lacks a strategy for scaling to meet increased C3PAO demand.

Additionally, one commenter pointed out that the rule indicates companies can pursue a certification assessment at any time after the rule is published, which could tie up already limited C3PAO resources and impede assessment opportunities for other companies bidding on an upcoming contract. Another expressed concern that often-extensive travel times required for assessors to reach rural-based companies like electric cooperatives will disincentivize assessors from prioritizing these companies and prevent their timely assessment.

Commenters suggested several actions the Department could take to mitigate capacity-related risks, including: extending the phase-in of Level 2 certification requirements; prioritizing companies for Level 2 phase-in; allowing C3PAOs to issue interim or conditional certifications when unable to timely complete contractor assessments; and waiving requirements for OSCs that are in the assessment process but not yet certified. Some asked that DoD forecast the volume and timing of Level 3 certification requirements and clearly communicate those assessment requirements with contractors. Another requested forecasts of both Level 2 and Level 3 assessment capacity against various demand scenarios for each certification level.

Several commenters suggested that CMMC assessment requirements for External Service Providers (ESPs) will also impede CMMC implementation, as ESPs (1) must be CMMC certified before an OSC can include them in their CMMC certification assessment scope and (2) will be competing with DIB companies for scarce C3PAO assessors. Commenters suggested ways to reduce burden on ESPs, which included: allowing use of non-compliant ESPs until Phase 3 and prioritizing certification assessments for ESPs ahead of other assessments.

Several commenters expressed concern about CCA and CCP roles, based on perceived scarcity of candidates in the job market compared with demand for similar services. Concerns included the potential for CCA and CCP burnout from overwork, dissatisfaction with repetitive assessments tasks, limited career path in the roles, and the complexity of operating within the CMMC ecosystem. One commenter compared CCA and CCP roles with those of Certified Public Accountants and Certified Information System Auditors, who have access to more varied opportunities and industries.

Response: DoD received numerous comments about the use of ESPs which do not process, store, or transmit CUI. In response, the DoD revised the rule to reduce the assessment burden for ESPs. ESP assessment, certification, and authorization requirements in 32 CFR 170.19(c)(2) and (d)(2) have been updated. ESPs that are not CSPs and do NOT process, store, or transmit CUI, do not require CMMC assessment or certification. Services provided by an ESP are in the OSA's assessment scope. The phased implementation plan described in § 170.3(e) is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies time to understand and implement CMMC requirements. The DoD has updated the rule to add an additional six months to the Phase 1 timeline. Phase 2 will start one calendar year after the start of Phase 1. It is beyond the scope of this rule for DoD to determine the order in which organizations are assessed.

The DoD declined to delete text stating that OSAs may elect to complete a self-assessment or pursue CMMC certification assessment to distinguish themselves as competitive because the recommendation did not result in a substantive change. CMMC rule describes anticipated impacts on the DIB in the Impact and Cost Analysis section. Speculation on market forces affecting the DIB is outside of the scope of the CMMC program. Speculation on market forces affecting CMMC ecosystem CCP and CCA roles are also outside of the scope of the CMMC program. Likewise, limitations on career opportunities and associated issues such as burn-out or job satisfaction are beyond the scope of the program.

The DoD declines to comment on external market factors impacting CMMC compliance. The seven-year timespan reflects the DoD's estimate for all DIB members to achieve CMMC compliance. The implementation plan ramps up CMMC assessment requirements over 4 phases, such that the ecosystem will reach maximum capacity by year four. The DoD does not agree with commenter assertions that 70,000 or more entities will require CMMC Level 2 assessment

by October 1, 2026. Table 6 of the Impact and Cost Analysis of CMMC 2.0 section provides the DoD's estimate of CMMC assessment numbers by year and level.

DoD considered many alternatives before deciding upon the current CMMC structure. By design, the CMMC program depends on the supply and demand dynamics of the free market, enabling it to naturally scale and adapt to capacity requirements. Planned changes to DCMA staffing levels have been considered with regard to implementation of CMMC Level 3 and C3PAO assessments as described in this rule. The DIBCAC will communicate extensively with contractors about the conduct of a Level 3 assessment during the pre-assessment planning phase.

15. Assessments:

a. Level 1 and Mapping of 15 Level 1 to 17 Level 2 Requirements

Comment: A few questions were submitted about CMMC level 1 requirements, on topics such as whether DoD intended affirmations for CMMC level 1 be required annually versus triennially, and whether specific policies and procedures documentation is required for Level 1 self-assessments. One commenter asked about limits on deficiency remediation and reaccomplishing an assessment in the event a company fails a CMMC Level 1 self-assessment. Another commenter asked for the specific wording to reflect a CMMC Level 1 assessment score in SPRS.

One commenter objected to CMMC level 1 annual affirmation, which they considered an unwarranted expansion of CUI safeguarding requirements to information systems that process only FCI. One commenter recommended revisions to explicitly indicate that OSAs may choose to engage the services of a C3PAO to inform the OSA's Level 1 self-assessment submission. Another commenter recommended editorial revisions to avoid use of the term "CMMC security requirements" based on the observation that CMMC requirements are aligned directly to those identified in FAR clause 52.204-21 or NIST publications.

One commenter asked for explanation of perceived differences between tables in the published rule that map CMMC Level 1 Security Requirements to NIST SP 800-171A Jun2018, as compared with prior versions of the document.

One commenter asked for the rationale associated with mapping 15 requirements for CMMC level 1 to 17 requirements in CMMC level 2. Two commenters asked if systems that process FCI (and require CMMC level 1) are considered within scope for CMMC level 2 or 3 assessments, and if so, how they should be documented.

Response: When applicable, the DoD does require an annual CMMC Level 1 selfassessment against the 15 safeguarding requirements aligned with FAR clause 52.204-21. Annual affirmations are required at every CMMC level. There are no explicit documentation requirements for a CMMC Level 1 Self-Assessment. The DoD modified the Level 1 Scoping Guide to provide clarity.

An OSA may complete as many self-assessments as desired, and there is no required timeframe between Level 1 self-assessments and updating CMMC Status in SPRS. The entry in SPRS for CMMC Level 1 is a binary selection between Yes and No based on meeting all Level 1 security requirements.

The CMMC Program verifies implementation of security requirements for FCI in accordance with FAR clause 52.204-21. The DoD has elected to use the CMMC Status postings and attestations in SPRS as the mechanism to verify compliance with applicable CMMC requirements.

An OSA engaging an authorized C3PAO to perform the Level 1 self-assessment and then using the resulting CMMC Status when "self-assessing" is permissible. The OSA however retains all the responsibilities and liabilities of the affirmation. No revisions to the rule were necessary.

Writing style recommendations were not incorporated and no responses were provided to those comments based on comparison of pre-publication draft versions with those officially published for public comment. DoD aligned the security requirements for Level 1 exactly with those in FAR clause 52.204-21 and aligned the security requirements in Level 2 exactly with those in NIST SP 800-171 R2. The 15 security requirements in FAR clause 52.204-21, which make up CMMC Level 1, were mapped by NIST into 17 security requirements in NIST SP

800171 R2. This was accomplished by splitting 1 requirement into 3 parts, while the other 14 align.
Table 2 to § 170.15(c)(1)(ii) provides a mapping.

Meeting the CMMC Level 2 self-assessment (§ 170.16) or CMMC Level 2 certification assessment (§ 170.17) requirements also satisfies the CMMC Level 1 self-assessment requirements detailed in § 170.15 for the same CMMC Assessment Scope. ***b. Level 2***

Comment: Commenters provided a number of very specific Level 2 assessment scenarios and asked for rule interpretation for each scenario. Scenarios included differing scores for selfassessment and third-party assessment; assessment timing; conditional assessment expiration; and CUI enclaves.

One commenter stated the language describing certificates of assessment lacked clarity and seems to allow an OSC to be issued a certificate of assessment but not be certified. Two comments stated that wording describing the expiration of a Conditional Level 2 self-assessment or certification could be interpreted to mean that the OSA/OSC would be permanently barred from seeking further contracts using information systems within that CMMC Assessment Scope. One comment said it was not clearly stated that a Level 2 third party assessment would satisfy contractual requirements for a Level 2 self-assessment. One comment stated that the rule does not clearly indicate whether a Level 2 assessment checks for more than just proper implementation of the 110 requirements in NIST SP 800-171 R2 and includes paragraphs – (c) through (g) of DFARS clause 252.204-7012. This commenter advocated that those requirements be assessed only during DIBCAC assessments.

Response: The rule has been updated to clarify that meeting the requirements for a CMMC Level 2 certification assessment satisfies a CMMC Level 2 self-assessment requirement for the same CMMC Assessment Scope.

The term "certificate of assessment" has been replaced with the term “Certificate of CMMC Status” in the final rule. When an OSC has met all the requirements for a Level 2 certification assessment, a Certificate of CMMC Status is obtained from the C3PAO conducting the assessment. See § 170.9. Under CMMC, OSCs are not certified; rather, the assessed network receives a Certificate of CMMC Status for the CMMC Assessment Scope if the network meets all applicable certification requirements. No rule edit is necessary because § 170.19 is clear on this point.

The phrase "until such time as a valid CMMC Level 2 self-assessment is achieved" is added to the rule in the event a Conditional Level 2 self-assessment or Conditional Level 3 expires [see sections §§ 170.16(a)(1)(ii)(B)) and 170.17(a)(1)(ii)(B)].
The CMMC program does not assess paragraph (c) through (g) of DFARS clause 252.204-7012. The CMMC Program assesses the security requirements set forth in the FAR clause 52.204-21; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 R2; and selected requirements from the NIST SP 800-172 Feb2021, as applicable (see table 1 to § 170.14(c)(4) CMMC Level 3 Requirements).

If the contract requires a Level 2 self-assessment (i.e., a CMMC Status of “Conditional/Final Level 2 (Self)”), then the Level 2 self-assessment score with a current affirmation is valid for that contract but not for a contract with a Level 2 certification assessment requirement. The DoD does not consider it realistic or likely that C3PAOs will purposefully “slow roll” completion of assessments for which they have been engaged by an OSC. However, the OSA’s CMMC Status is based on final results of an assessment and a valid affirmation. A POA&M Close-out assessment need only re-assess those requirements that were assessed as NOT MET in the original assessment as addressed in § 170.21(b). The OSA status is based on the results of this POA&M Close-out assessment with a valid affirmation. If the subcontractor will process, store, or transmit CUI, then the flow down requirement for a Prime contract that specifies CMMC Level 3 certification assessment is, at a minimum, CMMC Level 2 certification assessment (i.e., a CMMC Status of “Conditional/Final Level 2 (C3PAO)”).

A POA&M closeout applies to all NOT-MET requirements so if one practice is not remediated within the 180-day time limit, the conditional certification will expire. Scope cannot

be changed in the middle of an assessment, so the conditional certification will expire. If the scope is changed, a new assessment is required.

The assessment is performed based on the defined CMMC Assessment Scope. The OSA is only approved to process, store, or transmit FCI and CUI within the CMMC Assessment Scope defined.

If the conditional assessment certification expires due to exceeding the 180-day limit, a new full certification assessment is required. Contracting officers can utilize standard contract remedies during any period under which the OSA is not in compliance with CMMC requirements. If an OSC closed out their POA&M 32 months ago, that Level 2 Conditional certification assessment would have closed and the OSC would have received a Level 2 Final certification assessment for the remainder of the 3-year validity period. If after completing the Level 2 Final certification assessment, the OSC is reassessed and does not achieve a score of 110, then the OSC will either get a new Conditional Level 2 (C3PAO) CMMC Status certificate (if they meet the associated POA&M requirements), or the OSC will not receive a new certificate.

c. Level 3

Comment: Several comments addressed CMMC Level 3 assessment requirements and the relationship of Level 3 assessments to Level 2 assessments. One comment noted that a final version of the Level 3 assessment guidance was not available at the same time as other CMMC assessment guides. Another recommended the DoD first pilot implementation of CMMC Level 3 security requirements and clearly identify (in advance) the data or programs that will be subject to them. One commenter asked how DoD will maintain Level 3 requirements to align with NIST's guidance since Level 3 includes only a subset of NIST's SP 800-172 Feb2021 requirements.

Another asked about validating compliance for assets that changed asset categories when transitioning from Level 2 certification to Level 3 certification. One comment said it was that Level 2 certification is not clearly identified as a prerequisite for Level 3 certification, and that organizations might try to bypass Level 2. One comment asked whether those entities that would need a CMMC level 3 assessment could seek a combined Level 2 and Level 3 certification from the DIBCAC to reduce cost to the OSC.

One comment sought clarification of how long an OSC would be prohibited from seeking additional contract awards if a Level 3 certification expired. Two comments were concerned about the DIBCAC's ability to terminate a Level 3 assessment if the review identifies a Level 2 requirement that is not met.

Response: For CMMC Level 3, the DoD selected a subset of NIST SP 800-172 Feb2021 requirements for enhanced safeguarding. The CMMC Level 3 supplemental documents were not finalized prior to publication of the Proposed Rule. DoD's final determination of the specific subset of NIST SP 800-172 Feb2021 requirements is included in this final rule, which defines the ODPs for Level 3 in table 1 to § 170.14(c)(4). DoD will update the rule when required to change the security requirements, to include CMMC Level 3.

DoD has reviewed and declined the recommendation to conduct a pilot prior to phasing in CMMC Level 3 requirements. Given the evolving cybersecurity threat, DoD's best interests are served by ensuring that the selected CMMC Level 3 NIST SP 800-172 Feb2021 security requirements are in place to provide enhanced protections for sensitive DoD CUI.

In those cases when DCMA DIBCAC identifies that a Level 2 security requirement is NOT MET, DCMA DIBCAC may allow for remediation, place the assessment process on hold, or may immediately terminate the Level 3 assessment, depending on significance of the NOT MET security requirement(s) and the nature of the required remediation. The determination of whether a NOT MET requirement is significant is reserved for the judgment of the DCMA DIBCAC.

The rule has been updated to clarify that DCMA DIBCAC has the responsibility to validate compliance of all assets that changed asset category (i.e., CRMA to CUI Asset) or assessment requirements (i.e., Specialized Assets) between the Level 2 and Level 3 assessments. As

addressed in § 170.18, a condition to request a Level 3 certification assessment from DCMA DIBCAC is the receipt of a Final Level 2 (C3PAO) CMMC Status. The DoD considered, but declined, the recommendation to allow OSAs to simultaneously pursue Level 2 and Level 3 in one assessment. DoD must enforce CMMC requirements uniformly across the Defense Industrial Base for all contractors and subcontractors who process, store, or transmit CUI, regardless of an OSA's intended CMMC level. Permitting OSCs to seek combined CMMC Level 2 and 3 assessments would unfairly benefit only a subset of OSCs that were identified to meet CMMC Level 3 requirements.

The rule has been updated to clarify that the OSC will be ineligible for additional contract awards that require a CMMC Level 3 certification assessment until such time as a valid (Conditional or Final) CMMC Level 3 (DIBCAC) CMMC Status is achieved for the information systems within the CMMC Assessment Scope.

d. Scoring Methodology

1. CMMC Point Value System

Comment: Multiple comments were received concerning the point values assigned to CMMC security requirements, their association to other frameworks, consistency between CMMC levels, and their use in POA&M eligibility determination. Numerous comments recommended that the CMMC Level 2 weighted point system where security requirements are valued as 1, 3, or 5 be modeled after the one point per requirement used in CMMC Level 3 scoring. Some also questioned why the CMMC Level 2 scoring structure was the same as the NIST SP 800-171 DoD Assessment Methodology (DODAM). Four comments recommended changes to the criteria for adding unimplemented security requirements to an Assessment POA&M. One comment noted that temporary deficiencies which are appropriately addressed in plans of action should be assessed as implemented. Some of the comments recommended not assigning point values to determine POA&M eligibility. Two other comments recommended dropping the NIST Basic and Derived security requirement designations and disassociating them from CMMC point values.

Response: Recommendations to assign a point value of 1 to all CMMC Level 2 security requirements were not accepted. CMMC adopted the scoring as included in the NIST SP 800171 DoD Assessment Methodology (DoDAM) used by the DCMA DIBCAC and referenced in DFARS clause 252.204-7020. As addressed in § 170.20(a) in this rule, there is qualified standards acceptance between a DCMA DIBCAC High Assessment and CMMC Level 2 certification assessment. Revisions to the CMMC Scoring Methodology will be made concurrently with changes to the DoDAM. The variable point values of 1, 3, and 5 are linked to the NIST determination of Basic Security Requirements and Derived Security Requirements as described in § 170.24. The DoD has updated the rule text at § 170.24 to clarify which requirements may be included on a POA&M. CMMC Level 2 security requirement SC.L2–3.13.11 can be partially effective and may be included on a POA&M if encryption is employed and is not FIPS-validated.

The DoD added a definition for enduring exceptions and temporary deficiencies to the rule. § 170.21 addresses POA&Ms for assessments. Security requirement CA.L2-3.12.2 allows for the development and implementation of an operational plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. These operational plans of action are different from POA&Ms permitted under Conditional assessment. The rule has been updated to make this distinction clear. The CMMC rule does not prohibit the use of an operational plan of action to address necessary information system updates, patches, or reconfiguration as threats evolve.

2. NIST SP 800-171A Jun2018 Assessment Objectives

Comment: Multiple comments questioned the role of NIST SP 800-171A Jun2018 Assessment Objectives within the CMMC assessment process. Three comments asked whether all assessment objectives needed to be met to score a security requirement as MET. Two comments questioned the need to report assessment results at the assessment objective level within the CMMC instantiation of eMASS for CMMC Level 2 and CMMC Level 3 certification

assessments. Some comments suggested that the DoD allow for contractors to take a more riskbased approach to include compensating controls instead of a strict security requirement-based model.

Response: DoD must enforce CMMC requirements uniformly for all defense contractors and subcontractors who process, store, or transmit CUI. Each assessment objective in NIST SP 800-171A Jun2018 must yield a finding of MET or NOT APPLICABLE for the overall security requirement to be scored as MET. Assessors exercise judgment, within CMMC guidelines, in determining when sufficient and adequate evidence has been presented to make an assessment finding. A security requirement can be applicable, even with assessment objectives that are N/A. The security requirement is NOT MET when one or more applicable assessment objectives is NOT MET. CMMC assessments are conducted at the security requirement objective level, and the results are captured at the security requirement objective level. Assessment results are entered into the CMMC instantiation of eMASS at the NIST SP 800-171A Jun2018 assessment objective level of detail to provide metrics on which assessment objectives are proving difficult to implement and to indicate where additional assessor training and guidance may be warranted.

The DoD declines to change requirements to allow additional organization-specific riskbased approaches. National Institute of Standards and Technology (NIST) determined the appropriate characteristics and considered the appropriate attack vectors when NIST SP 800-171 R2 was created, and tailored the security requirements to protect the confidentiality of CUI. Questions and comments related to NIST SP 800-171 R2 background, development and scenarios are outside the scope of the CMMC rule.

3. Other Scoring Comments

Comment: Three comments were received concerning the use of operational plans of action to document security requirements which are not fully implemented due to limitations beyond the ability of an OSA to address. The use of temporary deficiencies and enduring exceptions were suggested along with the recommendation that these items be scored as MET.
The scoring of FIPS-validated modules was questioned in four comments. An error in the point value for encryption (1 and 3 points vs the correct 3 and 5 points) was identified. Clarification on full credit for incomplete implementation of FIPS encryption was also requested.

Two comments were received about the relationship between CMMC Level 2 and CMMC Level 3 scoring asking if the point values in each assessment were cumulative and how the 80% eligibility for an assessment POA&M and Conditional certification would be calculated. Three comments requested clarification around the use of N/A in security requirements, assessment objectives, and in matters pertaining to previously granted DoD CIO variances. One comment questioned what types of artifacts are required to substantiate a determination of N/A for a security requirement or assessment objective. Three comments addressed the need for a System Security Plan, its point value, if any, and the need for an SSP as a prerequisite for assessment as it exists in the DIBCAC DODAM.

Response: The government cannot comment on the suitability of specific implementations or products to meet CMMC security requirements and is aware that FIPS module validation can exceed the 180-day CMMC assessment POA&M threshold. Guidance regarding FIPS implementation on Windows 11 is not appropriate for inclusion in the rule text and DoD declines to make an update. Limitations of the FIPS-validated module process do not impact the implementation status of FIPS cryptography. The rule has been updated to include enduring exceptions and temporary deficiencies. Vendor limitations with respect to FIPS validation could be considered enduring exceptions or temporary deficiencies and should be addressed in an OSA's operational plan of action.

Several requirements within NIST SP 800-171 R2 specify the use of encryption without consideration of the processing, storage, or transmission of CUI. Requirement 3.13.11 requires that the encryption used be a FIPS-validated module if the encryption is used to protect the confidentiality of CUI. The scoring in § 170.24(c)(2)(i)(B)(4)(ii) is based on the use of encryption and whether the encryption uses a FIPS-validated module. There is no consideration for multiple layers of encryption so specific guidance to assessors regarding layers of encryption

is not needed and DoD declines to make the suggested addition. OSAs may choose how they implement security requirements and C3PAOs will assess based on the stated implementations. CCAs are trained in the correct process to assess security requirements. The DoD has updated the rule text at § 170.24(c) to clarify which requirements may be included on a POA&M, which addresses the error in the point value for encryption.

The scoring for CMMC Level 3 is separate from the scoring for CMMC Level 2. As stated in § 170.24(c)(3), the CMMC Level 3 assessment score is equal to the number of CMMC Level 3 security requirements that are assessed as MET. There are twenty-four CMMC Level 3 security requirements, identified in table 1 to § 170.14(c)(4). CMMC Level 3 POA&M eligibility is based on the number of CMMC Level 3 security requirements and does NOT include the 110 CMMC Level 2 requirements.

"Not applicable" was removed from § 170.24(c)(9) for the case where the DoD CIO previously approved a variance. The rule has been updated to reflect the language of DFARS clause 252.204-7012 and the DoDAM, including nonapplicable or to have an alternative, but equally effective, security measure. Regarding the comment on N/A objectives, § 170.23 is clear that MET means all applicable objectives for the requirement and that if an objective does not apply, then it is equivalent to being MET. A security requirement can be applicable, even with one or more objectives that are N/A. The overall requirement is only NOT MET when one or more applicable objectives is not satisfied. The determination of assessment findings is made by an Assessor following the assessment methodology. In the case of a self-assessment, the Assessor is from the OSA. In the case of a certification assessment, the Assessor is from the C3PAO or DIBCAC. An assessment finding of NOT APPLICABLE (N/A) means a security requirement (or assessment objective) does not apply at the time of the CMMC assessment. For each assessment objective or security requirement marked N/A, the Certified Assessor includes a statement that explains why it does not apply to the contractor. The OSC should document in its SSP why the security requirement does not apply and provide justification. There is no standard set of artifacts required to justify a finding of N/A.

A System Security Plan as described in security requirement CA.L2-3.12.4 is required to conduct an assessment. The rule has been updated at § 170.24(c)(2)(i)(B)(6) for clarity. Security requirement CA.L2-3.12.4 does not have an associated point value. The OSA will not receive a -1 for a missing or incomplete SSP. The absence of an up-to-date system security plan at the time of the assessment would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.' The rule has been updated in § 170.24(c)(6) to clarify this.

e. Artifacts

Comment: Several comments and requests for clarification dealt with artifacts that are reviewed or created during a CMMC assessment, or as part of compliance with other contractual requirements, including DFARS clause 252.204-7012. Some commenters asked whether standardized SSP and POA&M templates would be provided to assist with compliance. Other templates requested included pre-assessment planning materials, final assessment reports, and the resulting Certificate of CMMC Status.

Others expressed concern that sharing certain artifacts during the assessment process or permitting assessors to retain them would create vulnerability. In addition, commenters asked whether security protections are required for documents held due to the artifact retention requirements. One commenter asked how CMMC assessment scores, or affirmation information will be protected, and whether the CMMC program office will share this information outside of DoD. Another suggested that C3PAOs should not be required to retain any OSC provided materials.

One commenter misinterpreted the supplemental hashing guide as requiring use of the MS PowerShell script with the SHA256 algorithm. The commenter also stated it would be more efficient to specify a single hash be provided for combined artifacts rather than requiring separate hash values for each artifact. They recommended deletion of the hashing requirement. Another commenter suggested requiring OSCs to generate hashes for artifacts as part of a Level 2

selfassessment. One comment also asked whether hashing is required for Level 3 artifacts. One comment asked how long OSAs must retain artifacts following an assessment.
Some comments expressed concern that C3PAOs that receive or retain OSA artifacts identified as CUI would be required to undergo assessment by both the DIBCAC and another C3PAO. Four commenters objected to the 6-year artifact retention requirement for C3PAOs and requested reduction to 1 year. Three commenters asked whether self-assessors at level 1 or level 2 must also retain supporting artifacts for 6 years. Two commenters recommended revised wording of CMMC Level 3 requirements to provide greater clarity about artifact retention and integrity.

One commenter requested edits to the description of SSP content, advocating for deletion of references to organizational policies and procedures in place to comply with NIST SP 800-171 R2. The recommended edits also changed attribution of the requirement to create an SSP to reflect DFARS clause 252.204-7020 rather than DFARS clause 252.204-7012. This commenter also suggested additional wording to specify that the OSA need not define roles and responsibilities of security personnel in the SSP but may do so in ancillary documents.

Response: This rule retains the reference to DFARS clause 252.204-7012 that implements NIST SP 800-171 as the basis for the requirement to create and update an SSP. The DoD has considered the recommended changes to the rule regarding the SSP content and declines to make the revision. The NIST SP 800-171 R2 requirement for an SSP is foundational to performing a NIST SP 800-171 R2 self-assessment and its purpose is to provide critical information for performing the assessment. The SSP should detail the policies and procedures that support "...how security requirements are implemented..." for all NIST SP 800-171 R2 controls. DoD declines to establish a specific SSP format, as OSAs should define the best format for their organizations. The Overview section of the rule has been updated to remove the statement indicating SSPs will outline the roles and responsibilities of security personnel. DoD does not plan to provide document templates for SSPs and POA&Ms, as they are already available in existing NIST guidance. Templates and schemas for the pre-assessment and assessment results documents are available to authorized CMMC eMASS users at https://cmmc.emass.apps.mil.

Commenter concerns about artifact retention reflect misunderstanding of the assessment process. Assessors and C3PAOs do not retain OSC artifacts, they only retain the hash value captured during the assessment process. Assessors will retain documents created during the assessment such as their notes and the Assessment Findings Reports. To facilitate the protection of these documents, authorized C3PAOs are required to go through a DIBCAC conducted CMMC Level 2 assessment and CMMC Assessors are only authorized to use C3PAO issued equipment that was within the scope of the DIBCAC assessment. Separately, the DIBCAC processes, stores, and transmits its assessment related data on DoD networks. Assessment Reports are submitted to DoD via eMASS, which is a government-owned, secured database. Sharing of this information is subject to DoD policies.

The OSC is responsible for maintaining and hashing all artifacts that supported the assessment. The rule has been modified to clarify C3PAOs do not maintain artifacts from the OSC. The OSCs artifacts must be hashed, and the value provided to the assessor for submission into CMMC eMASS. That hash value contains no sensitive information. An OSC's System Security Plan (SSP) will be reviewed as part of a CMMC certification assessment, but not shared outside of the OSC. Assessors will not retain copies of the SSP or any other proprietary OSC information. Assessors will retain the name, date, and version of the SSP for uploading in SPRS or eMASS, as appropriate for the level of assessment. Assessors will upload assessment information (e.g., list of artifacts, hash of artifacts, and hashing algorithm used) into CMMC eMASS as addressed in § 170.9(b)(17), and the OSC will retain its assessment documentation as addressed in § 170.17(c)(4) and § 170.18(c)(4)

CMMC Level 2 self-assessments procedures as described in § 170.16(c)(1) require assessment in accordance with NIST SP 800-171A Jun2018, which if conducted properly will generate evidence. The rule has been modified to incorporate data retention requirements for self-assessments into §§ 170.15 and 170.16. OSAs are not required to generate hashes for selfassessment artifacts. Hashing is only required for Level 2 or Level 3 assessments by

C3PAOs and DCMA DIBCAC. The rule and Hashing Guide have been updated to add clarity that only a single hash is required, and that artifact retention is for six years. The use of SHA256 algorithm is not mandatory and therefore, the name of the hash algorithm needs to be stored in eMASS.

There are no additional requirements for artifact storage and retention beyond those identified in the rule. It is up to the OSA to determine the best way to ensure artifact availability during the six-year retention period. The rule has been updated in §§ 170.15 through 170.18 to clarify artifact retention requirements.

DoD declines to reduce the artifact retention period from six years to one year. The rule has been updated to clarify that all OSAs and Assessors are required to retain their respective assessment data for six years. The requirement for an artifact retention period of six years is a result of the Department of Justice's input to the proposed rule.

f. POA&Ms

Comment: Over forty comments were received about POA&Ms seeking clarification or revision to the rule content on that topic.

Several commenters misinterpreted the requirement to remediate or close POA&M items within 180 days as eliminating acceptability of operational plans of action for normal corrective actions such as patching or other routine maintenance activities, thus making the achievement of 100% compliance impossible. Some commenters requested rule revisions to describe operational plans of action in more detail. One commenter asked that the concept of Enduring Exceptions be added to the rule to address special circumstances when remediation and full compliance with CMMC security requirements is not feasible as described in the NIST SP 800-171A Jun2018 assessment methodology.

Several commenters expressed concern with the 180-day timeline to close out POA&Ms or limits on which practices can be placed on them. Recommendations for changing the POA&M timeline ranged from completely deleting the time limit to extending it by 1 to 3 years. One variation was to permit more than 180 days for closeout only during an initial one-year "rampup" period. One commenter encouraged DoD to reduce POA&M restrictions to facilitate contractors' genuine attempts to meet requirements and mitigate information security risks. Three commenters also thought the rule should allow contractors to request approval to delay POA&M close-out when meeting the original timeline is impracticable, while another commenter suggested defining the close-out timeline in the contract, allowing negotiation of extension or renewal of POA&Ms through the contracting officer. Two commenters asked when the 180-day timeline begins and one asked what actions occur if the POA&M is not closed out within that period.

Four commenters noted that the number of security requirements explicitly precluded from POA&Ms makes CMMC challenging and requested greater flexibility in how many, and which practices may be included. Three commenters recommended that companies be allowed to have any number of failed practices reassessed for up to six-months after an assessment without having to complete and pay for a new full assessment. Three other commenters recommended that the DoD allow for risk informed POA&Ms, while one stated that the rule should not specify which requirements must be met. One commenter requested clarification on how many items of each point value may be included on a POA&M for CMMC Level 2 conditional certification. One commenter also asked DoD to consider abandoning controls with high failure rates, lowering score requirements based on evidence of sufficient mitigation.

Several comments expressed concern that CMMC conditional certification does not allow higher weighted practices on a POA&M and recommended the rule reduce those restrictions to allow more security practices. One commenter also recommended eliminating weighting altogether, permitting any requirement to be part of the POA&M. As rationale, one commenter referenced DFARS clause 252.204-7012 verbiage that permits contractors to request DoD CIO approval to vary from NIST SP 800-171 requirements, saying that since all approved variances are considered as "Not Applicable", all requirements should be POA&M eligible.

Two commenters asked where POA&Ms are maintained, who is responsible for validating close-out, and whether affirmation is required after each assessment (including POA&M closeout). One commenter asked about applicability of the 180-day POA&M close-out requirement to Critical, High, Medium, or Low findings against Service Level Agreements.

One commenter recommended that a description of appropriate POA&M entries to be added to the rule and provided other recommended edits to the POA&M section, including addition of terms of art such as "assessment-related" and "non-assessment-related", and deletion of the words "as applicable."

Response: The CMMC Program allows the use of POA&Ms. Section 170.21 delineates the requirements that may be addressed as part of an assessment with a POA&M, that must be closed out by a POA&M closeout assessment within 180 days of the initial assessment to achieve the assessment requirement for Final certification. At Level 1, the OSA must affirm annually that it has reassessed its environment. Security requirement CA.L2-3.12.2 allows for the development and implementation of an operational plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. The CMMC rule does not prohibit an OSA from using an operational plan of action at any CMMC level to address necessary information system updates, patches, or reconfiguration as threats evolve. These are different from POA&Ms permitted under a Conditional certification assessment. The DoD has updated the rule to make this distinction clear. The Department also updated the rule to include a definition and clarity for enduring exceptions. The DoD CIO option for variances in DFARS clause 252.204-7012 is beyond the scope of this rule.

Operational plans of action are the appropriate mechanism to handle CSPs, ESPs (not a CSP) and third-party vendors that are no longer compliant with a CMMC requirement. Operational plans of action may be necessary when the relevant security requirement or control was fully implemented, but a vulnerability or deficiency is discovered after gaining a CMMC final compliance status, such as, but not limited to, routine updates, patches, or updates to CMMC compliance status. For purposes of CMMC compliance, operational plans of action are acceptable and are not subject to the 180-day timetable established for initial assessment. In addition, the rule has been modified to include a definition for Enduring Exceptions.

The DoD does not accept the recommendation to change the criteria for POA&Ms or the timeline allowed to remediate open POA&M items. The 180-day period allowed for POA&Ms and the determination of which weighted practices can be placed on a POA&M was a risk-based decision. The determination considers the relative risk DoD is willing to accept when a particular practice is not met and the amount of risk the DoD is willing to accept for those security practices that go "NOT MET" for an extended period. The DoD declined to edit the rule regarding the closeout of security requirements that are not allowed on the POA&M as stated in § 170.21. The decision in this scenario is a business decision between the applicable C3PAO and the OSC

Given the evolving cybersecurity threat, DoD's best interests are served by ensuring that POA&Ms remain open for no longer than 180 days, regardless of which controls are included or the plan for remediation.

The 180-day period starts when the CMMC assessment results are finalized and submitted to SPRS or eMASS, as appropriate. As addressed in §§ 170.17(a)(1)(ii)(B) and 170.18(a)(1)(ii)(B), if the POA&M is not closed out within the 180-day timeframe, the Conditional Certification will expire. If the Conditional Certification expires within the period of performance of a contract, standard contractual remedies will apply, and the OSC will be ineligible for additional awards with CMMC Level 2 or 3 requirements for the information systems within the same CMMC Assessment Scope. The scoring methodology created by the DoD reflects the relative risk to DoD information when a security requirement is NOT MET. As defined in § 170.17(c)(2), a security requirement that is NOT MET may be re-evaluated during the Level 2 certification assessment and for 10 business days following the active assessment period under certain conditions. Likewise, when an OSC executes a contract with a C3PAO it may account for the

timeliness of any re-assessments. The language in DFARS clause 252.204-7012 describing the DoD CIO's authority to approve variances is beyond the scope of this rule.
A POA&M for CMMC Level 2 can include up to 22 security requirements that have a value of 1, excluding those in § 170.21(a)(2)(iii), or may include non-FIPS-validated encryption and up to 19 security requirements that have a value of 1.

The OSA is responsible for maintaining the POA&M that resulted from a CMMC assessment; however, those security requirements that were NOT MET and placed on a POA&M are recorded in eMASS. The OSA is responsible for validating the close-out of the security requirements on the POA&M within 180 days of a self-assessment. The C3PAO or DCMA (as applicable) must perform the POA&M Close-out Assessment for a Final certification assessment. An affirmation of compliance is required upon the completion of any assessment - Conditional, Close-out, or Final - and annually after the completion of a Final assessment. The requirement outlined in § 170.21 for POA&M close out does not apply to Service Level Agreement (SLA) severity levels.

The Department declines to include recommended POA&M examples in the rule, as they are already available in existing NIST guidance, or make other word changes to § 170.21. This section of the CMMC rule has been updated to add clarity when discussing the POA&M regarding security requirements that were assessed as NOT MET during a CMMC assessment. These POA&Ms are distinct from an operational plan of action.

g. Assessment Activities and Reporting

1. Data Entry

Comment: One comment requested the rule state that records in SPRS must be updated within six months of the rule's effective date or when the functionality is in place, whichever is longer. Two comments asked for mitigations for assessment delays that could impact the timeliness of certification. One comment asked for more information about assessment frequency guidelines, and one asked which date would be used to determine timing of CMMC Level 2 triennial assessments, where this date is maintained, and who is responsible for ensuring contractors meet all applicable security requirements.

Response: To be eligible for a contract with a CMMC Level 1 self-assessment requirement, the OSA must perform a Level 1 self-assessment, input the result into SPRS, and submit an affirmation. The timeline for initiating and reporting a self- assessment is a business decision to be made by each contractor considering contract opportunities it wishes to pursue.
Because the OSA can fully control timelines for completion of self-assessments and plan for changes within the assessment scope, and because CMMC certification assessments occur on a standard 3-year cycle, the DoD expects that companies will plan assessments well in advance of need. The required assessment frequency is every year for CMMC Level 1, and every 3 years for CMMC Levels 2 and 3, or when changes within the CMMC Assessment Scope invalidate the assessment.

Certification dates for CMMC levels 2 and 3 are set to the date the certification assessment results are entered into SPRS for self-assessments or the date the Certificate of CMMC Status is entered into eMASS for third-party assessments. The triennial requirement renews on that date; there is no grace period. Each OSA's annual affirmation attests that they have implemented, and are maintaining their implementation of, the security requirements.

2. Supplier Risk Performance System and eMASS

Comment: Three commenters viewed CMMC's intent to store CMMC related data in an existing DoD system, SPRS, as an indication that SPRS would replace other DoD risk tracking systems or the risk monitoring responsibilities of other agencies. One commenter asked whether other Services would have their own systems, as the SPRS Program Office is within the Navy. Another comment stated CMMC and SPRS should not be tasked with the responsibility of addressing Supply Chain Risk Management (SCRM). One comment asked if the DoD intended to make CMMC Level 2 and 3 certification information available to other agencies, which could reduce the cost burden of compliance with assessment/certification programs adopted by other agencies. One comment asked how PII would be protected in SPRS. Another comment asked

for SPRS to be redesigned to list assessment results for each security requirement instead of the aggregate level. One comment asked for a CMMC-specific process for entering data into SPRS to make it easier for small businesses and another comment asked for vendor visibility into a potential sub-contractor's SPRS score.

Several comments asked about the CAGE code requirement and noted a perception that businesses outside the U.S are unable to obtain a CAGE or become a member of PIEE and therefore unable to access SPRS. One comment asked whether each contract would require a new SPRS entry.

One comment asked if OSCs that already have an eMASS account would be able to access the CMMC instantiation of eMASS and one comment questioned the cost/benefit of entering pre-assessment data into eMASS. Another comment asked for clarification on the roles and responsibilities of DoD Program Managers regarding the data uploaded into eMASS. One commenter suggested that eMASS be modified to permit tracking of self-assessment, in addition to certification assessments.

Response: SPRS is used to provide CMMC Status, score results, and affirmation status to contracting officers and program managers as part of the contract award process. It does not supersede other DoD program office risk register systems. SPRS will be used for reporting CMMC Status of all contractors, regardless of which service issued the contract. Although the SPRS program is managed by the Department of the Navy, its use spans across the Department. There is no role for other agencies associated with this CMMC rule, which applies only to DoD contractors that process, store, or transmit FCI or CUI. The CMMC PMO has no current agreements with other Federal agencies to share CMMC assessment results. There is nothing that prevents an OSA from sharing their CMMC Status with other entities.

SPRS is an existing DoD database that is compliant with DoD regulations, which includes meeting Privacy requirements. DoD suppliers are already required to use SPRS to record NIST SP 800-171 self-assessment scores, as referenced in DFARS clause 252.204-7020. The CMMC rule expands the use of SPRS to include CMMC Status, certification assessment scores, and affirmations.

SPRS is the tool that the DoD acquisition workforce will use to verify companies meet CMMC requirements to be eligible for contract award. SPRS data entry does not make available to Contracting Officers scoring of individual security requirements.
The DoD does not concur with granting prime contractors access to view the CMMC scores or Certificates of CMMC Status for potential subcontractors in SPRS. Subcontractors may voluntarily share their CMMC Status, assessment scores, or certificates to facilitate business teaming arrangements. Changing access to PIEE and SPRS is outside the scope of this rule.

CMMC eMASS is a tailored, stand-alone instantiation of eMASS for use by authorized representatives from C3PAOs, the DCMA DIBCAC, and the CMMC PMO. Individuals from each C3PAO will have access to CMMC eMASS to upload Level 2 assessment data. DCMA DIBCAC personnel will have access to CMMC eMASS to upload Level 3 assessment data. OSAs will not have access to CMMC eMASS. Authorized personnel from OSAs may access SPRS, which will host assessment certification and self-assessment data, and will be able to upload and view scores only for their OSA.

The DOD declines to add requirements for submitting self-assessments in eMASS. The requirement is for the OSA to enter scores into SPRS. There is value to the DoD in having the pre-assessment information in CMMC eMASS for overall program management and oversight. The information indicates that an assessment is either scheduled or in-process. The CMMC PMO seeks to track CMMC program adoption, and pre-assessment information allows reporting on upcoming assessments. Based on the DoD cost analysis, the effort to upload pre-assessment material is minimal.

DoD Program Managers are not responsible for uploading data into eMASS, nor do they have any responsibility regarding the data uploaded to eMASS by DCMA.An ESP, OSA, or OSC seeking CMMC assessment will need a CAGE code and an account in SPRS to complete the annual attestation required of all CMMC certified or CMMC compliant organizations.

An OSA/ OSC must obtain a CAGE code via https://sam.gov before registering in PIEE. Step by Step instructions for how to obtain an account can be found on the PIEE Vendor Account website: https://piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml. CAGE codes (or NCAGE codes for non-US-based companies) are also required. US-based contractors obtain a Commercial and Government Entity (CAGE) code from https://cage.dla.mil/Home/UsageAgree. Businesses outside of the US must obtain a NATO Commercial and Government Entity (NCAGE) code from https://eportal.nspa.nato.int/Codification/CageTool/home.

As specified in §§ 170.15 and 170.16, SPRS inputs include the industry CAGE codes(s) associated with the information system(s) addressed by the CMMC Assessment Scope. For each new information system used to support a DoD contract with FCI or CUI, a new SPRS entry is required. If the contractor or subcontractor will use an information system associated with a CAGE code already recorded in SPRS then a new entry is not required.

3. Assessors and Certificates

Comment: One commenter asked if an assessor is prohibited from interacting with OSA IT tools such as MS Office 365 or cloud based GRC tools. One commenter requested the CMMC rule require C3PAOs to clearly indicate the CMMC Assessment Scope on the CMMC Certificate of CMMC Status, to include CAGE codes, that could be shared with trusted partners.

Response: The rule text in § 170.11(b)(7) does not prohibit collecting assessment evidence within the OSC environment using the OSC's IT. This section applies only to IT used by the assessors to process, store, or transmit assessment-related information once it leaves the OSC environment. The rule has been modified to list the minimum required information to be included on the Certificate of CMMC Status, including CAGE code.

h. Reassessment

Comment: Some commenters interpreted the end of a CMMC assessment validity period (and need for new assessment) as having the same significance or meaning as a "reassessment", which the rule describes as potentially necessary only in rare circumstances when cybersecurity risks, threats, or awareness have changed.

Another commenter asked for examples of circumstances that might prompt a re-assessment and description of the process for completing one. Four commenters expressed concern that reassessments might be frequent, costly, and time-consuming. These commenters sought confirmation that relatively common system maintenance activities would not require a new assessment or prevent annual affirmation.

One commenter questioned the rationale for differences between validity periods for CMMC Level 1 versus Levels 2 and 3 assessment and recommended standardization on either a 1-year or 3-year frequency for all levels. Other commenters asserted that annual affirmations would drive a need for annual assessments at levels 2 or 3 and requested deletion of the affirmation requirement.

One commenter asked whether system changes within an assessment scope would require notification to the contracting agency. Another asked for guidance on remediation of POA&M items and asked whether systems that fall out of compliance must be identified to the contracting agency.

Response: The DoD considered duration of assessment validity periods and has chosen to require self-assessment of the basic Level 1 requirements every year, rather than every three years. Levels 2 and 3 require implementation of a significantly larger number of more complex security requirements, which require more time and attention to assess.

The DoD also declines to delete the annual affirmation requirement and does not agree that it equates to an annual assessment. The rule was modified to clarify that reassessments may be required based on post-assessment indicators of cybersecurity issues or non-compliance and are different from new assessments that occur when an assessment validity period expires. Reassessment is expected to be infrequent, conducted by the DoD, and necessary when cybersecurity risks, threats, or awareness have changed, or indicators of cybersecurity

deficiencies and/or non-compliance are present. When required, DCMA DIBCAC will initiate the re-assessment process using established procedures. The rule has been further updated to add this DCMA DIBCAC responsibility in § 170.7. OSCs seeking confirmation upon CMMC Level 2 POA&M close-out may undergo POA&M close-out assessment by a C3PAO, which is different from reassessment.

Self-assessments and certification assessments are valid for a defined CMMC Assessment Scope as outlined in § 170.19 CMMC Scoping. A new assessment is required if there are significant architectural or boundary changes to the previous CMMC Assessment Scope. Examples include, but are not limited to, expansions of networks or mergers and acquisitions. Operational changes within a CMMC Assessment Scope, such as adding or subtracting resources within the existing assessment boundary that follow the existing SSP do not require a new assessment, but rather are covered by the annual affirmations to the continuing compliance with requirements. The CMMC rule does not prohibit an OSA from using an operational plan of action at any CMMC Level to address necessary information system updates, patches, or reconfiguration as threats evolve.

If the CMMC Assessment Scope changes, then the current assessment is no longer valid and a new assessment is required. Requirements to notify the contracting agency of compliance changes are described in the 48 CFR part 204 CMMC Acquisition rule. An annual affirmation is required at each CMMC level.

16. CMMC Assessment Scoping Policy

Comment: One comment asked whether the requirements of DFARS clause 252.204-7012 apply to the entire contractor-owned information system, or only those components of the system that process, store, or transmit the CUI. Another questioned whether assets that process both FCI and CUI require CMMC Level 1 assessment.

One comment asserted that assessments described in DFARS provision 252.204-7019 and 7020 are scoped differently than CMMC assessments, and requested the rule be revised to avoid duplication with those assessments, where applicable. Another recommended that DoD determine scoping, boundaries, standards, and assessments based on CUI data rather than by systems.

One comment suggested that the rule be modified to address CMMC applicability to service providers that only provide temporary services, such as penetration testing, cyber incident response, or forensic analysis.

Response: OSAs determine the CMMC Assessment Scope based on how and where they will process, store, and transmit FCI and CUI. DoD has reviewed the suggested changes and declines to make any updates. Additional information for CMMC Scoping (§ 170.19) can be found in the relevant scoping guides. The applicability of DFARS clause 252.204-7012 requirements is not within the scope of this rule.

Meeting CMMC Level 2 self-assessment or certification assessment requirements also satisfies CMMC Level 1 self-assessment requirements for the same CMMC Assessment Scope. One commenter incorrectly assumes that CMMC asset categories drive a change to the assessment scope from what exists in DFARS clause 252.204-7012, which implements NIST SP 800-171 R2. No conflicts exist between the DFARS clause 252.204-7012 requirements and the CMMC requirements in this rule.

The DoD declines to change the rule to base scoping, boundaries, standards, or assessments solely on CUI data rather than on systems. The purpose of the CMMC Program is for contractors and subcontractors to demonstrate that FCI and CUI is adequately safeguarded through the methodology provided in the rule. The decision on what CMMC level is required for a contract is made by the Government after considering the nature of the planned effort, associated risks, and CUI to be shared. OSAs determine the CMMC Assessment Scope based on how and where they will process, store, and transmit FCI and CUI.

Service providers who only need temporary access to perform services such as penetration testing, cyber incident response, or forensic analysis do not meet the definition of an ESP in § 170.4 and do not process, store, or transmit CUI. Therefore, they are not within scope and the

DoD declines to modify the rule to include them.

17. CMMC Assessment Scope for ESPs

a. CMMC Applicability to ESPs

Comment: DoD received numerous comments about the implications of using an ESP while seeking to comply with CMMC requirements. Many comments were concerns that the ESP assessment requirements expanded the scope and cost of the CMMC program. Additionally, some comments described overarching concerns about applicability of CMMC requirements to an ESP when it only provided a Security Protection Asset or processed Security Protection Data. In general, commenters requested to narrow the rule while providing more clarity and definition related to CMMC requirements for ESPs and CSPs. Many comments gave either hypothetical or actual scenarios and asked whether the ESP in that scenario would be required to complete a CMMC assessment at the level required for the OSA being supported.

One comment suggested that ESPs should be treated the same as Risk Managed Assets. Another comment suggested that they be treated as Specialized Assets. Two comments proposed that DoD restrict DoD contractors to the use of an ESP/MSP/MSSP that is ISO/IEC 27001:2022(E) certified. Two comments suggest that OSA's be allowed to use non-certified or some form of conditionally certified ESPs if they retain the appropriate artifacts for review.

Response: The DoD has revised the rule to reduce the assessment burden on External Service Providers (ESP). ESP assessment, certification, and authorization requirements in §§ 170.19(c)(2) and (d)(2) have been updated. The use of an ESP, its relationship to the OSA, and the services provided need to be documented in the OSA's SSP and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSA and ESP with respect to the services provided.

ESPs that are CSPs, and process, store, or transmit CUI, must meet the FedRAMP requirements in DFARS clause 252.204-7012. ESPs that are CSPs and do NOT process, store, or transmit CUI, are not required to meet FedRAMP requirements in DFARS clause 252.204-7012. Services provided by the CSP are in the OSA's scope.

When ESPs that are not CSPs, process, store, or transmit CUI, a CMMC assessment is required to verify compliance with requirements for safeguarding CUI. Any ESP services used to meet OSA requirements are within the scope of the OSA's CMMC assessment.

When ESPs that are not CSPs do NOT process, store, or transmit CUI, they do not require CMMC assessment or certification, however, services they provide are in the OSA's assessment scope. There is nothing in the rule that precludes an ESP, that is not a CSP, from voluntarily requesting a C3PAO assessment. A C3PAO may perform such an assessment if the ESP makes that business decision.

ESPs can be part of the same corporate/organizational structure but still be external to the OSA such as a centralized Security Operations Center (SOC) or Network Operations Center (NOC) which supports multiple business units. The same requirements apply and are based on whether the ESP provides cloud services and whether the ESP processes, stores, or transmits CUI on their systems.

An ESP that is used as on-site staff augmentation only, i.e., the OSA provides all processes, technology, and facilities, does not need CMMC assessment. When ESPs are assessed as part of an OSA's assessment, the assessment type is dictated by the OSA's DoD contract CMMC requirement. The DoD declines to make any other suggested changes to the assessment of ESPs.

b. Definitions

Comment: Multiple comments state that the definition of CSP in the rule is overly broad and overlaps with the definition of ESP. One comment questioned whether a C3PAO is also a Security Protection Asset and by extension an ESP. Two comments requested change to the definition of Out-of-Scope Assets to stipulate that SPD is Out-of-Scope.

Response: Several comments requested clarification on when an ESP would be considered a CSP. CSPs, MSPs, and MSSPs are always considered ESPs. The DoD has updated the rule to narrow the definition of Cloud Service Provider based on the definition for cloud computing from NIST SP 800-145 Sept2011. An ESP would be considered a CSP when it provides its own

cloud services based on a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction on the part of the OSA.

An ESP (not a CSP) that provides technical support services to its clients would be considered an MSP. It does not host its own cloud platform offering. An ESP may utilize cloud offerings to deliver services to clients without being a CSP. An ESP that manages a third-party cloud service on behalf of an OSA would not be considered a CSP.

C3PAOs need not "receive" security protection data as part of an assessment; they view the security protection data while on premises at the OSC for the assessment. A C3PAO is not an ESP or security protection asset and is therefore not within the OSA assessment boundary. DoD declines to delete the phrase “except for assets that provide security protection for a CUI asset” from the definition of Out-of-Scope Assets. Assets that provide security protection for CUI are not Out-of-Scope Assets. A CMMC definition for Security Protection Data has been added to the rule.

c. OSA Relationship to ESP

Comment: Several comments request clarification related to use of an ESP that is internal to the OSA. One comment requested that DoD require CSPs grant the US Government, as part of the contract between the OSA and the CSP, access to any CUI that is subject to CMMC requirements in the event of contractual failures, criminal actions or other legal situations that warrant seizure of CUI data. Some comments also asked whether the DoD has standing or authority to require C3PAO assessment or conduct CMMC level 3 assessments of ESPs, given that the ESP’s direct contractual relationship is not with the Government but with the OSA. Two comments suggest that ESPs will be covered by the subcontractor flow down requirements from an OSA.

Response: DoD agrees with the need for added clarity around internal ESPs and the rule was modified to remove the term internal ESP. An ESP that provides staff augmentation, where the OSA provides all processes, technology, and facilities, does not need CMMC assessment. Alternatively, an ESP can be part of the same organizational structure but still be external to the OSA, such as a centralized SOC or NOC which supports multiple business units. The CMMC requirements apply and are based on whether the ESP provides cloud services and whether the ESP processes, stores, or transmits CUI on their systems.

The OSA’s contractual rights with its CSP are beyond the scope of this rule.
The rule states requirements for the OSA, not the ESP. The rule requires OSAs that process, store, or transmit FCI and CUI to protect that data. If those OSAs elect to use an ESP, and that ESP processes, stores, or transmits FCI or CUI from the OSA, then the OSA must require that the ESP protect the FCI and CUI and the ESP will be assessed as part of the OSA’s assessment or require FedRAMP Moderate or equivalent.

Specifically for Level 3, if an OSC is seeking Level 3 certification and uses an ESP that is not a CSP and that DOES process, store, or transmit CUI, then the ESP will need to be assessed by DIBCAC against the same Level 3 requirements as the OSC as part of the OSC’s assessment unless the ESP voluntarily seeks a DIBCAC Assessment. If an OSC is seeking Level 3 certification and uses an ESP that DOES NOT process, store, or transmit CUI, then the ESP will NOT need to be assessed by DIBCAC against the same Level 3 requirements as the OSC.
ESPs provide a service that meets the requirements specified by the OSA, and therefore ESPs are not subcontractors on a DoD contract and are not bound by subcontractor flow down requirements.

d. Assessment of ESPs

Comment: There were multiple comments regarding the assessment of an ESP. One comment recommends the rule be revised to identify the specific assessment requirements that would be considered NOT MET by the OSA when using a non-compliant ESP, and to further require C3PAOs to validate the OSCs use of compliant ESPs during a CMMC Level 2 assessment. One comment asks if an ESP, when assessed, will require a CAGE code, and enter scores into SPRS. Another comment asked whether CMMC certification would be required

when offering full IT management and online storage, including CUI, if the MSP policies prevent employees from accessing customer data.

One comment asks for clarification on the contents of the System Security Plan when documenting the use of an ESP. Two comments ask how to assess an OSA that is using a CSP to store CUI that does not meet the FedRAMP requirements. One comment asks how C3PAOs can check on the assessment status of an ESP. Three comments ask how to avoid redundant assessments of ESPs. One comment asks to clarify how to handle ESPs at Level 3 with respect to requirement AC.L3-3.1.2e that restricts access to systems that are owned, provisioned, or issued by the organization. One comment recommends DoD exempt CSPs that provide service with end-to-end encryption from CMMC requirements, similar to a common carrier.

Several comments inquired about guidelines and practices for obtaining Customer Responsibility Matrices (CRM) from CSPs and suggest the rule be modified to also require them from ESPs. One comment asks about how to obtain a CSP's System Security Plan.

Response: Implications for OSAs and C3PAOs for using non-compliant ESPs are adequately addressed in the rule. The CMMC compliance of an ESP, including a CSP, falls under the OSA's assessment. If an ESP is used to meet any of the CMMC requirements for the OSA, then the ESP is part of the scope of the OSA's assessment, and the compliance of the ESP will be verified.

An ESP that is seeking CMMC assessment will need to obtain a CAGE code and an account in SPRS to enable the reporting of its assessment results via CMMC eMASS. A SPRS account is required to complete the CMMC annual affirmation requirement included in DoD contracts that include a CMMC certification requirement.

An ESP that processes, stores, or transmits CUI, is an extension of the OSA's environment. As part of that environment, the ESP will be assessed against all requirements and accountable for all users who have access to CUI as part of the ESP's service, not just OSA employees. The government cannot comment on specific implementation or documentation choices of an OSA, including the use of an ESP.

The C3PAO can only give credit to a FedRAMP Moderate Authorized or equivalent CSP. Any requirements dependent on contributions from a CSP in any other stage of compliance are considered NOT MET. The requirements in the rule for FedRAMP Moderate equivalency have been updated to reflect DoD policy. OSAs can consider CSPs in the FedRAMP process for equivalency if they meet the requirements in DoD policy.

An ESP that is a CSP will be listed on the FedRAMP Marketplace. An ESP that is not a CSP and processes, stores, or transmits CUI will be within the OSA's assessment scope. An ESP can also volunteer to have a C3PAO assessment and could make that information available to the OSA.

ESPs that are not CSPs may request voluntary CMMC assessments of their environment and use that as a business discriminator. The marketplace for ESP services will adjust to find the efficient manner for ESPs to support OSA assessments that may include their services. With respect to requirement AC.L3-3.1.2e, when an OSA adds an ESP's services to its network, the ESP is considered to be provisioned by the OSA. It is subject to the requirements for the use of an ESP.

A common carrier's information system is not within the contractor's CMMC Assessment Scope if CUI is properly encrypted during transport across the common carrier's information system.

In a cloud model, the end-to-end encryption would apply when transmitting between OSA CUI assets and a cloud service. Once within the security boundary of the CSP, the common carrier's system no longer contributes to the handling of the CUI and the CSP's security practices apply. If an OSA chooses to use a CSP to process, store, or transmit CUI, FedRAMP Moderate or equivalency requirements apply.

The rule has been updated to include the use of a Customer Responsibility Matrix by all

ESPs, not just CSPs. Obtaining a copy of a CSP's SSP is not required for a CSP that is FedRAMP Authorized. Documentation on the services provided by the CSP and a CRM will be required.

e. Capacity for Assessment of ESPs

Comment: Some comments questioned whether the CMMC ecosystem would be adequate to provide the number of CMMC assessments necessary for ESPs. In response, some comments recommend ESPs be given priority for completing assessments. Others recommend different phasing or forms of assessment and certification during ramp up.

Response: DoD declines to make suggested changes to the ramp up and phasing of assessments for ESPs. DoD considered many alternatives before deciding upon the current CMMC assessment structure. By design, the CMMC program depends on the supply and demand dynamics of the free market, enabling it to naturally scale and adapt to capacity requirements. DoD declines to set priorities for the assessment marketplace. The DoD has utilized a phased implementation approach to reduce implementation risk. DoD expects that the public has utilized the lead-time prior to the publication of this rule to prepare for CMMC implementation and buy-down risk. CMMC Program requirements make no changes to existing policies for information security requirements implemented by the DoD. It is beyond the scope of this rule for DoD to determine the order in which organizations are assessed.

f. Remote Access by ESPs

Comment: Two comments ask for clarification on requirements for remote access by an ESP to an OSA, whether with OSA provided equipment or a VPN.

Response: The assessment of remote access may fall into several categories and is dependent on the specific architecture used and how the OSA creates its assessment environment. When an ESP is providing staff augmentation to the OSA and the OSA is providing all the systems used for remote access, then the OSA's policies and procedures apply and the ESP is not considered to be processing, storing, or transmitting CUI. When the ESP is using a Virtual Desktop solution, then the endpoint client device will be considered out of scope when it is configured to prevent storage, processing, or transmission of CUI on the end client beyond the Keyboard, Video, Mouse input that is part of the Virtual Desktop Infrastructure (VDI) solution.

Establishing a VPN connection with MSP equipment brings that equipment into the OSA's assessment scope. The equipment must meet the OSA's requirements for external access and connection to the network. Depending on the processing performed by the ESP with the VPN connection, other requirements may apply.

18. CMMC Assessment Scope for Security Protection Assets and Data

a. Scope and Authority

Comment: Multiple comments asserted that the use of Security Protection Data and Security Protection Assets increases the scope and cost of CMMC assessments and recommend changes to the costs or removing SPD and SPA from the rule. One comment presented the increased scope as an inconsistency between NARA and NIST SP 800-171A Jun2018. A few comments asked what authority DoD uses to include SPD as part of CMMC assessment.

Response: The commenter misread the rule's application to ESPs and SPA/SPD. Security Protection Assets are specified in NIST SP 800-171 R2 Sec 1.1 which states: "The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components." The rule has been updated in table 3 to § 170.19(c)(1) and table 5 to § 170.19(d)(1) to change the definition and requirements of Security Protection Assets. The phrase "irrespective of whether or not these assets process, store, or transmit CUI" has been removed from the SPA description and the CMMC assessment requirements have been changed to read "Assess against CMMC security requirements that are relevant to the capabilities provided." Similar changes were made to the guidance documents. In order to clarify and address concerns about the perceived "expansion" of requirements, the rule was revised to reflect that ESPs that only store SPD or provide an SPA and do not process, store, or transmit CUI do not require CMMC assessment or certification.

b. Definition and Requirements

Comment: Numerous comments requested that the DoD provide a definition for Security Protection Data (SPD) and configuration data, as well as requirements for SPD to help understand the scope of SPD and how that impacts the scope of Security Protection Assets and the assessment requirements of ESPs. One comment recommended the removal of the definition and use of SPD.

Multiple comments requested more information on the definition and scoping of Security Protection Assets, their relationship to CUI, and their requirements. Some comments suggested that the definition narrow the scope of Security Protection Assets and/or their security and assessment requirements. Other comments recommended eliminating the concept of SPA. Additional comments recommended changing the assessment requirements for SPAs to be the same as CRMAs Specialized Assets applicable NIST SP 800-171 R2 requirements, commensurate with the level of involvement with the security of CUI or to only assess the requirements provided by the SPA. Two comments recommended that the phrase" irrespective of whether these assets process, store, or transmit CUI" be removed from the definition of SPA.

Two comments asked for clarification on the requirements for CSPs that only handle SPD. Two comments recommended different security and assessment requirements for ESPs that host SPD but do not process, store, or transmit CUI.

Response: DoD added a CMMC definition for Security Protection Data to the rule. The DoD considered the NIST definitions for System Information and Security Relevant Information in the development of the CMMC definition for SPD.

This rule does not regulate OSA Security Protection Data, but instead implements existing regulatory requirements for the safeguarding of CUI, as defined in 32 CFR 2002.14(h)(2) and implemented by DFARS clause 252.204-7012. This clause requires protection of security protection assets and security protection data through its specification of NIST SP 800-171. DoD does not agree with the commentor's statement that the definition of Security Protection Assets "is an exceedingly dangerous adjustment to the NIST SP 800-171 Revision 2 Paragraph 1.1 Scope of Applicability." Security Protection Assets provide security to the entirety of an OSA's assessment scope which includes CUI Assets and other in-scope assets.

The SPD definition also defines configuration data as data required to operate a security protection asset. This limits the possible interpretations of configuration data. Further, the rule has been updated to reflect that ESPs that do NOT process, store, or transmit CUI do not require CMMC assessment or certification.

All assets within an OSA defined CMMC Level 2 or 3 assessment boundary have access to CUI and can process, store, or transmit CUI. They are therefore subject to DFARS clause 252.204-7012 and required to meet NIST SP 800-171 requirements. This is the authority for including Contractor Risk Managed Assets (CRMAs) within CMMC assessments. For Level 2, DoD has decided to assume some risk and lessen the assurance burden for a class of these assets called Contractor Risk Managed Assets, as specified in table 3 to § 170.19(c)(1). DoD does not assume this risk at Level 3. CRMAs are subject to assessment against all CMMC requirements as specified in table 5 to § 170.19(d)(1).

19. CMMC Assessment Scope and FedRAMP Moderate Equivalency Requirements

Comment: Several commenters identified inconsistencies between rule content and a separate DoD policy memo that defines requirements Cloud Service Providers (CSPs) must meet to be considered FedRAMP moderate "equivalent" in the context of DFARS clause 252.2047012. One commenter requested administrative changes to the rule for consistency, while others requested more substantive changes to deconflict the rule with DoD's policies. Differences between the two documents left some commenters unclear about when a CSP would be considered within a CMMC assessment scope or required to meet CMMC requirements. They also noted that some CSPs refuse to provide clients with Customer Responsibility Matrices (CRMs), which could impede an OSAs ability to meet CMMC requirements. One commenter asked for specific instances when a FedRAMP-moderate-authorized CSP would not be accepted as meeting CMMC requirements or which requirements such a CSP could not meet.

Another commenter stated the FedRAMP moderate equivalency requirements for CSPs in this rule will create confusion because they address only the NIST SP 800-171 requirements and do not include the additional cyber incident reporting requirements identified in DFARS clause 252.204-7012. One comment suggested that any expectation for CSPs to meet the DFARS clause 252.204-7012 requirements for cyber incident reporting or completion of a System Security Plan should be referenced in this CMMC rule. Another commenter suggested that all DoD contracts with CUI should include clauses and provisions for CSPs to meet Federal requirements, including a self-assessment and certification of their systems.

One commenter asked whether it is sufficient for MSP/MSSPs to have FedRAMP certification instead of CMMC certification. Another interpreted the rule's wording related to security protection assets and data as expanding requirements levied on CSPs.

One commenter interpreted CMMC Level 3 assessment requirements as meaning all parts of an OSCs infrastructure are within scope for CMMC assessment if the OSC uses a CSP, and recommended the rule specify that security requirements from the CRM must be documented in the SSP. Another asked whether OSCs must track all FedRAMP controls in their SSP or only those relevant to NIST SP 800-171 R2.

Response: Requirements associated with the use of cloud service providers (CSPs) are covered under section (b)(2)(ii)(D) of DFARS clause 252.204-7012. When a CSP is used, it must meet the requirements of the FedRAMP moderate baseline or the equivalent. The rule was updated for consistency with those requirements, and now requires FedRAMP moderate or FedRAMP moderate equivalency as defined in DoD Policy.

§§ 170.16(c)(2), 170.17(c)(5), 170.18(c)(5) address CMMC requirements for CSPs. The CMMC rule does not add new requirements on the use of CSPs, which are found in DFARS clause 252.204-7012. A CSP must be assessed against the FedRAMP moderate baseline when the CSP processes, stores, or transmits CUI. The CMMC rule does not oppose or contradict the requirements of DFARS clause 252.204-7012, nor does this rule relieve a CSP from any requirement defined in DFARS clause 252.204-7012.

§ 170.17(c)(5)(iii) and the corresponding requirement in § 170.18(c)(5)(iii) only apply to CSPs used to process, store, or transmit CUI in the execution of the contract or subcontract requiring CMMC assessment. It does not expand to any cloud provider outside the scope of the assessment. Interactions between DoD contractors and their service providers are beyond the scope of the rule.

CMMC Level 2 self-assessment and affirmation requirements described in § 170.16 make clear that an OSA using a FedRAMP Authorized CSP (at the FedRAMP Moderate or higher baseline) is not responsible for the CSP's compliance. The OSA needs to document in its SSP how the OSA meets its requirements assigned in the CSP's CRM. When using a CSP that is not FedRAMP Authorized, the OSA is responsible for determining if the CSP meets the requirements for FedRAMP Moderate equivalency as specified in DoD policy. In this case, the OSA also needs to document in its SSP how the OSA meets the requirements assigned to it in the CSP's CRM.

The rule has been updated to include verbiage from the DFARS clause 252.204-7012 "in the performance of a contract" for consistency. Use of the term CUI in this rule is deliberate because DoD intends to assess compliance with NIST SP 800-171 R2 for all CUI. The DoD declines to replace the word CUI with the word CDI, as the term CUI more clearly conveys that NIST SP 800-171 is the requirement for all CUI information, as described in 32 CFR 2002.14.

DoD received numerous comments about the use of ESPs which do not process, store, or transmit CUI. In response to comments, the DoD has reduced the assessment burden on ESPs. ESP assessment, certification, and authorization requirements in §§ 170.19(c)(2) and (d)(2) have been updated.

20. CMMC Assessment Scope for Devices and Asset Categorization

a. Asset Categorization

Comment: There were many comments regarding the scoping and treatment of assets when using table 3 to § 170.19(c)(1) and table 5 to § 170.19(d)(1). Several comments asked about

when asset categorization occurs, who approves it and how to document it. Two comments questioned the applicability of using NIST SP 800-171 R2 for Specialized Assets. Two comments suggested modifying the definition of Out-of-Scope assets by removing the last bullet or discussing the use of encryption. One commenter suggested adding more detailed definitions of the asset categories to the rule. One comment recommended removing asset categories from the rule.

Many comments requested scoping and categorization of specific scenarios, such as ERP systems, MRP systems, quantum computing systems, data diodes, asset isolation, and encrypted CUI. Numerous additional comments requested clarification on scoping and categorization of various security product classes.

Response: The OSA performs asset categorization and documents it in their SSP. The OSA may choose the format and content of its SSP. Table 3 to § 170.19(c)(1) requires that all asset categories, including Specialized Assets, be included in the asset inventory. There is no requirement to embed every asset in the SSP. In the SSP for Level 2, the OSA must show how Specialized Assets are managed using the contractor's risk-based security policies, procedures, and practices. Prior to the conduct of an assessment, the OSC engages with the C3PAO assessor. It is during this time that the classification of assets should be agreed upon, and the results of these discussions are documented in pre-planning materials. This is an example of the preassessment and planning material submitted by the C3PAO as required in § 170.9(b)(8) and the CMMC Assessment Scope submitted to eMASS as required in § 170.17(a)(i)(D). It is beyond the scope of this rule to address DoD review of specific Specialized Assets for individual contractors.

DoD does not agree with a commentor's statement that Specialized Assets are not actually assessed against CMMC security requirements. As documented in § 170.19, Specialized Assets are identified by the OSC. Assessment requirements of Specialized Assets differ between CMMC Level 2 and CMMC Level 3. If Specialized Assets are part of a CMMC Level 2 assessment, the OSA must document them in the asset inventory, document them in the SSP, and show how these assets are managed using the contractor's risk-based security policies, procedures, and practices. If Specialized Assets are part of a CMMC Level 3 assessment, they must be assessed against all CMMC Level 2 security requirements and CMMC Level 3 security requirements, identified in § 170.14(c)(4).

DoD agrees with one comment that even if NIST SP 800-171 R2 cannot be implemented, that does not mean the Specialized Assets cannot be secured. CMMC requirements are defined to align directly to NIST SP 800-171 R2 and NIST SP 800-172 Feb2021 requirements. For additional ease of burden, at Level 1, IoT and OT are not in scope, at Level 2 there are reduced requirements, but they become in-scope at Level 3, unless they are physically or logically isolated.

DoD has reviewed the text and declines to change the definition of Out-of-scope assets because CUI should not be transmitted via clear-text per NIST SP 800-171 R2. The DoD has reviewed the suggested changes to asset categories and scoping tables and declines to make an update. The asset categories in the rule help the OSA understand the requirements of various asset types that might be found within the assessment boundary.

OSAs determine the asset categories and assessment scope based on how and where they will process, store, and transmit FCI and CUI. DoD cannot comment on the suitability of any specific approach or technology to successfully implement CMMC security requirements.

b. Virtual Desktop Infrastructure

Comment: Several comments requested clarification on the use of Virtual Desktop Infrastructures and how to scope its components.

Response: The rule has been updated in table 3 to § 170.19(c)(1) and table 5 to § 170.19(d)(1) to state that an endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of FCI and CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered out of scope.

c. Contractor Risk Managed Assets

Comment: There were numerous comments regarding Contractor Risk Managed Assets. Several comments perceived conflicts in the changes between the current rule and previous intermediate documents regarding CRMA requirements. Multiple comments recommended additional details explaining risk-based management of assets. Two comments requested additional details on the limited checks that are permitted during assessment of CRMAs. Multiple comments requested clarification on CRMA requirements at Level 3 for the OSA and ESP. One comment requested clarification about the documentation requirements for CRMAs.

One comment asserted that the rule co-mingled CRMAs with assets of an ESP. One comment questioned why CRMAs were being included as in-scope assets subject to CMMC security requirements. One comment asked for clarification between the security requirements and assessment requirements for CRMAs.

Response: There was confusion and concern over conflicts from commenters regarding responses to comments on a previous version of the rule, other documentation, and the current rule. The DoD did not find any conflicting language around CRMAs. There is no conflict between CRMAs and the requirements for logical or physical boundaries. CRMAs are only applicable within the CMMC Assessment Scope. DoD does not agree with the statement that the wording change around Contractor Risk Managed Asset (CRMA) effectively makes the asset category moot.

The CRMA category was created to ease the assessment burden, based on the Department's risk tolerance. It is not intended to reduce the level of protection and the CMMC security requirements which apply to the assets.

Despite the wording changes identified by the commentor, the CMMC security requirements and the assessor's ability to conduct a limited check to identify deficiencies as addressed in table 3 to § 170.19(c)(1) are unchanged.

Contractor Risk Managed Assets (CRMA) should be prepared to be assessed against CMMC security requirements at Level 2, and included in the SSP, asset inventory, and network diagrams.

Table 3 to § 170.19(c)(1) clearly addresses the assessment requirements for Contractor Risk Managed Assets. All CMMC security requirements must be MET when the OSA chooses to designate certain assets as Contractor Risk Managed Assets.

Eight guidance documents for the CMMC Program are listed in Appendix A to Part 170—Guidance. These documents provide additional guidance for the CMMC model, assessments, scoping, and hashing. Use of the guidance documents is optional.

The OSA is responsible for determining its CMMC Assessment Scope and its relationship to security domains. Assets are out-of-scope when they are physically or logically separated from the assessment scope. Contractor Risk Managed Assets are only applicable within the OSA's assessment scope. Table 3 to § 170.19(c)(1) is used to identify the asset categories within the assessment scope and the associated requirements for each asset category. Contractor's riskbased security policies, procedures, and practices are not used to define the scope of the assessment, they are descriptive of the types of documents an assessor will use to meet the CMMC assessment requirements.

It is beyond the scope of the CMMC rule to provide a detailed explanation of the usage of "risk-based" terminology when implementing or assessing CMMC requirements. DoD declines to speculate and clarify the relationship between any NIST SP 800-171 R2 definitions and any pending NIST SP 800-171 Revision 3 definitions.

The DoD has defined the effort allowed during a limited check in table 1 to 170.19(c)(1). A limited check may require submission of evidence.

The DoD cannot anticipate how an OSC will scope its CMMC Level 3 assessment with respect to its CMMC Level 2 environment. As specified in table 5 to § 170.19(d)(1), Level 2 Contractor Risk Managed Assets are categorized as CUI Assets at Level 3.

The rule has been updated to clarify that ESPs do not require a Level 3 certification unless they process, store, or transmit CUI in the performance of a contract with a CMMC Level 3 requirement.

3 As stated in table 1 to § 170.19(c)(1), CRMA assets must be prepared to be assessed against CMMC requirements. The SSP must provide sufficient documentation describing how security requirements are met to allow the assessor to follow the instruction in table 1 to not assess against other requirements. The assessor will then decide if a limited spot check is warranted. The results of the limited spot check can result in a requirement being scored as NOT MET.

The rule does not create two classes of Contractor Risk Managed Assets as one commenter asserts. Contractor Risk Managed Assets are only those assets that are owned by the OSC and within the assessment scope. ESP assets are subject to the ESP requirements of the rule. All assets within the OSA defined assessment boundary have access to CUI and can process, store, or transmit CUI, and are therefore subject to DFARS clause 252.204-7012 and required to meet NIST SP 800-171 requirements. This is the authority for including CRMAs within CMMC assessments. For Level 2, DoD has decided to assume some risk and lessen the assurance burden for a class of these assets called Contractor Risk Managed Assets, as specified in table 3 to § 170.19(c)(1). DoD does not assume this risk at Level 3. Contractor Risk Managed Assets are subject to assessment against all CMMC requirements as specified in table 5 to § 170.19(d)(1).

At CMMC Level 2, Contractor Risk Managed Assets and Specialized Assets are assessed differently. Both types of assets must be documented in the SSPs; Specialized Assets will not, however, be assessed by the C3PAO while limited checks may be performed on Contractor Risk Managed Assets. OSCs should be prepared for assessment of Contractor Risk Managed Assets because a deeper assessment will be done if the assessor's evaluation of the OSC's policies and procedures raise questions. However, at Level 3, Contractor Risk Managed Assets and Specialized Assets are assessed, like CUI assets, against all CMMC security requirements, so no additional explanation is required.

d. Specialized Assets

Comment: There were numerous comments regarding Specialized Assets. Several comments discuss the use of enduring exceptions for Specialized Assets and the use of the term in NIST SP 800-171 R2. Two comments confuse the current rule with responses to a previous version of the rule. A comment requests clarification why specialized assets are not CUI assets. Another comment asks about the difference in assessment requirements between CRMAs and Specialized assets. One comment requested processes and best practices for evaluation of specialized assets.

Two comments recommend that the Specialized asset requirements for Level 3 remain the same as Level 2 due to the difficulty of meeting the Level 3 requirements in a manufacturing environment. Two comments request additional clarification on the Level 2 assessment of Specialized assets when the assessment is a precursor to a Level 3 assessment.

Response: Definitions for enduring exceptions and temporary deficiencies have been added to the rule. Specialized Assets are a type of enduring exception and cover a broad range of circumstances and system types that may not be able to be fully secured as described in NIST SP 800-171 R2. It does not give an OSA the flexibility to broadly categorize assets as Specialized Assets.

The OSA would be expected to address asset categorization with a C3PAO during the initial scoping discussion to avoid disagreements during the assessment process.

In one example provided, a single asset which is unable to meet a single security requirement would be a temporary deficiency and be addressed using an operational plan of action, describing the cause with appropriate mitigation and remediation identified.

The sentence "NIST SP 800-171 Rev 2 uses the term "enduring exceptions" to describe how to handle exceptions for Specialized Assets" appears in answers to public comments on a previous version of the rule, which responded to the initial CMMC Program requirements, therefore the inclusion of the sentence is not relevant to the rule.

One commenter has misinterpreted the answer to a public comment on a previous version of the rule, which responded to the initial CMMC Program requirements. Specialized Assets are

not evaluated at Level 1. Specialized Assets at Level 2 need to be documented in the SSP and included in the asset inventory and network diagrams. They also are to be managed using the contractor's risk-based security policies, procedures, and practices.

At Level 2, Specialized Assets do not need to be assessed against other CMMC security requirements. At Level 3, Specialized Assets should be prepared to be assessed against CMMC security requirements. CMMC also provides for the use of intermediary devices to safeguard OT and IOT devices that otherwise would be difficult or expensive to protect. The phrase "or information systems not logically or physically isolated from all such systems" only appears in answers to public comments on the original 48 CFR CMMC interim final rule publication, therefore the inclusion of the phrase is not relevant to the rule.

Specialized Assets span a broad spectrum of components and have different limitations on the application of security controls. Processes and practices to implement and assess security requirements on these devices are outside the scope of the CMMC rule.

The Level 3 assessment is designed to provide additional safeguards to protect the most sensitive CUI against advanced persistent threats (APTs). DoD estimates that only one percent of defense contractors will require a CMMC Level 3 assessment. DoD has judged that the risks associated with the exposure of this CUI are sufficient to justify the increased cost of a Level 3 assessment on the small percentage of the DIB that is processing, storing, or transmitting this type of data.

CMMC also provides for the use of intermediary devices to safeguard OT and IOT devices that otherwise would be difficult or expensive to protect. This difference between how a Specialized Asset is assessed at Level 2 and Level 3 is risk-based and affords a reduction in cost for a Level 2 certification. The CMMC Assessment Scope for a CMMC Level 2 certification assessment is discussed between the OSC and the C3PAO. If the OSC has a goal to undergo a CMMC Level 3 certification assessment for the same assessment scope, it may be good business practice for the OSC to disclose this information to the C3PAO and be assessed based on the Level 3 scoping, however this is not required.

e. Intermediary Devices

Comment: One comment asks for additional information on intermediary devices as referenced in table 5 to § 170.19(d)(1). Another comment asks for direction in situations where the comment asserts intermediary devices are not practical.

Response: An intermediary device is used in conjunction with a specialized asset to provide the capability to meet one or more of the CMMC security requirements. For example, such a device could be a boundary device or a proxy, depending on which requirements are being met. The rule is agnostic as to how many requirements are met and what technology is used to meet them. Implementation guidance for OT/IOT/IIOT is outside the scope of the CMMC rule.

21. CMMC Assessment Scope for Enterprise versus Segmented Environments

Comment: Two commenters sought guidance for segmented networks that inherit some controls from an enterprise network that has a valid CMMC certification, and asked whether certification assessments may be shared between the networks.

Response: § 170.19 states that prior to a CMMC assessment, the OSA must define the CMMC Assessment Scope for the assessment, representing the boundary with which the CMMC assessment will be associated. Any CMMC certification granted applies only to the assessed CMMC Assessment Scope. An enclave may be able to leverage some elements of the enterprise assessment by inheriting some requirements from the enterprise network, but it cannot inherit the enterprise certification. Enclaves beyond the certified CMMC Assessment Scope must be assessed separately based on their own CMMC Assessment Scope.

There is no established metric for inherited implementations from an enterprise to any defined enclaves. The OSA determines the architecture that best meets its business needs and complies with CMMC requirements. Within the enclave, the OSA determines which requirements are implemented and which requirements are inherited; all requirements must be MET. If a process, policy, tool, or technology within the enclave would invalidate an implementation at the Enterprise level, that requirement cannot be inherited and the OSA must

demonstrate that it is MET by implementation in some other way. Additional guidance related to assessments and enclaves has been added to the CMMC Scoping Guide Level 2 and Level 3.

22. Revocations and Appeals Process

Comment: One comment asked for more clarification regarding the granting and revoking of interim validity status for a CMMC assessment. Several comments requested an appeal and remediation process if a CMMC assessment status is revoked by the DoD. One comment requested that the revocation process not be arbitrary or capricious and provide for due process. And one comment recommended removing the word "maintained" from the criteria for revocation of the validity status because maintenance is part of ongoing operations as specified in the security requirement for Risk Assessments and Continuous Monitoring (CA.L2-3.12.2). One commenter asked whether SPRS reporting is the only mechanism in place to ensure that OSAs maintain the SSP and conduct self-assessments correctly.

Three comments recommended that the DoD or CMMC PMO have a role in the assessment appeals process. Of these, one cited the DFARS clause 252.204-7012 clause as precedent for DoD CIO to render final decisions. Some commenters suggested the CMMC AB relationship to C3PAOs would bias any decisions they may make, and that final appeal authority is an inherently governmental risk acceptance decision. One comment suggested that the DIBCAC or other DoD entity render final appeals decisions or take responsibility for certifying OSCs. They also asked for the C3PAOs to be released from liability for reasonable assessment judgments. Two comments asked whether the only means to appeal a CMMC AB final decision is through litigation. Another comment asked who could escalate an appeal to the CMMC AB. One comment requested the rule include more requirements for the C3PAO appeals process, including that the process be time bound and address disputes related to perceived assessor errors, malfeasance, and unethical conduct, while another comment requested a simpler appeals process. One comment requested clarification as to how the OSC interfaces with the C3PAO for appeals purposes. One comment asked if there was a process to challenge C3PAOs' findings of non-compliance if additional requirements are applied from an assessment guide that are not included in the source standard. One comment asked how to dispute the specific CMMC level included in a solicitation.

Response: Requirements for CMMC Conditional certification assessments for each level are defined in §§ 170.16 through 170.18. Section 170.6(e) describes indications that may trigger investigative evaluations of an OSA's CMMC Status. The DoD has revised the rule throughout to delete the term "revocation" and to clarify that the DoD reserves its right to conduct a DCMA DIBCAC assessment of the OSA, as permitted under DFARS clause 252.204-7012 and DFARS clause 252.204-7020. If the results of a subsequent DIBCAC assessment show that adherence to provisions of this rule have not been achieved or maintained, the DIBCAC results take precedence over any pre-existing CMMC self-assessment(s) or Final certification assessment(s) and will result in SPRS reflecting that the OSA is not in compliance (i.e., lacks a current Certificate of CMMC Status). There are no additional requirements or checks on selfassessments to ensure that OSAs maintain the SSP and conduct self-assessments correctly, beyond those identified in the rule.

One commenter misunderstood the meaning of 'maintained' with respect to the Level 1, 2, and 3 provisions. An operational plan of action can be created without risk to the certification validity period. If a security event generates risk for the protection of FCI or CUI, the associated security requirements should be readdressed expeditiously. If one or more of the requirements can't be remediated, the OSA should create an operational plan of action and resolve it in a time frame that continues to provide protection to FCI or CUI.

The Accreditation Body must have its own appeals process, as required under ISO/IEC 17011:2017(E). Each C3PAO is required to have an appeals process which involves elevation to the CMMC Accreditation Body for resolution. The appeals process is derived from and consistent with ISO/IEC 17020:2012(E) and ISO/IEC 17011:2017(E). The appeals process is addressed in §§ 170.7(b), 170.8(b)(16), and 170.9(b)(13), (19), and (20). An OSC, the CMMC

AB, or a C3PAO may appeal the outcome of its DCMA DIBCAC conducted assessment within 21 days of the assessment by submitting a written basis for appeal that include the requirements in question for DCMA DIBCAC consideration. An OSC, the CMMC AB, or a C3PAO should visit www.dcma.mil/DIBCAC to obtain the latest for contact information for submitting appeals. A DCMA DIBCAC Quality Assurance Review Team will respond to acknowledge receipt of the appeal and may request additional supporting documentation.

By defining the requirements in this rule to become a C3PAO, and defining a scoring methodology, the DoD is providing the authority and guidance necessary for C3PAOs to conduct assessments. The CMMC Accreditation Body will administer the CMMC Ecosystem. The DoD will not assume the workload of directly managing the CMMC ecosystem or the other alternatives suggested. DoD declines to give the PMO responsibility to render the final decision on all CMMC Level 2 assessment appeals as this role is properly aligned to the CMMC Accreditation Body. The CMMC AB is under contract with the Department of Defense to execute defined roles and responsibilities for the DoD CMMC Program as outlined in § 170.8. The specified CMMC AB requirements were selected and approved by the DoD. They include Conflict of Interest, Code of Professional Conduct, and Ethics policies as set forth in the DoD contract.

For ISO/IEC 17020:2012(E) and ISO/IEC 17011:2017(E) compliance, an appeals process is required. CMMC-specific requirements for appeals are addressed in §§ 170.8(b)(16) and 170.9(b)(13), (19), and (20). The DoD expects the process to be managed efficiently, however setting a specific timeline is not appropriate as the time may vary based on the complexity of the issue.

Responsibility for final appeals determination rests with the CMMC AB. The DoD declines to mandate that the CMMC AB consult with the CMMC PMO or DIBCAC prior to rendering a decision. The CMMC PMO will serve in the oversight role for the entire CMMC program. OSCs may submit any appeal arising from CMMC Level 2 assessment activities to C3PAOs as addressed in § 170.9(b)(19). OSCs may request a copy of the process from their C3PAO. The rule has been revised to reflect that any dispute over assessment findings which cannot be resolved by the C3PAO may be escalated to the CMMC AB by either the C3PAO or the OSC. The decision rendered by the CMMC AB will be final as stated in § 170.8(b)(16). Appeals pertaining to an assessor's professional conduct that is not resolved with the C3PAO will also be escalated and resolved by the CMMC AB.

As addressed in § 170.9(b)(13), the C3PAO will have a quality assurance individual responsible for managing the appeals process in accordance with ISO/IEC 17020:2012(E) and ISO/IEC 17011:2017(E). Identification of the C3PAO staff that an OSC should interface with is beyond the scope of this rule. It is a business decision that may vary by C3PAO and should be addressed between the OSC and C3PAO prior to conduct of an assessment.

The supplemental documents listed in Appendix A provide additional guidance to aid in CMMC implementation and are not authoritative. In the event of conflicts with the security requirements incorporated by reference, this rule and NIST SP 800-171A Jun2018 or NIST SP 800-172A Mar2022 guidance will always take precedence. Disputes regarding the CMMC level specified in a contract solicitation should be addressed with the contracting officer using normal pre-award or post-award communications processes. No revision to the rule is required. Selection of the CMMC level is a DoD risk-based decision made by the Program Manager or Requiring Activity.

23. CMMC Cybersecurity Requirements

a. NIST SP 800-171 R2 Requirements

Comment: Several comments were received regarding FIPS-validated cryptography. Some recommended mitigating delays with FIPS validation testing and reducing the risk of CMMC assessment failures by allowing FIPS POA&Ms or POA&M extensions, waivers, or making encryption an organizationally defined parameter (ODP). Similarly, some recommended the DoD accept alternate FIPS solutions such as commercially viable modules with FIPS-approved protocols or FIPS-compliant—as opposed to FIPS-validated—protocols. One comment

recommended that DoD collaborate with NIST to either improve the processing of FIPS validation testing and/or to define the encryption ODP for NIST SP 800-171 Revision 3. One comment recommended DoD work with NIST to align NIST ODPs in NIST SP 800-171 Revision 3 to DoD ODPs defined in the CMMC Rule for CMMC Level 3 to ensure consistency. Another commenter asked if FIPS 140-3 was an acceptable FIPS implementation.

Multiple comments addressed NIST requirements. One comment stated the NIST cybersecurity standards and guidelines are not legal requirements. The commenter recommended edits to the CMMC rule to require contractors implement requirements "derived" from NIST SP 800-171 R2 with measurable specifications to protect CUI. Two commentors felt the body of the proposed rule should have included a list of the NIST requirements to be assessed at each CMMC level. One comment suggested clarifying when a Systems Security Plan is required for each level. And, one asked if the CMMC Assessment Scope and attestation requirements included Non-Federal Organization (NFO) controls or the flow-down and reporting requirements from DFARS clause 252.204-7012.

Some comments were speculative in nature and outside the scope of the rule. One commenter was concerned that a CMMC assessment would not address the risk of insider threats and national security problems driven by political divisions within Congress.

Response: DoD is aware of industry concerns regarding FIPS validation required in NIST SP 800-171 R2 requirement 3.13.11. Because this is a NIST requirement, changing it is beyond the scope of the CMMC rule. As stated in § 170.5(3), the CMMC Program does not alter any separately applicable requirements to protect FCI or CUI, including the requirement to use FIPSvalidated cryptography which comes from NIST SP 800-171 as required by DFARS clause 252.204-7012. Limitations of the FIPS-validated module process do not impact the implementation status of FIPS cryptography. However, the rule has been updated to allow for Enduring Exceptions and temporary deficiencies, which may apply to the implementation of FIPS.

DoD declined to update the rule to include "FIPS-compliant" encryption as opposed to "FIPS-validated" encryption. NIST SP 800-171 R2 requires the use of validated modules in specific conditions. Comments on the specific security requirements contained in NIST documentation are beyond the scope of this rule and should be directed to NIST. Collaboration between DoD and NIST about the NIST cryptographic module validation program, or to define cryptography related ODPs in NIST SP 800-171 Revision 3, is also beyond the scope of the rule. Recommendations for desired changes in NIST documentation should be directed to NIST.

The NIST Cryptographic Module Validation Program website provides a list of approved solutions and their timelines: https://csrc.nist.gov/projects/cryptographic-module-validationprogram.

NIST SP 800-171 information security requirements were codified in 32 CFR part 2002 in response to guidance (in E.O. 13556) to standardize Federal agency policies for safeguarding CUI. The DoD has elected to use FAR clause 52.204-21, NIST SP 800-171 R2, and a subset of NIST SP 800-172 Feb2021 as the basis for the security requirements in this rule.
As stated in § 170.14(c), CMMC Level 1 requirements are found in FAR clause 52.204-21, CMMC Level 2 requirements are found in NIST SP 800-171 R2, and CMMC Level 3 requirements are a selected subset of NIST SP 800-172 Feb2021 requirements as specified in the 32 CFR part 170 CMMC Program rule in table 1 of § 170.14.

NIST SP 800-171A Jun2018 provides authoritative procedures for assessing NIST SP 800171 R2 security requirements and the CMMC Level 2 Assessment Guide provides additional guidance for assessing CMMC Level 2 security requirements. Both documents are referenced in the 32 CFR part 170 CMMC Program rule, at §§ 170.16(c) and 170.17(c).

It is recommended that an OSA develop a SSP as a best practice at Level 1, however, it is not required for a CMMC Level 1 self-assessment. A CMMC assessment does not include NonFederal Organization (NFO) controls from table E in NIST SP 800-171 R2 nor the DFARS clause 252.204-7021 flow down and reporting requirements.

DoD concurs that CMMC provides no mechanism for addressing insider threats posed by political divisions in Congress. However, insider threat in general is addressed in the following CMMC security requirements: AT.L2-3.2.3-Insider Threat Awareness; AC.L2-3.1.7-Privileged Functions; PS.L3-3.9.2e - Adverse Information.

b. Transition to Future NIST Requirements

Comment: Many commenters raised concerns about the CMMC Proposed Rule's citation of a specific version of a relevant baseline document, i.e., NIST SP 800-171 R2. The expressed concerns focused mainly on a perceived potential for a timing conflict between the NIST revision requirements based on DFARS clause 252.204-7012 (revision in effect at time of solicitation) and this CMMC Program rule which specifies NIST SP 800-171 R2. Commentors provided a variety of differing suggestions to address these concerns. Some commenters recommended that no revision number be included, while others recommended citing Revision 3 rather than Revision 2. Others recommended delaying the CMMC Program. Some recommended changing DFARS clause 252.204-7012 or issuing a class deviation to address differences between the NIST revisions cited. Those that recommended citing to Revision 3 noted that to do otherwise could delay compliance with Revision 3 beyond NIST's anticipated finalization of that publication. Commenters noted that the criteria defined in guidance explaining how to assess against NIST requirements (i.e., NIST SP 800-171A Jun2018) does not identify a revision number for the NIST SP 800-171 requirements to which they apply. In addition to the comments about NIST SP 800-171 R2 and NIST SP 800-171 Revision 3, some commenters questioned how DoD would implement or how long the DoD would allow for transitioning to each future version of NIST standards once approved.

One commenter recommended defining a waiver process to manage the transition for each new NIST revision. Another commenter asked whether contract work stoppages are expected during such transitions and if industry would be afforded time to understand the impacts of new requirements to existing systems. One commenter suggested that CMMC affirmations should indicate continued compliance to the NIST SP 800-171 version that applied to the corresponding self-assessment or certification assessment.

Two commenters recommended changing the incorporation by reference version of NIST 800-53 that is cited in this rule be changed from Revision 5 to Revision 4, to better align with the incorporation of NIST SP 800-171 R2. Another commenter noted that both NIST SP 800-171 R2 and NIST SP 800-172 Feb2021 include Organizationally Defined Parameters (ODP), the latter of which are defined in this rule. The commenter advised against defining ODP for either reference, and recommended deletion of specific rule text that does so.

Response: DoD is aware of the differences between the language of DFARS clause 252.204-7012 and the proposed rule. 1 CFR part 51, which governs drafting of this rule, requires the specification of a revision to a standard. Specifying a revision benefits the CMMC Ecosystem by ensuring it moves forward from one NIST standard to the next in an organized manner. The DoD cites NIST SP 800-171 R2 in this final rule for a variety of reasons, including the time needed for industry preparation to implement the requirements and the time needed to prepare the CMMC Ecosystem to perform assessments against subsequent revisions. DoD is unable to incorporate suggestions that CMMC assessments be aligned to whichever NIST revision is current at the time of solicitation and declines to respond to speculation about the release timing of other publications. In May 2024, NIST published SP 800-171 Revision 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, after these comments were received. DoD will issue future amendments to this rule to incorporate the current version at that time. Comments on the content of the NIST SP 800-171 Revision 3 publication or future NIST SP 800-171 revisions should be directed to NIST.

The final rule has been updated to specify the use of NIST SP 800-171A Jun2018, *Assessing Security Requirements for Controlled Unclassified Information*, and NIST SP 800-172A Mar2022, *Assessing Enhanced Security Requirements for Controlled Unclassified Information*.

The DoD has included the numbering scheme in the rule because the numbering scheme is a key element of the model. The CMMC numbering scheme for security requirements must pull

together the independent numbering schemes of FAR clause 52.204-21 (for Level 1), NIST SP 800-171 R2 (for Level 2), and NIST SP 800-172 Feb2021 (for Level 3); it must also identify the domain and CMMC level of the security requirement. DoD developed the least complicated scheme that met all these criteria.

The CMMC Program Office is unable to respond to comments proposing changes to the DFARS, which is subject to separate rulemaking procedures. One commenter described a hypothetical scenario wherein a solicitation is issued such that DFARS clause 252.204-7012 would require compliance with NIST SP 800-171 Revision 3, but the CMMC requirement identified is for assessment against NIST SP 800-171 R2. In this hypothetical scenario, it is possible that the bidder may meet the CMMC requirement by citing a valid CMMC assessment against NIST SP 800-171 R2, while also availing themselves of the flexibilities provided in DFARS clause 252.204-7012 (2)(ii)(B) to submit a written request to the Contracting Officer to vary from the current version of NIST SP 800-171.

Recommendations for modification to or deviation from DFARS clause 252.204-7012 are beyond the scope of this rule. The DoD has evaluated the potential interaction between the CMMC program requirements and the existing requirements in DFARS clause 252.204-7012 and believes that potential conflicts have been resolved.

NIST SP 800-53 R5 is incorporated by reference only for applicable definitions because DoD chose to use the latest definitions available. While it is also true that NIST SP 800-171 R2 was based on NIST SP 800-53 Revision 4, the origination of NIST SP 800-171 R2 is beyond the scope of this rule.

Contractors and subcontractors will not be expected to stop work while they implement changing standards. Implementation of this rule will be introduced as a pre-award requirement in new DoD solicitations, as described in the timeline at § 170.3(e).
Any substantive change to CMMC security requirements must go through rulemaking, and its associated timeline, which may include public comment. The new rule may include a transition period for implementation of the new security requirements.

The commenter correctly identifies that the programmatic intent of this rule is for affirmations to signify systems in question remain compliant as indicated by the assessment that was conducted. Assessments are conducted against the specified NIST publication versions or the requirements in FAR clause 52.204-21. The 48 CFR part 204 CMMC Acquisition rule also reinforces this thought by providing specific wording of the affirmation.

c. NIST SP 800-172 Feb2021 Requirements

Comment: Multiple comments recommended adding all the omitted requirements from NIST SP 800-172 Feb2021 or a subset including Network Intrusion Detection System, Deception and Unpredictability, arguing that they are necessary for protecting CUI and to defend against advanced persistent threats.

Two comments inferred that the requirement to restrict access to systems owned, provisioned or issued by the OSC means that the OSC must provide all equipment used to access the system, which they asserted is impossible because outside entities using GFE, to include DoD, may need access. One commenter also asked if DIB Furnished Equipment would be required, and one commenter argued for an exception for GFE, even though it is not owned, provisioned, or issued by the OSC.

Three comments stated that Organizationally Defined Parameters (ODP) values need to be set by OSAs, not DoD. One commenter argued this will be necessary because of the emerging ODPs at Level 2 associated with NIST SP 800-171 Revision 3. One commenter argued this is critical for uniformity across the Federal enterprise as many contractors support multiple Federal agencies. The commenter further offered that allowing ODP values to be set by OSAs could be limited to contractor systems not operated on behalf of the DoD. One commenter suggested that ODP values set by OSAs may require approval by the contracting officer. One comment stated that the ODPs are too detailed for the 32 CFR part 170 CMMC Program rule, and table 1 to § 170.14 should be moved to the Level 3 Assessment Guide.

One comment argued that removal or quarantine of components to facilitate patching or reconfiguration, as specified in table 1 to § 170.14(c)(4) CM.L3-3.4.2e, is a disruptive and possibly a destructive operational constraint affecting business operations. They asserted that patching and reconfiguration are standard day-to-day IT administrative activity, and components do not need to be removed or quarantined.

One comment asserted that CMMC should be based on NIST SP 800-53 R5 requirements (linked to the associated NIST SP 800-172 Feb2021 requirements) due to additional labor required to create NIST SP 800-53 R5 solutions and benefits to be gained from NIST SP 800-53 R5 overlays.

Two comments argued that IA:L3-3.5.3e regarding 'the prohibition of system components from connecting to organizational systems unless certain conditions are met' is essentially the same requirement as CM:L2-3.4.7 'restricting, disabling, or preventing the use of nonessential programs, functions, ports, protocols, and services'.

Response: DoD considered many alternatives before deciding which NIST SP 800-172 Feb2021 requirements to include as part of CMMC Level 3. NIST SP 800-172 Feb2021 notes that "There is no expectation that all of the enhanced security requirements will be selected by Federal agencies implementing this guidance." For a variety of reasons, including DoD's estimation of cybersecurity maturity and complexity across the DIB, and potential cost of certain Level 3 requirements compared with the benefit, the DoD has included a limited set of NIST SP 800-172 Feb2021 requirements. On a contract-by-contract basis, additional requirements may be added. OSAs are at liberty to implement additional requirements.

The intent of AC.L3–3.1.2e, which requires restricted access to systems and system components, is not that DIB companies issue laptops to external users wishing to access Level 3 enclaves. While laptop issuance is one solution, other options are available. The important concept in this requirement is "comply to connect", and it applies to all users, both within the OSA and externally, equally. In complying with this requirement, GFE may be considered provisioned by the OSC and therefore is not restricted under that requirement.

DoD defines the ODPs for NIST SP 800-172 Feb2021 included in CMMC Level 3. This eliminates the risk of different parameters being set for different DoD programs. Rulemaking requirements dictate that table 1 to 170.14(c)(4) be codified in the rule. The Assessment Guide is an optional document.

DoD declines to accept the risk of removing security requirement CM.L3-3.4.2e. The Assessment Guide has been updated to include additional discussion on this security requirement. Feedback on individual security requirements should be direct to NIST.

Any relationship to the NIST SP 800-53 R5 controls is for information only. The requirements that must be implemented for CMMC Level 3 are defined in the rule table 1 to § 170.14(c)(4).

IA:L3-3.5.3e and CM:L2-3.4.7 are different requirements. The L2 requirement is about functionality, and the L3 requirement is about trust. Feedback on individual security requirements should be direct to NIST.

24. CMMC Annual Affirmation Requirements

Comment: One commenter recommended the affirmation statement include a statement confirming the scope has not changed and requested the rule be modified to identify types of changes that would constitute a change of system scope. Another commenter recommended removing any requirement for affirmation after assessment certificate issuance or else revising the rule to identify any benefits the affirmation provides that conducting an independent assessment does not already provide. Another commenter recommended the DoD clarify that out-of-cycle affirmations are not needed.

Three comments said the affirmation language needs revision because maintaining perfect scores is not possible and asking individuals to affirm continuous compliance is unreasonable. One commenter voiced apprehension that signing the affirmation statement would make a person criminally liable under the False Claims Act, due to the need for system maintenance to fix things that break. One commenter expressed concern that continuous monitoring by contractors

increases cost and burden to stay in compliance and opens companies up to False Claims Act liabilities. One of these commenters recommended DoD rely on representation and selfassessment in lieu of affirmations to indicate that the offeror meets the requirements of the CMMC level required by the solicitation. Two commenters requested clarification on what affirmation entails. Another commenter requested modification to clarify that the Affirming Official will attest only that the requirements are implemented as of the certification date, or proposal submission date, and requested removal of affirmation references to continuous compliance.

Two commenters urged the Department to align the annual affirmation timeline with the 3year assessment timeline to ensure consistency and reduce potential False Claims Act liability. One commenter also incorrectly believed a prime contractor affirmation would be made on behalf of its entire supply chain.

Another commenter asked DoD to clarify that an organization may obtain from C3PAOs a limited review of changes made since the last assessment in support of required affirmations and noted that the DoD or CMMC AB may wish to clarify what supporting evidence is required for annual affirmations. Additionally, the commenter recommended that DoD reconsider the requirements for CMMC Level 1 since these are covered by System for Award Management (SAM).

One commenter asked, in reference to POA&M closeout affirmations, if there was no longer an expectation that a C3PAO will confirm the close out of a POA&M. One commenter provided a recommendation to include an executive summary in the affirmation that includes POA&M related metrics as an indicator of an OSA's effective O&M, security, and continuous monitoring activities.

Response: As described in § 170.22(a)(2)(ii), the CMMC affirmation shall include a statement to the effect that the OSA has implemented and will maintain implementation "within the relevant assessment scope", which adequately addresses the commenters suggestion. No change to the rule text was therefore required. Annual affirmations ensure OSAs conduct periodic checks and verify to the Department that changes to their networks have not taken them out of compliance during the certification period. The annual affirmation requirement enables DoD to permit 3 years between CMMC Level 2 or 3 assessments, rather than requiring annual assessments. The DoD does not agree with the comment that following the procedures in § 170.22 creates an additional burden. The DoD does not concur with removing the terms "continuing" or "continuous "as it relates to an OSA's affirmation. Continuing compliance means that the contractor system in question remains in compliance and that the OSA intends to maintain compliance over time, not that the OSA cannot have an operational plan of action. Any changes to the information system beyond use of operational plans of action require a new assessment and a new affirmation. Operational plans of action as described in CA.L2-3.12.2 are part of normal maintenance of a system and do not require a separate out-of-cycle affirmation. The DoD declines to address specific cases when affirmations are not required. DoD's use of the term OSA within the affirmations section is deliberate and conveys that each organization is responsible for affirmations pertaining to their own assessments. An Affirming Official definition was added to the rule and provides that clarification.

The rule delineates which requirements may be addressed with a POA&M for up to 180 days to achieve Final CMMC Status. As stated in § 170.22, an Affirming Official attests the organization is satisfying and will maintain its specified cybersecurity requirements. An OSA may complete a self-assessment and submit a new affirmation at any time. POA&Ms associated with conditional assessments are closed-out by C3PAOs for Level 2 final certification assessments and by DCMA DIBCAC for Level 3 final certification assessments. OSAs must affirm results in SPRS for all assessments.

If an OSA makes significant changes within the CMMC Assessment Scope, a new assessment and affirmation are required. The rule does not preclude OSAs from contacting a C3PAO for a review prior to an annual affirmation, however this is not required. No supporting evidence is required for an annual affirmation. Annual representations and certifications

submitted in the System for Award Management (SAM) serve a different purpose from the CMMC affirmation requirement completed in SPRS. Furthermore, given the sensitivity of an OSA's cyber security status, the DoD has elected not to use SAM, a public website. Details for completion of the annual affirmation, including wording of the affirmation statement, are addressed in the 48 CFR part 204 CMMC Acquisition rule. The affirmation signifies the requirements were implemented as of the date of the self-assessment or certification, and that the OSA has and intends to maintain the system as assessed. The DoD declines to require the use of an executive summary or the publication of metrics in the affirmation statement as part of the affirmation because that is not consistent with the purpose of the affirmation requirement.

Regarding the alignment of assessments and affirmation timelines, the DoD declines to adopt recommended changes which would allow up to 3 years to elapse before DIB companies would be required to assess the status of their cybersecurity compliance.

25. CMMC Acceptance of Alternate Standards

a. CMMC and Other Agency Standards or Acceptance of CMMC Assessments

Comment: Several commenters asked for additional detail about § 170.20 Standards Acceptance. One commenter described discussions from various DoD industry engagements and suggested the rule is inconsistent with information provided at those information exchange events.

Some commenters observed the rule does not describe DoD efforts to coordinate with other agencies regarding any additional cybersecurity requirements they choose to implement, which could conflict or add burden for companies that must also comply CMMC requirements. One comment suggested implementing the CMMC program government wide. An industry association submitted several comments regarding perceived duplication between this rule and cybersecurity requirements of other Federal agencies and foreign governments. They also recommended the DoD modify the rule to reflect other agency standards, such as TSA and CISA security directives requiring cyber incident reporting for natural gas utilities.

Several commenters thought the rule did not adequately explain potential portability of CMMC assessments, referring to whether other agencies might recognize CMMC compliance as meeting or partially meeting their requirements. One specifically suggested CMMC affirmations could be accepted as evidence of compliance with any similar cybersecurity requirements other agencies may implement. One comment suggested that by assessing compliance of all applicable security requirements, the CMMC program will impede efforts to establish DoD information sharing agreements with other non-DoD organizations, including other agencies and foreign governments.

Response: Some comments received lacked relevance to the rule's content, which is limited to specific CMMC Program requirements. The DoD declines to respond to speculative or editorial comments about private citizens or entities, all of which are not within the scope of this rule.

Similar data security requirements are already applied to contractors across all Federal agencies, due to the applicability of FAR clause 52.204-21, and 32 CFR part 2002. All executive agencies are required to comply with the same standards for protection of FCI and CUI in those regulations. Once attained, a current CMMC certification may be presented for consideration by any entity (including other government agencies) as an indicator that the security requirements associated with the certificate level (e.g., CMMC Level 2) have in fact been implemented.

CMMC Program requirements are designed to ensure compliance with existing standards for protection of FCI and CUI and align directly to NIST guidelines (e.g., NIST SP 800-171 R2) and the basic safeguarding requirements of FAR clause 52.204-21 that apply to all executive agencies. Regulations issued by any executive agency must be aligned to these overarching requirements, therefore CMMC Program requirements will not conflict with any FCI or CUI safeguarding regulations that may be issued by other agencies as cited by the commenter. All executive agencies are permitted to submit and review comments as part of the formal rulemaking process, and additional coordination is not required. This rule provides a consistent way of verifying contractors' compliance with the referenced FAR and NIST requirements, in addition to those from NIST SP 800-172 Feb2021 where applicable.

b. Requests to Recognize Alternate Standards

Comment: Several commenters requested the rule be modified to accept or recognize alternate standards for the purpose of meeting CMMC assessment requirements. Some small to medium businesses recommended acceptance of healthcare relevant standards or other recognized certification frameworks as a substitute for CMMC and FedRAMP Equivalency.

Another comment cited verbiage in the DFARS clause 252.204-7012 clause that references DoD CIO approval to "vary" from NIST SP 800-171 requirements as rationale for revising the CMMC rule to permit acceptance of other standards such as the NERC Critical Infrastructure Protection standards which apply to North America's Bulk Electric System (BES).

Some comments expressed concern that absent greater acceptance of the standards required by other agencies, companies complying with CMMC would be at a competitive disadvantage due to the perceived costs of complying with CMMC standards. Another comment expressed a similar concern but cited the need for acceptance of foreign C3PAOs to effectively scale CMMC to include assessment of foreign OSCs.

Response: CMMC Program requirements apply to those contractors that seek to bid for DoD work which requires processing, storing, or transmitting FCI or CUI in a contractor owned information system. Section 170.20 addresses Standards Acceptance and delineates the only existing bases for accepting alternate standards in this rule. The DoD does not currently have standards acceptance with other Federal entities in lieu of the CMMC requirement. DoD's harmonization of requirements with other agencies is achieved through compliance with NIST standards. DoD's recognition of the standards of other nations occurs through negotiation of international arrangements and agreements, which is beyond the scope of this rule. The CMMC Program has aligned requirements with NIST standards, and many foreign nations are adopting NIST standards as well. In developing this rule, the DoD worked with standards bodies, removed unique requirements, and aligned new requirements directly with NIST SP 800-171 R2 and select NIST SP 800-172 Feb2021 requirements to reduce and streamline cybersecurity burden across the industry. CMMC Program requirements make no change to existing policies for limits on dissemination of CUI. Comments on information sharing between other agencies or foreign entities are beyond the scope of this rule. The requirement to comply with NIST SP 800-171 was mandated in DFARS clause 252.204-7012. Granting alternatives to that standard is beyond the scope of this rule.

Several foreign or international companies submitted comments expressing interest in the rule section pertaining to C3PAO requirements (§ 170.9(b)) and correctly noted that this section does not preclude otherwise qualified foreign companies from achieving C3PAO accreditation. Note that the DoD does permit 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.

c. CMMC Acceptance of Other DIBCAC Assessments

Comment: Some commenters either did not understand or objected to the fact that standards acceptance requirements for DIBCAC High Assessments require a score of 110 without POA&Ms. Other comments requested clarity regarding standards acceptance of DIBCAC High Assessments at CMMC Levels 2 and 3. One comment inquired about the programmatic details of DCMA's Joint Surveillance Program.

Another comment expressed concerns over disparities between how CMMC C3PAOs and DIBCAC assess, given the fact that DIBCAC assessors are empowered to make risk acceptance decisions on behalf of the Government, whereas C3PAO assessors are not. One commenter questioned the use of the NIST SP 800-171 R2 Cybersecurity FAQs as published in the DoD Procurement Toolbox. Another commenter asked whether C3PAOs assess for compliance with DFARS clause 252.204-7012, paragraphs c-g, as DCMA DIBCAC does in their assessments of OSAs. One commenter suggested that the DIBCAC is not certified to conduct Level 3 assessments and that training requirements for CMMC Level 2 C3PAO assessors should also apply to DIBCAC assessors, or else Level 3 assessments should be conducted by C3PAOs.

Response: There is qualified standards acceptance between DCMA DIBCAC High Assessment and CMMC Level 2 Certification Assessment as described in § 170.20(a). There is no standards acceptance between DCMA DIBCAC High Assessment and CMMC Level 3. To be eligible for standards acceptance resulting in a CMMC certification, an OSC must achieve a perfect 110 score on the Joint Surveillance assessment without any open POA&Ms at the time of assessment. If the Joint Surveillance assessment results in POA&M actions, any POA&M must be closed prior to standards acceptance.

Completion of a prior DCMA DIBCAC High Assessment does not necessarily indicate the likelihood of a future CMMC Level 3 requirement. DIBCAC High assessments are currently conducted against the NIST SP 800-171 R2 requirements, whereas the DoD will identify the need for a CMMC Level 3 assessment when its internal policies indicate the added protections of NIST SP 800-172 Feb2021 are necessary to adequately safeguard DoD information.

Acceptance of a small number of DIBCAC High or Joint Surveillance Program assessments to meet future CMMC Level 2 assessment requirements will reduce the initial demand for C3PAO assessment. Only those DIBCAC High Assessments completed prior to the effective date of the rule are eligible for standards acceptance to meet CMMC Level 2 Certification requirements. The DoD will enter CMMC Level 2 Certifications into eMASS for suitable DIBCAC High Assessments, with a validity period of 3 years from the date of the original High Assessment. A CMMC Final Level 2 certification assessment is entered into eMASS by the C3PAO following a successful (i.e., perfect score with no POA&Ms) joint surveillance assessment against NIST SP 800-171 R2. It is not the result of a CMMC Level 3 assessment but can be provided as evidence that an OSC is ready to initiate a CMMC Level 3 assessment.

Although Joint Surveillance is listed as standards acceptance in 170.20(a)(1), the details of this DCMA program and any changes to it are beyond the scope of this rule. A Joint surveillance is a DCMA DIBCAC assessment and falls under their purview. The CMMC office understands that there is disparity between what is assessed by a C3PAO and the DIBCAC and that the guidance information in the DoD Procurement Toolbox is the driving factor. Since the Procurement Toolbox is outside of the scope of the 32 CFR part 170 CMMC Program rule, it cannot be properly addressed here or in the rule. With CMMC the DoD utilizes a risk-based approach in its allowance for POA&Ms, gradient scoring for certain controls (e.g., FIPS and MFA), temporary deficiencies, and enduring exceptions.

DCMA DIBCAC assessors are trained and qualified to conduct assessment against NIST SP 800-171 R2 for the DoD. DoD determined that C3PAOs conducting assessments on other C3PAOs introduced a significant conflict of interest. Given the sensitivity of the programs requiring Level 3 assessments, the DoD determined that those assessments must be completed by a DoD entity. The DoD declines to respond to speculative or editorial comments regarding DCMA DIBCAC assessments.

The CMMC model (§ 170.14) only incorporates requirements from FAR clause 52.204-21, NIST SP 800-171 R2, and NIST SP 800-172 Feb2021. C3PAOs are only responsible for assessing the requirements of § 170.17. DCMA DIBCAC operates under different authorities and can address all the requirements of DFARS clause 252.204-7012.

d. Validity Period for Standards Acceptance

Comment: Two comments asked how SPRS would be updated to reflect CMMC Level 2 certification when based on standards acceptance. One asked whether that update would be automatic. One comment asked whether CMMC standards acceptance for DIBCAC joint surveillance assessments would result in certifications being issued to the OSA by the C3PAO or by DIBCAC.

Some comments, including those from three industry associations, objected to the start date for the 3-year validity of CMMC certification based on standards acceptance of prior DIBCAC assessments. Those comments requested the validity period begin with the effective date of the 32 CFR part 170 CMMC Program rule. Along these lines, another commenter asked whether C3PAOs may certify an OSA based on evidence of a perfect 110-scored DIBCAC High

Assessment. One comment requested a 1-year extension of the validity period to 4 years.
Response: The DoD has considered the recommendation to modify the validity period for certifications resulting from standards acceptance and declines to revise the rule text. It is important that contractors maintain security compliance for systems that process, store, or transmit DoD CUI. Given the evolving cybersecurity threat, DoD's best interests are served by ensuring that CMMC Level 2 assessments remain valid for no longer than a 3-year period, regardless of who performs the assessment.

A C3PAO may not simply read the DIBCAC assessment score in SPRS and grant a completed CMMC Level 2 certification assessment. C3PAOs may only submit certification assessment results based on having conducted a certification assessment. An OSA is free to seek a C3PAO certification assessment, but this would be unnecessary, because a valid DIBCAC High assessment with a 110 score will automatically be converted in SPRS to reflect a CMMC Final Level 2 certification assessment provided all requirements of § 170.20(a)(1) are met. A DIBCAC High assessment conducted after the rule is effective is not eligible for standards acceptance.

26. CMMC Requirements and International Entities

a. Applicability to International Entities

Comment: Several public commenters asked whether and how the CMMC rule content would apply to foreign based or international companies, either as companies seeking to comply with assessment requirements or as companies seeking to participate in the CMMC Ecosystem.

Some questions asked for interpretation of requirements for specific scenarios, such as how CMMC requirements might affect Status of Forces Agreements for DoD installations overseas. Others asked about application of flow-down requirements to foreign subcontractors, including in circumstances when DFARS clauses do not apply or when international agreements supersede application of DFARS clause 252.204-7012. A few comments asked how foreign or multinational corporations with facilities abroad can attain CAGE codes, access SPRS, or meet other aspects of CMMC requirements. Some asserted that specific systems contractors need to access, such as SPRS and PIEE, are not designed to accommodate foreign address formats and requested modifications or alternative options to facilitate submission of CMMC affirmations. One commenter suggested that assessment of foreign contractor information systems should only be conducted by the host country, and asked whether foreign contractors should be partially exempted from CMMC requirements.

Response: CMMC Program requirements are applicable when DoD requires processing, storing, or transmitting of either FCI or CUI during performance of a DoD contract. CMMC Program requirements would not apply to a DoD Installation's communication with a Host Nation government on matters related to the Installation. CMMC program requirements apply to all DoD contractors alike when contract performance will require processing, storing, or transmitting of FCI or CUI on contractor-owned information systems. This 32 CFR part 170 CMMC Program rule does not permit partial exemption of assessment requirements for foreign contractors. Any discussion of exemptions or deviations for foreign businesses are outside the scope of the 32 CFR part 170 CMMC Program rule and must be addressed through governmentto-government international arrangements or agreements. Pathways and timelines for achieving these agreements are outside the scope of this rule.

CMMC requirements apply to both domestic and international primes and flow down to subcontractors throughout the supply chain if their information systems process, store, or transmit FCI or CUI. CMMC requirements are based upon the type of information processed and shared, regardless of where the company is headquartered or operates. Certification requirements for subcontractors are addressed in § 170.23(a)(1) through (4). For additional information about flow-down of contractual requirements, see the 48 CFR part 204 CMMC Acquisition rule. The CMMC process is the same for international and domestic contractors and subcontractors. International sub-contractors must undergo a CMMC assessment at the appropriate level to demonstrate compliance with NIST SP 800-171 R2 requirements. All OSAs must register in https://sam.gov, which has instructions for obtaining applicable CAGE or NATO

CAGE codes (NCAGE codes).

Address data is not a required SPRS data input for CMMC purposes. Contractor address information is required to obtain a CAGE code that, along with a Unique Entity ID, is required to register in SAM. SPRS currently receives assessment information from domestic and international entities. International organizations get CAGE codes in the same manner that US organizations do, including in some instances NCAGE codes. CAGE codes are required for a contractor to register for a user account in Procurement Integrated Enterprise Environment (PIEE) that provides contractors access to SPRS and other applications as necessary for DoD contracts.

b. International Agreements

Comment: Several commenters asked about procedures for establishing recognition of other nations' cybersecurity standards or assessment programs as acceptable alternatives to CMMC program requirements. Another commenter noted the rule provides no explicit recognition of existing agreements between the DoD and other nations related to information sharing and defense procurement. They and other commenters asked that the rule identify a specific process for reaching agreements related to CMMC program requirements. Some of these commenters identified specific foreign cybersecurity programs and requested that the DoD work toward reciprocal recognition of their underlying standards. One of these commenters requested that DoD identify timelines for establishing bilateral agreements.
In particular, the Canadian counterpart for the CMMC program expressed concern that Canadian companies could be disadvantaged in seeking CMMC certification and requested the DoD consider establishing a unified accreditation body for Canadian and US C3PAOs.

Response: While the rule does address application to foreign contractors and ecosystem participants throughout, these requirements may be superseded by the terms and conditions of applicable international arrangements or agreements.

CMMC validates cybersecurity requirements, as defined in FAR clause 52.204-21, NIST SP 800-171 R2, and a selected subset of NIST SP 800-172 Feb2021, where applicable. These cybersecurity requirements apply to international and domestic companies when included in a DoD contract. The Department cannot speculate about the arrangements of any international agreement and how it may or may not impact international partners, as these arrangements are beyond the scope of this 32 CFR part 170 CMMC Program rule.

The DoD has designed CMMC Program requirements to apply to those contractors that bid for DoD work which will require access to process, store, or transmit FCI or CUI in a contractor owned information system. A CMMC certification assessment is portable in the sense that it provides confidence that the holder has been assessed by an authorized third party for compliance with the applicable security standards (e.g., NIST SP 800-171 R2 or NIST SP 800172 Feb2021). Once attained, CMMC certification assessment status may be presented for consideration by any entity as an indicator that they have implemented security requirements associated with the certificate level (e.g., NIST SP 800-171 R2 or NIST SP 800-172 Feb2021). Section 170.20 delineates the only existing bases for accepting alternate standards in this rule.- It is beyond the scope of this rule to provide a specific set of directions or guidance on recognition for alternate cybersecurity standards. Deviations from DFARS clauses are also beyond the scope of this rule.

Section 170.20 has been modified to state that an OSC with a perfect score from a prior DCMA DIBCAC High Assessment aligned with the same CMMC Level 2 Scoping may meet CMMC Final Level 2 certification assessment requirements via acceptance of the prior DIBCAC assessment in lieu of a C3PAO assessment. Standards Acceptance does not refer to international standards acceptance, which is not described within the rule.

c. C3PAO, CCP, and CCA Requirements

Comment: In addition to the interest in international agreements, some commenters expressed concern about CMMC ecosystem capacity to meet demand for Level 2 certification. They advocated support for accreditation of non-U.S. based C3PAOs. One commenter suggested that FOCI requirements be deleted from the rule and managed via DoD's oversight of the

CMMC AB. One commenter speculated the phased CMMC implementation plan would require all non-US firms to comply simultaneously and recommended that foreign contractors be allowed additional time to comply. Another recommended that foreign companies be permitted to simply self-assess in lieu of obtaining a CMMC Level 2 certification assessment.

Several commenters asked about foreign nationals participating in the CMMC ecosystem and noted discrepancies between qualifications identified in the rule and content on the CMMC AB's website at the time of rule publication. These commenters expressed interest in the ability for foreign citizens to become CCAs, CCPs, and LTPs (a term no longer used in the rule).

One commenter presumed that only US-based Cloud Service Providers (CSPs) may become FedRAMP authorized, and asserted a need to authorize or accredit foreign-based CSPs that foreign DIB contractors might use while still achieving CMMC compliance. Another asked how foreign small businesses can comply with CMMC without access to U.S. approved CSPs. One commenter asked for guidance on how to get foreign products and services, such as encryption and decryption mechanisms, approved for use in information systems that require CMMC assessment. One commenter suggested that the CMMC program permit assessment by C3PAOs and assessors accredited in accordance with other ISO/IEC standards than those identified in this rule. They cited ISO/IEC 27001 or 9901 as suitable alternate ISO/IEC standards.

Response: The DoD declines to delay CMMC Program implementation for non-U.S. organizations. International businesses will not receive special accommodations because the CMMC Program's phased implementation will impact both U.S. and non-U.S. defense contractors equally. The implementation plan described in the rule does not promote or prioritize certification assessments of any contractor over any other contractor. All companies, regardless of location or nationality, will have access to any authorized C3PAO. The rule does not preclude non-U.S. citizens or foreign-owned C3PAOs from operating in the U.S. Additionally, U.S. owned C3PAOs may operate in a foreign nation.

As stated in the rule, C3PAOs must meet the criteria in § 170.9. Non-U.S. organizations and employees that meet all the requirements in §§ 170.9 and 170.11 will not be prohibited from operating as a C3PAO within the U.S. or abroad. A list of authorized C3PAOs is available on the current CMMC AB marketplace. DoD does not concur with the recommendation to delete § 170.9(b)(5) content identifying FOCI requirements. Those details for complying with FOCI are necessary for understanding the requirement.

Some commenters noted differences between the rule content and information on the CMMC AB web site. The CMMC AB is part of the public and had no access to advance information prior to publication of the proposed rule. The rule takes precedence in the event of any discrepancy with CMMC AB materials.

The document 'Career Pathway Certified Assessor 612', dated 2020, has been replaced by a regularly updated DoD Cyberspace Workforce Framework which may be found at https://public.cyber.mil/dcwf-work-role/security-control-assessor/. Intermediate and Advanced Foundational Qualification Options in the DoD Cyberspace Workforce Framework's Security Control Assessor (612) Work Role are available to foreign nationals. The rule has been updated to reflect this reference update.

A domestic or international business seeking a contract that contains DFARS clause 252.204-7012, and using a cloud service provider to process, store, or transmit covered defense information in performance of that DoD contract, must ensure that the CSP meets FedRAMP authorization or equivalency requirements. As the FedRAMP program and FedRAMP equivalency are available to international organizations, foreign entities do not need to develop their own FedRAMP program. FedRAMP authorization or equivalency is also available to small businesses. The DoD leverages the FedRAMP program to implement requirements for the adoption of secure cloud services across the Federal Government and provide a standardized approach to security and risk assessment for cloud technologies. Export controlled goods and ITAR are outside the scope of the 32 CFR part 170 CMMC Program rule.

The process for identifying specific products or services that may meet NIST security requirements is beyond the scope of this rule. CMMC program requirements are unrelated to

evaluation or approval of encryption or decryption products manufactured by foreign information security companies.

DoD considered many alternatives before deciding upon the current CMMC structure. Alternative methods of assessment have proven inadequate and necessitated the establishment of CMMC. DoD declines to accept the recommendation of an alternate path to C3PAO accreditation.

27. Impact to Small Businesses

a. Funding the CMMC Program

Comment: One comment asserted that the rule does not address CMMC program funding, affordability, and sustainability. They recommended the DoD conduct and publish a comprehensive cost assessment for each level of CMMC certification and explore ways to reduce the financial burden on contractors.

Response: DoD included an analysis of costs to meet CMMC requirements in the regulatory impact analysis for this rule.

As described in the estimate included with the rule, the major cost categories for compliance with CMMC requirements are anticipated to include costs for completing a self-assessment (e.g., Level 1 or 2); costs to prepare for and undergo C3PAO assessment (Level 2); costs required to implement the Level 3 security requirements and for preparing to undergo DCMA DIBCAC assessment (Level 3). All of these except the market costs of a C3PAO are controlled by the organization seeking assessment. Market forces of supply and demand will determine C3PAO pricing for CMMC Level 2 certification assessments.

Analysis of costs to meet CMMC requirements is provided in the regulatory impact analysis for this rule. The CMMC rule does not make any change to cost allowability as defined in the FAR 31.201-2 Determining Allowability. Verifying compliance with applicable security requirements may increase cost and is necessary for the protection of DoD CUI. With the revised CMMC, the DoD has streamlined requirements to align directly to NIST guidelines and has eliminated unique security practices to ease the burden on smaller companies. DoD must enforce CMMC requirements uniformly across the Defense Industrial Base for all contractors and subcontractors who process, store, or transmit CUI. The value of information (and impact of its loss) does not diminish when the information moves to contractors and subcontractors. The DoD declines to speculate about how OSCs and C3PAOs negotiate mutually acceptable terms and conditions for assessment agreements. The DoD declined to modify the estimates, which are intended to be representative and to inform rulemaking.

b. Disproportionate Cost Burden

Comment: Many comments emphasized the importance of small business to the DoD contracting environment and expressed the concern that increased cost burden on small companies will result in an anti-competitive barrier to entry. Specifically, commenters state the lack of in-house security resources, inability to amortize costs, upfront costs to comply with CMMC Level 1 and 2 without guaranteed contracts, keeping pace with requirements changes, paying market rates for C3PAO assessments, and obtaining "perfect" compliance with requirement or assessment objectives may not be affordable or may cause unacceptable enterprise disruption. One comment asserted that the DoD is not considering additional costs to small- and medium-sized businesses (SMBs) for ongoing compliance. One comment stated the cost of entry for a new SMB may be insurmountable even with cost recovery. One comment suggested "right-sizing" CMMC by tailoring security requirements based on business size and number of employees. Additionally, one comment asserted that small businesses would be unfairly punished while large, legacy primes would lobby and get waivers.

Two comments noted that CMMC will increase costs, perhaps doubling annual IT and security spending, ultimately passing the cost to customers, the government and the taxpayer and asked how the DoD plans to deal with price increases from subcontractors and primes. One comment suggested the DoD pay contractor employees to learn to cyber defend rather than pay auditor assessment costs.

Response: The DoD concurs with commenters' assessment of the importance of small businesses to the DoD. The DoD has streamlined CMMC requirements to align directly to NIST guidelines and has eliminated unique security practices to ease the burden on smaller companies. In recognition of the cyber threat both to DoD and to the DIB, CMMC Program requirements are designed to ensure compliance with existing standards for protection of FCI and CUI. These cybersecurity requirements align directly to NIST guidelines (i.e., NIST SP 800-171 R2 and NIST SP 800-172 Feb2021) and the basic safeguarding requirements (FAR clause 52.204-21) that apply to all executive agencies.

The analysis of costs to meet CMMC Level 1 and 2 requirements are provided in the Regulatory Impact Analysis published with this rule. Note that certification is never required for CMMC Level 1, which is a self-assessment requirement. CMMC Level 2 may either be met via self-assessment, or via certification following a C3PAO assessment, depending on the specific requirement cited in the solicitation. Some comments appeared to reference costs to meet the requirements of existing DFARS clause 252.204-7012. Please refer to 81 FR 72990, October 21, 2016, for DoD's final rule implementing the DoD's requirement that "contractors shall implement NIST SP 800-171 as soon as practical, but not later than December 31, 2017."

The cost estimates for SMBs represent average derived estimates based on internal expertise and public feedback in accordance with OMB Circular A-4. The size and complexity of the network within scope of the assessment impacts the estimates as well.
The DoD has streamlined CMMC requirements to align directly to NIST guidelines and has eliminated unique security practices to ease the burden on smaller companies. In addition, CMMC Level 1 and select CMMC Level 2 requirements are now met via self-assessment, which reduces burden to small businesses.

The CMMC program incorporates flexibility with the use of self-assessment, POA&Ms, and waivers. Since December 2017, DFARS clause 252.204-7012 has required contractors to implement the NIST SP 800-171 security requirements to provide adequate security applicable for processing, storing, or transmitting CUI in support of the performance of a DoD contract. OSAs that are currently attesting that they meet DFARS clause 252.204-7012 should not have difficulty successfully achieving a Level 2 self-assessment.

Some comments received lacked relevance to the rule's content, which is limited to specific CMMC Program requirements. The DoD declines to address speculation about lobbying activities. Verifying compliance with applicable security requirements may increase financial cost to the DoD due to increased contract costs but it is necessary for the protection of DoD CUI. The cost of lost technological advantage over potential adversaries is greater than the costs of such enforcement. The value of information (and impact of its loss) does not diminish when the information moves to contractors.

The trade-off is between protecting sensitive information from our nation's adversaries and accepting the fact that security costs increase for numerous reasons. Many of those cost-drivers are completely independent of CMMC. While CMMC compliance adds to an organization's cost, no member of the DIB can assume the status-quo in today's ever-changing cyber security environment. Increasing costs to protect the nation's data and industries from emerging threats is simply a component of doing business anywhere in the world. Processing, storing, or transmitting sensitive Government information comes with a handling cost that needs to be built into each organization's business model.

Some comments included suggestions about how workflow should occur between prime and subcontractors to decrease or eliminate the transfer of CUI to subcontractors. The DoD cannot dictate these business practices but encourages prime contractors to work with its subcontractors to flow down CUI with the required security and the least burden. Questions regarding what to mark as CUI are out of scope of this rule. At the time of award, the DoD may have no visibility into whether the awardee will choose to further disseminate DoD's CUI, but DFARS clause 252.204-7012 and DFARS clause 252.204-7021 require that the prime contractor to flow down the information security requirement to any subcontractor with which the CUI will be shared. Decisions regarding which DoD information must be shared to support completion of which

subcontractor tasks takes place between the prime contractor and the subcontractors chosen to complete the specific tasks.

c. Phasing the Cost to Comply

Comment: Two comments suggested a phased compliance would help offset financial burden while working toward full compliance. One comment expressed concern that Managed Service Providers (MSPs), many of which are small businesses, will not have time to achieve Level 2 certification before their OSA and OSC customers need them to be certified and recommended extending the phased timeline.

Several comments stated that recouping compliance costs could take years, forcing SMBs into financial debt, contract termination, and exclusion from the market for DoD contracts. One commenter expressed concern about implementation of CMMC as a condition of contract award and the implication that compliance costs are incurred prior to receiving a DoD contract.

Response: DoD declined to implement a small entity specific "phased compliance". Since December 2017, DFARS clause 252.204-7012 has required contractors to implement the NIST SP 800-171 security requirements to provide adequate security applicable for processing, storing, or transmitting CUI in support of the performance of a DoD contract.

DoD received numerous comments about the use of ESPs, including MSPs, which do not process, store, or transmit CUI. In response to comments, the DoD has reduced the assessment burden on External Service Providers (ESPs). ESP assessment, certification, and authorization requirements in §§ 170.19(c)(2) and (d)(2) have been updated. ESPs that are not CSPs and do NOT process, store, or transmit CUI, do not require CMMC assessment or certification. Services provided by an ESP are in the OSA's assessment scope.

CMMC has taken several steps to keep the cost of compliance with the rule commensurate with the risk to the DoD's information. Level 1 only requires self-assessment, and many contracts with CUI will only require a Level 2 self-assessment. Companies that currently attest that they meet DFARS clause 252.204-7012 should not have difficulty completing a Level 2 self-assessment. In accordance with the rulemaking process, this rule was reviewed by both DoD cost analysts and OMB economists for realism and completeness.

This is a 32 CFR part 170 CMMC Program rule, not an acquisition rule. The 48 CFR part 204 CMMC Acquisition rule will address implementation of CMMC as it pertains to DoD contracts.

d. Detailed Cost Analysis

Comment: A few comments suggested a detailed cost analysis should consider SMBs of various sizes, types, and challenges to ensure compliance is sustainable. One comment asked whether a profit margin analysis was performed, while another asserted that other third-party assessments are less expensive than the estimates for CMMC assessment. Another stated CMMC Level 3 cost estimates are too low and suggested using costs associated with SECRETlevel networks for calculation.

Response: The DoD provided an analysis of costs to meet CMMC Level 1 and 2 requirements in the regulatory impact analysis for this rule. The cost estimates provided for this rule represent average costs for companies to comply with CMMC requirements, including the need for self-assessment or independent assessment against the specified standards. Comparing costs with other third-party security audits presumes that the security and assessment requirements are identical, and DoD disagrees with that assumption.

The DoD declined to produce another cost estimate for CMMC assessment and certification. As required by the Rulemaking Guidance, the DoD provided cost estimates and impact analyses in the proposed rule. The analysis included estimated costs for each level and type of assessment or certification for different sized contractor businesses. The cost estimates did not include an analysis of profit margins, which is not required. This rule also does not provide the cost analysis for all actions, personnel, and security measures required to protect CUI information, data, systems, and technical products through the life cycle of the work and data generated. The cost estimates represent derived estimates based on internal expertise and public feedback in accordance with OMB Circular A-4.

Market forces of supply and demand will determine C3PAO pricing for CMMC Level 2 certification assessments. The size and complexity of the network within scope of the assessment impacts the costs as well. CMMC Level 3 assessments against the NIST SP 800-172 Feb2021 baseline are performed free of cost by DoD assessors, which reduces the cost of CMMC Level 3.

The costs associated with a government-owned SECRET-level network are not relevant to the CMMC Program which ensures protection of FCI and CUI.

e. Assistance Programs or Other Relief

Comment: Several commenters proposed that financial assistance, contract incentives, direct reimbursement of assessment costs (in whole or in part), and market rate price caps be considered to lessen financial burden and decrease the entry barrier for SMBs. Several comments also inquired about DoD SMB grant programs to help SMBs cover the cost of CMMC Level 2 certification assessments.

Multiple comments suggested DOD provide actionable guidance through outreach support and assistance along with free or reduced cost cybersecurity services to SMBs, with two referencing the DoD Office of Small Business Programs and one the DoD Procurement Toolbox. One comment, from a large business with SMB suppliers, requested clearer guidance and support for flow down to sub-tier suppliers and SMB supply chains.

One comment stated firms who receive a low number of CUI documents (30 docs in 3-years on 10 computers) do not justify the cost of becoming CMMC compliant, and added the cost is nearly as much as protection for classified documents. One commenter suggested NIST SP 800171 R2 security requirements would not apply to their specific characteristics, i.e., a very small business with minimal internet connectivity, no remote access, no public access, no mobile devices, no remote work, and no known cybersecurity issues. The comment asserted that the company posed minimal risk to CUI and should be excused from adhering to CMMC program requirements based on cost burden.

One comment proposed eliminating third party assessment costs and relying only on selfcertification to address the cost burdens. One comment noted that free market pricing and a short supply of C3PAOs combined with excessive waiting times may result in SMB attrition.

Response: It is not within in scope of this rule to address how companies recover assessment costs. The CMMC rule makes no change to the cost allowability parameters described in FAR 31.201-2 Determining Allowability.

Contractors are required to comply with all terms and conditions of DoD contracts, to include terms and conditions relating to cybersecurity protections and assessment requirements, as implemented by this rule. This holds true when a contract clause is flowed down to subcontractors.

Several of the commenters' recommendations have potential benefit for the contractor and sub-contractor communities; however, they are beyond the scope of the rule. These recommendations included creation or expansion of:
grants and assistance programs, financial support for small business, the DoD [Procurement] Toolbox, the DoD Office of Small Business Programs, contract incentives and free or reduced cost DoD cybersecurity services.

DoD understands the burden on small business. Nonetheless, DoD must enforce CMMC requirements uniformly across the Defense Industrial Base for all contractors who process, store, or transmit CUI. The requirements necessary to protect a single document are the same as to protect many documents, therefore scaling by amount of CUI expected is not a viable approach.

Solicitations for DoD contracts that will involve the processing, storing, or transmitting of FCI or CUI on any nonfederal system, regardless of the size or configuration of the nonfederal system, will specify the required CMMC Level (1, 2 or 3) and assessment type (self-assessment or independent third-party assessment). That requirement applies, regardless of the number of computers or components in a nonfederal information system.

DoD's original implementation of security requirements for adequate safeguarding of CUI relied upon self-attestation by contractors. Since that time, the DoD Inspector General and

DCMA found that contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information.

All contactors or sub-contractors with access to CUI need to be capable of protecting that information to the standard specified in 32 CFR part 2002. If a small business cannot comply with DFARS clause 252.204-7012 and NIST SP 800-171 R2, then that business should not be processing, storing, or transmitting CUI. DoD's programs, technological superiority, and best interests are not served if CUI is not consistently safeguarded by all who process, store, or transmit it.

28. Perceived Cost of CMMC Program

Comment: Several comments expressed disagreement with assumptions supporting the cost estimate, namely that implementation costs to comply with the requirements of FAR clause 52.204-21 and DFARS clause 252.204-7012 predate and are not included as CMMC costs. These comments assert that the cost of CMMC compliance should include those costs, and therefore dwarfs the cost of CMMC certification. They further assert that DoD's position does not account for those contractors who have only recently joined the DIB marketplace or those that aspire to do so. The concern expressed in the comments is that the cost of standing up an infrastructure to achieve and maintain DoD cybersecurity requirements regarding the protection of FCI and CUI, combined with CMMC assessment costs, is prohibitive and will create a lack of diverse suppliers.

Two commenters asserted the CMMC Program expanded application of DFARS clause 252.204–7012 requirements due to a perceived extension of those requirements to additional organizations, such as External Service Providers (ESPs). One of the commenters further speculated that CMMC requirements may decrease the availability of ESPs that are available and suitable to support DIB members as needed to comply with CMMC requirements. Another commenter stated that this scope expansion increases direct implementation and compliance costs above and beyond the CMMC Program's estimated assessment costs. The comment cites the introduction of the terms "Security Protection Assets" and "Security Protection Data" as extending applicability of those requirements and incurring the additional direct implementation and compliance costs. Lastly, the comment notes these changes will drive costs to "rip and replace" existing tools and likely purchase more expensive FedRAMP or CMMC-certified tools. One comment indicated that, while compliance with NIST SP 800-171 was required by December 31, 2017, compliance with NIST SP 800-171A Jun2018 increases requirements and cost because NIST SP 800-171A Jun2018 emphasizes process and documentation in addition to the intent of the security requirement.

Two comments pointed out that some contractors may need to accelerate remediation efforts and close out POA&Ms under existing DoD contracts that are subject to DFARS clause 252.2047012 to meet CMMC requirements. These comments requested that since these contractors will now be faced with accelerating close-out of their POA&Ms, which will incur additional costs, that DoD account for those costs in the estimate and potentially allow for recovery of those costs. One comment asserts that CMMC assessment failures, remediation implementation, and subsequent reassessments will be very costly in both time and money.

Response: 81 FR 72990, October 21, 2016 implemented the DoD's requirement that "contractors shall implement NIST SP 800-171 as soon as practical, but not later than December 31, 2017." Public comments related to costs for implementation were published with that final rule, along with DoD's responses. CMMC cost estimates are derived estimates based on internal expertise and public feedback in accordance with OMB Circular A-4 and are representative of average assessment efforts not actual prices of C3PAO services available in the marketplace. Market forces of supply and demand will determine C3PAO pricing for CMMC Level 2 certification assessments and how C3PAOs choose to distinguish their service offerings from other C3PAOs, including the timely availability of an assessment team, or re-assessments after an assessment failure. The size and complexity of the network within the scope of the

assessment impacts the costs as well. The DoD declines to speculate about how OSCs and C3PAOs negotiate mutually acceptable terms and conditions for assessment agreements.

OSA implementation of the requirements of FAR clause 52.204-21 and DFARS clause 252.204-7012 long predate CMMC and are not included in CMMC cost estimates, since those requirements are not driven by or attributable to CMMC, even for new or aspiring defense contractors, and have been in force since 2017 on DoD contracts that include the processing, storing, or transmitting of FCI or CUI in the performance of a DoD contract. The DoD has taken measures to make a self-assessment as straight forward as possible and provided guidance to mitigate any variance in assessment scores. Additionally, the DoD has streamlined CMMC requirements to align directly to NIST guidelines and has eliminated unique security practices to ease the burden on smaller companies. DoD must enforce CMMC requirements uniformly across the Defense Industrial Base for all contractors and subcontractors who process, store, or transmit CUI. Creation of a grants and assistance programs are beyond the scope of this rule. DFARS clause 252.204-7012 requires protection of security protection assets and security protection data. Section 1.1 of NIST SP 800-171 R2 states: "The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components." There is therefore no increase in the scope as described in the rule.

Security protection data requires protection commensurate with the CUI it protects and is based on how and where the security protection data is stored. The FedRAMP requirements for handling security protection data is therefore the same as that for handling CUI. Any impact to the cost of serving Government customers across the DoD is beyond the scope of this rule.

As NIST states in NIST SP 800-171A Jun2018, "The assessment procedures are flexible and can be customized to the needs of the organizations and the assessors conducting the assessments. Security assessments can be conducted as self-assessments; independent, thirdparty assessments; or government-sponsored assessments and can be applied with various degrees of rigor, based on customer-defined depth and coverage attributes." CMMC Program requirements are designed to ensure compliance with existing standards for protection of FCI and CUI and align directly to NIST guidelines (i.e., NIST SP 800-171 R2 and NIST SP 800-172 Feb2021) and the basic safeguarding requirements (of FAR clause 52.204-21) that apply to all executive agencies. The rule accounts for costs associated with assessment via NIST SP 800-171A Jun2018.

Within the limitations of section § 170.21 Plan of Action and Milestones Requirements, offerors may bid on a contract while continuing to work towards full CMMC compliance. DoD rejects the notion that organizations must "accelerate" to meet a requirement in place since 2017. DoD did not intend nor expect that POA&Ms would remain open-ended and unimplemented for years.

The DoD provided an analysis of costs to meet CMMC Level 1 and 2 requirements in the regulatory impact analysis for this rule. Certification is never required for CMMC Level 1, which is a self-assessment requirement. CMMC Level 2 may either be met via self-assessment, or via a C3PAO assessment, depending on the specific requirement cited in the solicitation. It is not within in scope of this rule to address the way companies recover assessment costs.

Verifying compliance with applicable security requirements may increase cost and is necessary for the protection of DoD FCI and CUI. The cost of lost technological advantage over potential adversaries is greater than the costs of such enforcement.

29. CMMC Benefits and Cost Estimates

a. Cost Estimate Assumptions

Comment: Some comments proposed the DoD directly assume the costs for industrial base compliance, increase contract award prices, offer grants and loans, or provide tax credits to offset the costs associated with compliance. One asked for clarification regarding allowable versus unallowable costs. One comment stated the cost estimate was a good guesstimate of the total cost to the USG, but the flow down costs and the price of doing business will be at the Program Office level. The commenter requested the DoD provide a table of Program Office funding

requirements to aid Program Managers in reflecting CMMC costs in an Acquisition Strategy and Cost Analysis Requirements Document (CARD).

A few comments asked about the assumptions used to estimate numbers of assessments by category and stated the labor rates for ESPs and C3PAOs were too low, and costs associated with small entities were incorrect. Two comments also suggested the number of hours estimated for self-assessment are too low, and three questioned the accuracy of small and medium sized business labor rates and asserted that the assessment costs for small businesses were not sustainable. One comment suggested that cost data in existing/past contracts should be used as a part of CMMC cost analysis and Section H costs should apply to the current CMMC cost estimate.

One comment claimed it is cost prohibitive for individuals to obtain a CCP or CCA certification, which will hamper the CMMC Program's scalability.

One comment requested the government elaborate on how the estimated 417.83 hours per response was derived for table 39, C3PAOs Level 1 Certification and Assessment, in section § 170.17(a). Another comment asserted that assessments conducted by Defense Technical Risk Assessment Methodology (DTRAM) assessment teams require more manhours than are anticipated for CMMC certification assessments.

One comment stated that while DoD included an estimate for annual senior official affirmations in the Regulatory Impact Analysis, it assumed a minimal number of hours will be required to complete this task which may not be adequate to complete a full compliance review.

One comment stated the DoD self-assessment resource allocations for an ESP for both CMMC Level 1 and Level 2 are estimated 125% to 175% too low based on the belief that a selfassessment should have more rigor than a gap analysis. Specifically, the commenter posed questions on what inputs from potential OSAs were used and identifying the rigor a Certifying Official would require for attestation. Recommendations include that the DoD clearly state its assumptions regarding self-assessment rigor, have OSA legal counsel review assumptions and cost factors, and identify a representative cross-section of stakeholders to determine appropriate rigor assumptions for company's ESPs and new to CMMC self-assessments.

One comment stated that the DoD's assumptions for the level of effort expressed as Director and staff IT specialist hours are too low. Although there are continuous monitoring requirements of NIST 800-171 R2, those requirements do not invoke the level of effort necessary for an executive to make an attestation corresponding to the level of personal risk and corporate liability incurred under the False Claims Act. The comment asserted that DoD's assumptions failed to account for an SMB to acquire and manage technical tools or manage the reaffirmation or an enterprise change management effort. The comment included several questions regarding the inputs used to determine lack of ongoing management resource requirements for reaffirmation, a risk management application, and inputs across the DIB regarding the level of assurance needed for affirmations to address liability concerns with the False Claims Act. Another recommendation suggested the DoD clearly state the degree of rigor an OSA should assume and revisit the cost assumptions involved to provide the Entity official with assurance for reaffirmation.

One commenter reviewed the CMMC AB's draft CMMC Assessment Process (CAP) document and agreed that 120 hours for a C3PAO's three-person team inclusive of Phases 1, 2 and 3 is appropriate for smaller companies and should be considered a lower bound for C3PAOs deployed resources but suggested the 156 ESP assessment hours should be decreased.

One comment highlighted the following rule text, "The total estimated Public (large and small entities) and Government costs associated with this rule, calculated in over a 20-year horizon in 2023 dollars at a 7 percent discount rate and a 3 percent discount rate are provided as follows," and asked how an organization could become eligible for the 7% discount.

One comment proposed DOD remove CMMC Level 1, or defer CMMC Level 1 implementation for several years, since it does not involve CUI. The comment stated CMMC Level 1 cost estimations and burden of compliance in the rule were greatly understated, that few companies subject to this CMMC level have any idea what is expected of them, and most will

struggle with financial, technical, and human resources. Though FAR clause 52.204-21 is widely used in Federal contracts, it has not been successfully communicated that NIST SP 800171A Jun2018 will be used. The comment concludes stating CMMC Level 1 does not include CUI, therefore making cost and compliance an excessive demand.

Response: Subsidizing costs for the defense industrial base compliance is not within the scope of this rule. The rule has taken several steps to keep the cost of compliance with the rule commensurate with the risk to the DoD's information. In addition, Level 1 only requires selfassessment, and many contracts with CUI will only require a Level 2 self-assessment. Companies that are currently and validly attesting that they meet DFARS clause 252.204-7012 should not have difficulty passing a Level 2 self-assessment.

Cost estimates provided in this rule were based on internal expertise, compliant with OMB Circular A-4, and informed by public feedback. Certain elements of the estimated costs will be influenced by market forces of supply and demand, which will determine C3PAO pricing for CMMC Level 2 certification assessments.

The number of assessments over the phase-in period were estimated using data from the Electronic Data Access system for the contracts containing DFARS clause 252.204-7012 in fiscal years 2019, 2020, and 2021, as well as data calculated for the initial CMMC Program. This data was used in combination with an expected growth factor to estimate DoD contracts and orders in the future. Data also showed the number of awards that were made to small entities and other than small entities. The resulting estimate was phased in over 7 years to allow the ecosystem to grow and accommodate an increasing number of assessments.

The assumptions and analysis of costs are provided in the regulatory impact analysis for this rule and are explained in depth. One of the assumptions is that Non-Small Entities have a team of full-time cybersecurity professionals on staff while Small Entities do not. The assumptions reflect Small Entities will likely obtain support from External Service Providers and have a staff member submit affirmations and SPRS scores for self-assessments (when applicable).

DoD included an analysis of costs to meet CMMC requirements in the regulatory impact analysis for this rule. As described in the estimate included with the rule, the major cost categories for compliance with CMMC requirements are anticipated to include costs for completing a self-assessment (e.g., Level 1 or 2); costs to prepare for and undergo C3PAO assessment (Level 2); costs required to implement the Level 3 security requirements and for preparing to undergo DCMA DIBCAC assessment (Level 3). Market forces of supply and demand will determine C3PAO pricing for CMMC Level 2 certification assessments. The CMMC rule does not make any change to cost allowability as defined in the FAR 31.201-2, Determining Allowability.

As addressed in the Assumptions section of the Regulatory Impact Analysis (RIA), the cost estimates for CMMC Levels 1 and 2 are based only on the assessment, certification, and affirmation activities that a defense contractor, subcontractor, or ecosystem member must take to allow DoD to verify implementation of the relevant underlying security requirements. For CMMC Level 3, cost estimates to implement applicable security requirements are included as they are a new addition to current security protection requirements. Section H costs of existing/past contracts do not apply.

CCP and CCA certification costs are set by the CAICO and are market driven.
The hours used in the cost estimations are based on estimates by subject matter experts. The 417.83 hours per response questioned by the commentor ties to C3PAO reporting and recordkeeping requirements for Level 2 certification assessment on small entities as identified in table 36, not Level 1 or table 39 as stated in the comment.

In response to public comments received in the initial 48 CFR CMMC interim final rule public comment period, DoD streamlined the CMMC model to ease the assessment burden. At the same time, estimates were increased for the time and cost of self-assessment based on industry and DIBCAC input. DoD estimates are based on defendable assumptions and documented labor rates. Therefore, DoD declines to modify the self-assessment estimates.

The DoD has streamlined CMMC requirements to align directly to NIST guidelines and eliminated unique security practices to ease the burden on smaller companies, included an analysis of costs to meet CMMC requirements in the regulatory impact analysis for this rule. The DoD declined to modify the estimates, which are intended to be representative and to inform rulemaking.

Verifying compliance with applicable security requirements may increase cost and is necessary for the protection of DoD CUI. The cost of lost technological advantage over potential adversaries is greater than the costs of such enforcement. The value of information (and impact of its loss) does not diminish when the information moves to contractors.

DoD rejected the recommendation to adjust the annual requirement for senior affirmations to a triennial requirement to decrease senior affirmation costs. The requirement for annual affirmations is to ensure the Affirming Official responsible for CMMC requirements are monitoring compliance with the requirements. If compliance is being maintained as required, this should not require more time or cost than provided in the estimates. Further, DFARS clause 252.204-7012 already requires NIST SP 800-171 continuous monitoring via requirement 3.12.3. DoD also declined to make the recommended edits to further delineate a company's internal review of self-assessments and reaffirmations in the cost assumptions.

The cost estimates provided for this rule represent average costs for companies to comply with the CMMC requirement, including the need for self-assessment or independent assessment against the specified standards. Whether the OSA elects to satisfy those requirements themselves, or by using one ESP for many requirements, or by using several ESPs for individual requirements, is a decision to be made by the OSA. That decision does not change DoDs estimate of average costs to meet CMMC requirements. The DoD declined to recalculate cost estimates using lower costs for ESP assessments.

The 7% discount rate is not a discount for organizations. The discount rate is a part of a formula used in a business impact analysis calculation. When calculating 20 years in the future, a discount rate is used to determine the net present value of money. Discount rates are explained in step seven of OMB Circular A-4: Regulatory Impact Analysis: A Primer.

The DoD does not agree with the commenter's assertion that the cost estimates greatly understate the costs and burden to Level 1 compliance. The 15 FAR security requirements that comprise CMMC Level 1 should already have the requirements implemented if an OSA network processes, stores, or transmits FCI. In addition to NIST SP 800-171A Jun2018, the CMMC Level 1 Assessment Guide provides supplemental information to help facilitate implementation and assessment of the Level 1 security requirements.

b. Economic Impact

Comment: One comment suggested the government evaluate the economic impact of implementing the rule's reporting requirements at scale. Another comment expressed the notion that the cost impact analysis does not account for the free market response, referring to the associated cost increases and schedule delays that directly impact the warfighter and taxpayer. The commentor suggested the cost could dwarf both the cost of implementing compliance and achieving certification.

One comment stated the CMMC Level 2 and Level 3 cost burdens for companies that were historically never subjected to such requirements may be disproportionate to the risk their operations pose to the inadvertent disclosure of CUI or FCI. It suggested ensuring requirements be proportional to the subcontractor's activity and risk levels. The comment further mentioned that costs may be passed on to the prime contractor, and DoD should consider providing recovery costs in the price of implementation.

One comment stated the 100% compliance to CMMC Level 2 certification may be financially unachievable and suggests if a risk assessment shows the likelihood of harm is comparatively low, the DoD should direct CMMC Program assessors to use their professional judgments and not require seeking maximum evidence of compliance where there is evidence of sufficiency.

Response: The DoD has already evaluated the reporting requirements and the analysis of the costs is provided in the Regulatory Impact Analysis published with this rule.
The DoD declined to respond to speculative or editorial comments about downstream impacts of the market's reaction to CMMC, all of which are beyond the scope of this rule.

The DoD declined the recommendation to restructure CMMC to be proportional to the subcontractor's activity and risk levels. DoD must enforce CMMC requirements uniformly across the Defense Industrial Base for all contractors and subcontractors who process, store, or transmit CUI. The value of information (and impact of its loss) does not diminish when the information moves to contractors and subcontractors.

Assessors exercise judgment in determining when sufficient and adequate evidence has been presented to make an assessment finding. This is consistent with current DIBCAC High Assessments and assessments conducted under the Joint Surveillance Voluntary Assessment (JSVA) program. Furthermore, to reduce burden to small businesses, the CMMC program has implemented flexibility with self-assessment, POA&Ms, and waivers.

c. Cross-Functional Requirements and Artifacts

Comment: Multiple comments maintained that DoD underestimated the cross-functional (Human Resources, Physical Security, Training, etc.) manhours and associated cost to collect artifacts and evidence in preparation for a C3PAO assessment. One comment stated the DoD's overestimation of CMMC Level 1 requirements would correspond to an underestimation of compliance costs. The comment referred to current NIST requirements and asserted that potential revisions would force changes to POA&Ms causing additional costs beyond those included in the estimates. The comment suggested the DoD should determine the range of potential compliance timelines, the use and value of existing and planned POA&Ms, and true certification costs, both for initial compliance as well as ongoing maintenance and oversight. One commentor claimed too much funding was expended over the past 5 years for the CMMC database system.

Response: OSCs prepare for C3PAO assessments based upon NIST guidelines as addressed in § 170.17. The cost and time estimates represent the time to gather the evidence to address all assessment objectives are derived averages based on internal expertise and public feedback in accordance with OMB Circular A-4 Regulatory Impact Analysis: A Primer. The size and complexity of the network within scope of the assessment impacts the costs as well.

The time estimates represent average derived estimates based on internal expertise and public feedback in accordance with OMB Circular A-4. The size and complexity of the network within scope of the assessment impacts the time estimates as well. The DoD does not concur with the commenter's claim that too much funding has been spent to develop the DoD's database for the CMMC Program.

d. Duplication or Overlap

Comment: One comment asserted CMMC requirements may be duplicative or conflict with existing utility industry compliance requirements that address CUI, since utility companies will not require CMMC Level 3 certification. They proposed the utilities and the DoD collaborate to harmonize requirements to limit the financial burden.
One comment highlighted a concern that cost for companies that have multiple contracts, each requiring different CMMC Program requirements. Concerns were specifically based on the increased costs from CMMC Level 2 to CMMC Level 3 compliancy and assuming costs would be borne by contractors. They expressed similar concerns about costs for FedRAMP certification, given a purported backlog in FedRAMP authorizations.

Response: Addressing the harmonization between the DoD, contractors, and subcontractors is beyond the scope of this rule. These are functions of the DIB Sector Coordinating Council and the DIB Government Coordinating Council. Additionally, non-DoD programs are outside the control and scope of the 32 CFR part 170 CMMC Program rule. The DoD encourages prime contractors to work with its subcontractors to flow down CUI with the required security and the least burden.

DoD is aware organizations may receive multiple contracts that may require different

CMMC levels based upon programmatic data security needs. It is beyond the scope of this rule to dictate how OSAs manage varying contract requirements. Contractors that have achieved a CMMC Level 2 or Level 3 certification automatically meet a stated requirement of a lower CMMC level if the same system/assessment scope will be used in performance of the contract.

30. Alternatives

a. Alternate Programs

Comment: Many comment submissions included lengthy proposals for alternatives to the CMMC program purported to alleviate specific concerns with aspects of CMMC program requirements. In some cases, the concerns were based on a misreading of the rule's content. The DoD has addressed some valid concerns through rule revisions that differ from the recommendations.

One commenter suggested eliminating compliance assessments in favor of establishing a DoD office to conduct penetration testing of each DIB company's network every two years. Other commenters also recommended the DoD establish a secure portal and share CUI with contractors only through that portal, as a way for the DIB to avoid the cost of securing their information systems. One commenter suggested the DoD monitor use of waivers and utilize this secure portal approach when CMMC waivers apply. Similar recommendations included sharing CUI only through password encrypted files or requiring contractors to store CUI in restricted access folders. In similar suggestions, several commenters thought the DoD should provide its contractors with training, GFE and other tools necessary to secure the contractor owned information systems being used to process or store CUI. One such commenter stated that the Government should appropriate funding for secure solutions rather than phasing in compliance assessments. One commenter suggested the DoD consider industry's application of alternate security mechanisms in lieu of CMMC Levels 2 and 3. Another recommended the DoD stand up a voluntary DIB Cyber Protection Program to improve real-time monitoring of the DIB, improve cybersecurity for firms that cannot afford the needed professional staff, and offer data and legal protections to DIB firms. Another such commenter suggested that DoD fund securing the DIB through contract incentives.

One commenter recommended mandating DIB use of the DoD CIO's DIB CS Program or other DoD cybersecurity related services as alternatives to the CMMC program. That comment suggested reassigning Government personnel to provide training for all assessors, to reduce training cost and ensure enough assessors to meet demand. Another commenter made similar recommendations about CISA cybersecurity service offerings.

Response: Many comments included lengthy proposals for alternate approaches to the CMMC program which would alleviate specific concerns with aspects of CMMC program requirements. In some cases, the suggestions were based on a misreading of the rule's content. The DoD has addressed some valid concerns via rule revisions that differ from commenter recommendations.

The DoD notes with interest one commenter's reference to initiatives described in a report to Congress about the breadth of cybersecurity related initiatives within the Department. While the CMMC is an important initiative, it is by no means the Department's only effort to improve DIB cybersecurity. The CMMC Program addresses adequate safeguarding of contractor owned information systems which process, store, or transmit FCI or CUI. Other DoD initiatives related to secure cloud or software development environments are beyond the scope of the CMMC Program.

The DoD did not adopt suggested alternatives, such as policy-based solutions that lack a rigorous assessment component. The DoD determined that sharing CUI only through DoDhosted secure platforms, in lieu of implementing the CMMC Program, was not a scalable or costeffective solution. Although the DoD expanded the availability of resources through the DIB Collaborative Information Sharing Environment (DCISE) program, the DoD also declines to rely only on training in lieu of assessment.

The purpose of CMMC is to require defense contractors and subcontractors to undergo an assessment to verify the implementation of prescribed cybersecurity standards. The security requirements are already specified in existing regulations (32 CFR part 2002, DFARS clause 252.204-7012, and FAR clause 52.204-21).

Comments which suggest that enrollment in the DoD's DIB CS Program can be an alternative means of meeting the objectives of CMMC misinterpret the services that the DIB CS Program provides. The DIB CS Program does not provide any mechanism for verifying whether those participants have secured their contractor owned information systems to the standards required by DFARS clause 252.204-7012. Likewise, the recommended NSA cybersecurity offerings also do not provide the same verification mechanism that CMMC will provide. CMMC Program requirements apply to contractor-owned information systems that process, store, or transmit FCI and CUI. Hardware and software approving authorities for GFE are not relevant to this CMMC rule. The DoD declined to adopt the recommendation to provide GFE to DIB contractors to maintain security, ownership of data and support Clinger-Cohen Act compliance.

Some comments received reflect a misinterpretation of the cost estimates that accompany this rule, which are intended to inform the rulemaking process. The cost estimates are not indicative of a funded budget line which could be reprogrammed to fund a new agency to meet the objectives of the CMMC Program. Comments recommending that funding be appropriated (by Congress) to provide the DIB with security solutions are beyond the scope of this rule.

b. Alternate Standards

Comment: One commenter recommended aligning requirements to DoD policies rather than to NIST standards and relying on FISMA compliance assessments in lieu of the CMMC model. Another commenter recommended the DoD and NIST work with other international standards organizations to incorporate CMMC requirements (really NIST standards) into existing ISO/IEC and CMMI standards. In general, these commenters recommended DoD accept alternate assessments conducted against alternate standards by assessors with alternate training and qualifications. They further recommended that DoD issue an RFI seeking recommendation of alternate third-party assessment schemes. One commenter recommended the rule be modified to require that contracts with a CMMC level 3 requirement also require use of a FedRAMP moderate or higher CSP, and that contracts with a CMMC level 2 requirement permit use of CSPs with either FedRAMP Moderate authorization (or higher) or CMMC level 2 or 3 certification assessment.

Response: CMMC is based on the executive branch's CUI Program as the authoritative source, as codified in 32 CFR part 2002. The definition of CUI and general requirements for its safeguarding are included in 32 CFR 2002.4 and 2002.14, respectively. 32 CFR 2002.14(h)(2) specifically requires that "Agencies must use NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems…" The CMMC Program makes no change to the CUI program or its implementing policies. Contractually, DFARS clause 252.204-7012, effective since December 2017, requires contractors to implement the NIST SP 800-171 security requirements to provide adequate security applicable for processing, storing, or transmitting CUI in support of the performance of a DoD contract. That requirement applies, regardless of the number of computers or components in a non-Federal information system.

The CMMC Program provides an assessment mechanism to verify that prospective offerors comply with the applicable information security requirements. All executive agencies are required to follow the policies described in 32 CFR 2002.14. DoD aligned CMMC requirements with NIST SP 800-171 R2 because it is enterprise focused and is already required in DoD contracts when DFARS clause 252.204-7012 is applicable. DFARS clause 252.204-7012 and NIST SP 800-171 R2 provide the cybersecurity requirements, whereas CMMC validates implementation of those requirements. CMMC does not duplicate these documents.

The DoD publishes Security Technical Implementation Guides (STIGs) for specific products, primarily to guide secure implementation in DoD systems. The OSA is responsible for creating

the implementation guidance they will use to meet the CMMC security requirements. OSAs are free to use the DoD STIGS if they feel they are appropriate. The DoD does not want to limit the choices available to the OSA for implementation guidance. In addition, the DoD declines to create STIGs for all products that might be used in the OSA's environment. Some comments lacked relevance to the rule's content, which is limited to specific CMMC program requirements.

Changes to DFARS clause 252.204-7012 are outside the scope of this rule. DoD declines to modify CMMC Level 2 or Level 3 requirements related to use of Cloud Service Providers (CSP). A CSP is assessed against the FedRAMP Moderate baseline. This is required when a CSP, regardless of the component or type of CSP, processes, stores, or transmits CUI.

The DoD declines to align CMMC requirements to alternate standards or accept compliance with alternate standards in lieu of the NIST SP 800-171 standard mandated by 32 CFR part 2002 for the protection of CUI. CMMI is focused on improving the software development process, while CMMC is focused on verifying the proper implementation of DIB cybersecurity requirements. Incorporating requirements into new or other existing standards would unacceptably delay action to improve DIB cybersecurity. The DoD must take action to improve DIB cybersecurity, regardless of the global state of cybersecurity. DoD's publication of this rule follows completion of OMB's formal rulemaking process, which includes both DoD internal coordination and Interagency coordination. The recommendation for the DoD to establish a voluntary DIB Cyber Protection Program is beyond the scope of this rule.

One commenter recommended administrative edits to identify CMMC levels at a particular place in the pre-amble description of the program. The preamble is not part of the official regulation. In addition to background and overview information about the proposed or final rule, the preamble includes responses to all comments received during the public comment period on the proposed rule. The certification requirements are in subpart D, §§ 170.15 through 170.18.

c. Alternate Implementation Timelines

Comment: Several commenters suggested that DoD abandon CMMC requirements in favor of simply continuing to rely upon self-assessments, or else allowing contractors to comply with DFARS clause 252.204-7012 requirements absent any assessment (self-conducted or thirdparty). Of those recommending self-assessment, two commenters limited the suggestion only to companies that self-certified as small businesses and one further recommended that DoD pay for certification assessment of all small businesses. One such commenter based their opinion on an interpretation that text in NIST SP 800-171 R2 identifies the requirements as a model for selfassessment. Another commenter made no suggestion to change assessment requirements, other than to implement them post-award, rather than pre-award.

One comment expressed doubt in the ability of the ecosystem to scale sufficiently to meet the demand for C3PAO assessments and assessor training.

One commenter suggested the rule be revised to eliminate POA&Ms but expand the period during which deficiencies can be reassessed from within 10 days of initial assessment to 60 days for those prospective contractors. Another commenter suggested varying timelines for POA&Ms based on a variety of criteria, including how many DoD contracts are held.

Response: The DoD declined to accept the risk associated with implementing CMMC solely as a post-award requirement. When contracts require contractors to process, store, or transmit CUI, DoD requires that they be compliant with DFARS clause 252.204-7012 and competent to adequately safeguard CUI from the beginning of the period of performance. DoD declines the recommendation to require primes to assume the cost of CMMC for their subcontractors. Arrangements between contractors and subcontractors are negotiated directly between those parties. The DoD does not accept the recommendation to eliminate or change the criteria for POA&Ms or the timeline allowed to remediate open POA&M items. The 180-day period allowed for POA&Ms and the determination of which weighted practices can be placed on a POA&M was a risk-based decision. The determination considers the relative risk DoD is willing to accept when a particular practice is not met and the amount of risk the DoD is willing to accept for those security practices that go "NOT MET" for an extended period.

The Department declines to adopt the recommendation to allow DIB members to assist in designing the DoD's mechanism for assessing DIB compliance with DoD's contractual requirements. In developing the CMMC program, the DoD sought and considered DIB input. DoD disagrees with the comment that there is a lack of scalability in the CMMC program. The phased implementation plan described in § 170.3(e) is intended to address any CMMC Ecosystem ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements. The rule has been updated to add an additional six months to the Phase 1 timeline. As with all its programs, the Department intends to effectively oversee the CMMC Program and act as needed to manage its effective implementation. Although the full extent of DoD's oversight process is beyond the scope of this rule, the rule text addresses DoD's authority to waive the application of CMMC requirements when warranted in accordance with all applicable policies, procedures, and approval requirements.

DoD has utilized a phased approach to the rollout to reduce implementation risk. CMMC Program requirements make no changes to existing policies for information security requirements implemented by the DoD. It is beyond the scope of this rule for DoD to determine the order in which organizations are assessed.

d. Alternate Assessors or Assessments (including Self-Assessment Only)

Comment: One commenter submitted numerous recommendations based on an opinion that skills required for conducting CMMC compliance assessments are like those required for conducting Independent Technical Risk Assessments (ITRAs) on Major Defense Acquisition Programs (MDAPs). Such assessments are conducted by the Office of the Undersecretary of Defense for Research & Engineering (OUSD(R&E)) in accordance with Defense Technical Risk Assessment Methodology (DTRAM) criteria. These criteria extend beyond compliance with cybersecurity requirements and include characteristics such as modular open systems architecture, software, manufacturing, reliability, availability, maintainability, and others. This commenter noted the DoD's Adaptive Acquisition Framework applies to both Information Systems and National Security Systems and suggested that existing acquisition requirements pertaining to ITRA and DTRAM should suffice in lieu of CMMC assessments. The commenter recommended that DoD use existing ITRA teams to perform compliance assessments of contractor-owned information systems. In addition, they recommended aligning requirements to DoD policies rather than to NIST standards. Other comments made similar suggestions to synchronize cybersecurity requirements with DoD policies rather than NIST standards but cited FISMA compliance assessments as the appropriate model rather than the DTRAM.

One comment suggested that C3PAOs be permitted to conduct partial assessments of ESPs, MSPs, and MSSPs. Multiple comments expressed concern with CMMC assessment requirements for OSAs that use ESPs, stating that OSAs would be unlikely to know which components of the services they purchased were covered by a required CMMC Level 2 assessment. This commenter recommended the creation of a separate type of CMMC assessment specifically for ESPs, which they further recommended should be highlighted on the CMMC AB marketplace to assist OSAs in selecting an appropriately vetted ESP. These comments provided an extended description of the specific scoping guidance that should be adding to existing CMMC supplemental documentation, as well as several sample scenarios explaining how requirements for this new type of assessment should be applied. Two comments highlighted that the rule's preamble does not include details of assessment and implementation requirements.

Several commenters recommended the DoD abandon the CMMC ecosystem model and conduct all cybersecurity compliance assessments using DIBCAC assessors, which would reduce cost to the DIB. One such commenter suggested that DIBCAC assessment of C3PAOs, as part of the accreditation process, detracts from DIBCAC's capacity to perform CMMC level 2 assessments for the DIB. Another noted that as Government employees, DIBCAC assessors could exercise judgement to make risk-tolerance decisions that non-Government C3PAOs cannot, including possible acceptance of partial non-compliance.

Response: DoD must enforce CMMC requirements uniformly across the Defense Industrial Base for all contractors and subcontractors who process, store, or transmit CUI. The value of information and impact of its loss does not diminish when the information moves to contractors and subcontractors. The DoD has considered the recommendation and declines to revise the rule text to rely solely on self-assessment or eliminate the 3-year validity period to rely on a one-time certification. It is important that contractors maintain security compliance for systems that process, store, or transmit DoD CUI. Given the evolving cybersecurity threat, DoD's best interests are served by ensuring that CMMC Level 2 assessments remain valid for no longer than a 3-year period, regardless of who performs the assessment.

CMMC Program requirements in this rule are designed to improve compliance with requirements for safeguarding of FCI and CUI. DoD has privity of contract to enforce these requirements and CISA does not. OSAs are free to choose CISA services as part of their implementation of DoD requirements. FISMA is for Federal systems that are used by Government personnel or the public and is therefore an unsuitable surrogate for CMMC requirements. If a contractor provides outsourced IT services to a Federal agency, the system is considered a Federal system and FISMA applies. In contrast, CMMC requirements apply to nonfederal systems that are used internally by contractor personnel.

The DoD disagreed with the commenter's assertions about NIST SP 800-171 R2 and the available assessment methods. DoD's DIBCAC currently performs assessments using the procedures in NIST SP 800-171A Jun2018, and these documents explicitly identify the target audience to include individuals with security assessment responsibilities, such as auditors, assessors, and "independent verifiers". The aggregated SPRS reporting and scoring is CUI. The DoD does not wish to make this information public, which might aid adversaries in coordinating their attacks.

The CMMC Program does not alleviate or supersede any existing requirements of the Adaptive Acquisition Framework, nor does CMMC alter any statutory or regulatory requirement for acquisition program documentation or deliverables.

One commenter referenced assessments required during the acquisition process for DoD systems. DoD's policies governing acquisition programs require that Independent Technical Risk Assessments be conducted on Major Defense Acquisition Programs. These assessments provide a view of program technical risk and are not well-suited to the assessment of contractor owned information systems against standards for safeguarding CUI. CMMC assessments are conducted on contractor owned information systems to gauge compliance with FAR and DFARS requirements for safeguarding FCI and CUI that is processed, stored, or transmitted within those contractor-owned information systems. One commenter incorrectly asserts that the CMMC Scoring Methodology does not parallel existing scoring methods, however the CMMC methodology is based on the DoDAM.

The DoD declined to accept the recommended alternative of self-assessment with the potential to require DIBCAC assessment for a sampling of DoD contractors, which is essentially the status quo. Both GAO reporting and other DoD analysis have shown that the DIB has not consistently implemented the NIST SP 800-171 requirements needed to comply with DFARS clause 252.204-7012, even though DoD's objective was for the contactor to implement NIST SP 800-171 as soon as practical, but not later than December 31, 2017.

The DoD reserves the right to decide when reliance on self-assessment will suffice, and when compliance should be assessed through CMMC certification. Based on DoD decision criteria that includes a risk assessment of the type and sensitivity of program information to be shared, Program Managers will identify the appropriate CMMC requirement (e.g., CMMC Level 2 selfassessment or Level 2 certification) in the solicitation.

The government does not have the capacity in house to adequately assess the 220,00+ companies in the DIB. The DoD cannot assume the workload of directly assessing every DIB contractor. With this final rule, DoD established a scalable way to verify, through assessment, that contractors have implemented required security measures necessary to safeguard DoD information. The DIBCAC's mission is derived from DoD priorities and the Department is

actively working to ensure that the DIBCAC is adequately resourced to effectively execute its mission areas. Planned changes to DCMA staffing levels have been considered and are necessary to implement the elements of the CMMC program described in this rule (i.e., Level 3 and C3PAO assessments).

By design, the CMMC Program depends on the supply and demand dynamics of the free market, enabling it to naturally scale and adapt to capacity requirements. The DoD established requirements for each part of the CMMC ecosystem to support a robust compliance assessment mechanism for DoD's contractual requirements to safeguard CUI that is processed, stored, or transmitted in contractor owned information systems. The DoD cannot assume the workload of directly assessing every DIB contractor.

One commenter provided numerous comments expressing concern that OSAs that use ESPs will be unlikely to know which ESP services require CMMC assessment within the OSAs boundary or scope. This commenter recommended an alternate type of CMMC assessment specifically for ESPs. In lieu of adopting that recommendation, the DoD has updated the rule in §§ 170.19(c)(2) and (d)(2) to reduce the assessment burden on ESPs.

DoD declined to allow partial CMMC Assessments. ESPs may request voluntary CMMC assessments of their environment and use that as a business discriminator. The marketplace for ESP services will adjust to find the efficient manner for ESPs to support OSA assessments.

e. Alternate Governance

Comment: Rather than abandon the CMMC ecosystem model entirely, some commenters recommended only that DoD revise the CMMC Accreditation Body's roles and responsibilities. Three recommended the DoD eliminate the CMMC AB and take on its responsibilities; of these, one further suggested the DoD publish detailed Security Technical Implementation Guides describing how to implement the applicable NIST requirements. One commenter questioned the reasons for creating a CMMC AB rather than accepting another existing accreditation body or multiple accreditation bodies. One comment expressed doubt in the ability of the ecosystem to scale sufficiently to meet the demand for C3PAO assessments and assessor training.

Multiple comments called for organizations other than the current CMMC AB to run the CMMC ecosystem such as a CMMC Advisory Council or a Civilian Cybersecurity Corps comprised of government and private sector staff. One such comment requested that, unlike the current CMMC AB, the proposed body would be funded and managed by the government. Two commenters recommended the DoD consider accepting other types of conformance assessment such as ISO/IEC 27001:2022(E) and Health Information Trust Alliance (HITRUST) certification. One noted this would require guidance to describe how to address the gaps between standards those assessments are aligned to and those that CMMC are aligned to (e.g., NIST SP 800-171 R2 for CMMC Level 2). This commenter further suggested that DoD accept alternate industry certifications in lieu of the training requirements identified for CMMC Assessors. One commenter suggested the DoD accept FedRAMP authorization to meet CMMC assessment requirements.

Response: DoD considered many alternatives before deciding upon the current CMMC structure. The DoD established requirements for a CMMC Accreditation Body, and this accreditation body will administer the CMMC Ecosystem. The DoD reviewed and assessed the whitepapers that were submitted by RFI respondents and determined that no single respondents could meet all the broad facets required to serve as the CMMC Accreditation Body. Based on this assessment, the DoD published notice of a planned meeting in November 2019 to allow the respondents and other members of the public to hear the senior DoD leadership address DoD perspectives regarding the notional CMMC implementation flow; the notional program structure; the notional CMMC Accreditation Body activities, structure, and relationship with the DoD; and the notional CMMC implementation schedule. The DoD also provided information regarding the Department's planned way forward. The result of the November 2019 meeting was the establishment of the current CMMC Accreditation Body. The relationship between the current CMMC Accreditation Body and the DoD was formalized through a Memorandum of

Understanding and then a No-Cost Contract. The DoD cannot assume the risk or the workload of directly managing the CMMC Ecosystem or the other alternatives suggested. The current CMMC Accreditation Body is aligned to the DoD through contractual arrangements.

31. Rulemaking Process

Comment: Some comments were submitted to identify problems with using the Federal eRulemaking Portal (at www.regulations.gov) or the *Federal Register* web site and did not address content of the proposed rule. One commenter was confused by the identification of the rule as "Proposed" rather than final. Another asked whether the rule could be republished with page numbers.

Many comments critiqued the format, heading and section numbering, use of incorporation by reference, or sections contained within the rule, rather than the substance of the content. For example, some comments described the CMMC rule as overly repetitive or containing duplicative sections. Some comments recommended deleting specific sections to shorten or simplify the rule, including "History of the Program". Some commenters perceived the preamble to the rule as unnecessary and recommended deleting or shortening that section. In addition, one commenter noted that responses to public comments received against an earlier CMMC rule publication ought to be published with the 48 CFR part 204 CMMC Acquisition rule rather than this 32 CFR part 170 CMMC Program rule. Several commenters simply thought the rule text too verbose and recommended rewriting the content with fewer words and simpler language or using tables to shorten the content. One comment criticized the organization of the documents.

Several comments addressed references to documents outside the rule, or those that are incorporated by reference. One commenter asked how the DoD will recognize when revisions to documents incorporated by reference cause them to be misaligned requirements identified in this rule. Other comments requested that additional documents be incorporated by reference, such as DoD Instructions on CUI and the DISA Cloud Security Technical Reference Architecture. Some commenters complained that the page count of the rule and documents incorporated by reference was too high and asked whether contractors are expected to read them all. Two commenters objected to certain terms in the definitions section pointing to other documents as the source of the definition. One further suggested that such definitions be revised to simply point to the URL of the source definition.

Some comments recommended moving content from the new 32 CFR part 170 CMMC Program rule to the CMMC supplemental documents or changing citations to reference them rather than the NIST documents that are incorporated by reference. Another asked why the scoring methodology was incorporated into the rule, rather than incorporated by reference. One comment questioned whether the supplemental documents are truly optional, rather than required for compliance with CMMC program requirements. One comment stated a public comment period should be required for all supplemental guidance prior to final publication.

One commenter asked what precipitated implementation of the CFR, which the DoD interpreted as a question about codification of the CMMC program in the CFR. One commenter asked whether the rulemaking process had afforded a certain group the opportunity to coordinate or comment on the rule. Another referenced the separate 48 CFR part 204 CMMC Acquisition rulemaking effort needed to implement the content of this rule and urged the DoD to consider public comments of both rules prior to their publication as final.

One comment specifically suggested the CMMC program be implemented Governmentwide. One commenter simply submitted a copy of a CMMC-related article from the February 2024 issue of National Defense Magazine and quoted or extracted from it rather than providing any specific comment or question.

Response: The process for creating Federal regulations generally has three main phases: initiating rulemaking actions, developing proposed rules, and developing final rules. A proposed rule is published for public comment prior to developing the final rule. A final rule must identify its effective date and be published 60 days prior to that date. The structure and formatting

requirements for proposed and final rules and the process for submitting public comments are prescribed by the Office of the Federal Register and OMB, respectively, and are outside of DoD's control.

OMB approved publishing the CMMC rule as a Proposed Rule. It has undergone a required notice-and-comment process to give the public an opportunity to submit comments. The Proposed Rule and the comments received informed the final rule. Issues with the *Federal Register* or www.regulations.gov functionality for submitting comments via attachment of pdf or other file type were raised with the appropriate help desk and resolved before conclusion of the public comment period. The public comment period for this rule permitted review and feedback from any member of the public.

This rule follows the format and includes all sections required in OMB guidelines for formal rulemaking. The length of this rule is necessary to ensure all affected parties have sufficient information to understand and comply with the rule. *Federal Register* page numbers are visible when viewing the PDF version of the rule published Tuesday, December 26, 2023 (88 FR 89058; www.govinfo.gov/content/pkg/FR-2023-12-26/pdf/2023-27280.pdf).

Material published in the *Federal Register* contains numerous sections, including portions that do not amend the CFR. Specifically, the preamble for this rule, is written in a summary format and is not intended to provide the detailed information that is in the regulatory text.

DoD declines to delete reserved sections because the editorial standard for orderly codification is that for every (a) there must be at least a (b), and for every (1) there must be at least a (2), etc. "Reserved" meets this standard when there is no additional text required. The DoD declined to make other administrative changes, because the recommendations did not result in a substantive change.

One commenter correctly identified that the initial 32 CFR part 170 CMMC Program proposed rule included discussion and analysis of comments made against prior publication of a 48 CFR CMMC interim final rule. The decision to include that material was made for the public's convenience and to facilitate greater understanding of the 32 CFR part 170 CMMC Program proposed rule and the CMMC Program. Codification of the CMMC Program requires publication of both the 32 CFR part 170 CMMC Program final rule and the 48 CFR part 204 CMMC Acquisition final rule. Each of those final rules will include a discussion and analysis of public comments received during their respective comment periods. The DoD CIO worked in conjunction with OUSD(A&S) to ensure that the 32 CFR part 170 CMMC Program rule and the 48 CFR part 204 CMMC Acquisition rule are in sync.

The preamble is not regulatory text. The preamble includes a response to the significant, relevant issues raised in previous public comments on the original CMMC program. DoD declines to adopt recommendations to move content from the 32 CFR part 170 CMMC Program rule to the supplemental documents, which are not codified. As such, the supplemental documents are provided for optional use, and the regulatory text takes precedence. The CMMC Assessment Process (CAP) guidance is a product of the Accreditation Body and is not codified in the CFR as part of the CMMC rule, and the regulatory text in part 170 takes precedence.

Comments on the CMMC Supplemental Guidance were received as part of the public comment period review. Final versions of these documents were published with this rule. Other supplemental materials published by the Accreditation Body do not convey government direction and are therefore do not require rulemaking. Supplemental documents (e.g., CMMC assessment and scoping guides) are not codified in the CFR as part of the regulatory text. To codify CMMC program requirements, content must be included in the 32 CFR part 170 CMMC Program rule text. DoD developed the CMMC Assessment Guides to provide supplemental information to the public offering added clarity on the intent of the NIST SP 800-171A Jun2018 and NIST SP 800172A Mar2022 guides. The CMMC Assessment Guides are particularly important for security requirements with organization-defined parameters (ODPs) (e.g., CMMC Level 3). There is no requirement to use the supplemental guidance documents.

Office of the Federal Register (OFR) regulations, at 1 CFR part 51, govern the IBR process. IBR is only available if the applicable regulations are published in the *Federal Register* and

codified in the CFR. When incorporated by reference, this material has the force and effect of law, as do all regulations published in the *Federal Register* and codified in the CFR. 1 CFR part 51 requires the specification of a revision to a standard, for example NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Revision 2, February 2020 (includes updates as of January 28, 2021), which is incorporated by reference in this rule. The DoD will determine when to update this rule after documents incorporated by reference have been revised. Per OFR guidance, § 170.4 points to other sections of part 170 where applicable and repeats definitions for terms incorporated by reference.

Contractors complying with CMMC requirements need to be familiar with those documents that are incorporated by reference. The definition of subcontractor is not incorporated by reference, but rather points to a definition codified in 48 CFR 3.502-1, as recommended in OMB guidelines for formal rulemaking. DoD has determined that the Defense Information Systems Agency's Cloud Security Technical Reference Architecture does not meet the criteria for approved IBR material. However, the rule has been updated to use a different definition for Cloud Service Provider. The requirements of NARA's CUI program (32 CFR part 2002) and DoD's implementing policies for identifying and managing CUI are beyond the scope of the CMMC rule.

The CFR is the codification of the Federal Government's rules and regulations published in the *Federal Register*. The CFR was created with the passage of the Federal Register Act and amended in 1937 to provide a "codification" of all regulations at least once a year. The CFR reflects the tenet that the Federal Government must follow an open public process when rulemaking.

Due to the broad application of CMMC requirements for DoD acquisition support by the defense industrial base, the Department determined that codifying the CMMC Program and its associated requirements in 32 CFR part 170 CMMC Program rule (for national defense and security) was needed in conjunction with the corresponding DFARS contractual requirements codified in 48 CFR part 204 CMMC Acquisition rule.

The DoD has no authority to make CMMC a Federal-wide program. The notice of the required CMMC level is provided at time of solicitation. This does not prohibit contractors from pursuing CMMC assessments prior to receipt of a solicitation.

DoD declines to comment on the reposting of information being reported in the media. ***32. Administrative changes to Terms, References and Notations***

Comment: Over 160 comments asked for clarification of terminology or the addition, removal, or modification of a definition. Most requests focused on Security Protection Data and Assets, Senior Officials, Information System, External Service Providers, Cloud Service Providers, Managed Support Providers, Internet of Things, CMMC Security Requirements, Organization Seeking Assessment, and Organization Seeking Certification. Numerous comments recommended the following terms could be clarified, expanded, or defined: "Defense Industrial Base", "personal information", "contractor", "sub-contractor", "Prime Contractor", "equipment", "contractor information system", "Information System", "system" "Information Resource", "CMMC Approved Training Materials (CATM)", "CMMC Certified Instructor (CCI)", "Provisional Instructor (PI)", "cyber incident", "Accreditation Body", "Assessment Findings Report", "Organizationally-Defined", "Organizationally-Defined Parameter (ODP)", "Periodically", "Risk Assessment", "Risk Analysis", Supervisory Control", Data Acquisition", "Operationally Critical Support", "System Security Plan (SSP)", "TTP", "CMMC", "COTS", "NARA","C3PAO" "IS", NSS", "Technology Asset", "Personnel Assets", "Asset Categories", "DIBCAC High", and "Enterprise".

Response: All requests for changes to terminology definitions, references, and usage have been reviewed. In response, many terms were updated in § 170.4 Acronyms and definitions. The DoD determined those terms that were not changed to be sufficiently defined and appropriately referenced, and the requested administrative changes would not have resulted in a substantive change.

a. SPA/SPD/Asset:

Comment: Numerous comments asked the DoD to expand on the definition, explanation, and guidance for Security Protection Data (SPD) and Security Protection Assets (SPA). Several other comments requested that the rule and supplemental documents add or expand definitions for "Asset", including various specific types of assets like "Technology Assets", "Personnel Assets", "Organizational Assets" "Specialized Assets". Some comments asked to modify the definition for "Security Protection Asset", "CUI Asset", "FCI Asset", and "Out-of-Scope Assets".

Response: The DoD modified the rule to add a definition for "Security Protection Data (SPD)." The DoD considered the NIST definitions for "System Information" and "Security Relevant Information" in the development of the new SPD definition. CMMC does not regulate the OSA's SPD, but instead implements existing regulatory requirements for the safeguarding of CUI. The DoD does not agree with the statement that the ESP definition conflates SPA with CUI assets. The definition of Security Protection Assets is consistent with its application in the NIST SP 800-171 R2 abstract. The phrase "FCI Assets are part of the Level 1 CMMC Assessment Scope and are assessed against all CMMC Level 1 requirements" was removed from the rule. The DoD declined to rephrase the term "CUI Assets." The DoD reviewed the recommended edit and declined to make an update to "Out-of-Scope Assets." The definition, as written, provides a clear distinction with Security Protection Assets (SPAs).

b. Senior Official:

Comment: Several comments asked for additional definition or guidance about the Senior Official role.

Response: The DoD modified the rule to replace all references to the "Senior Official" with "Affirming Official" and provided additional clarity on this term. It is beyond the purview of the DoD to define technical qualifications for an OSA Affirming Official.

c. ESP/CSP/MSP

Comment: Some comments asked for additional clarification of the terms related to External Service Providers (ESPs) and Cloud Service Providers (CSPs). Two comments requested the rule add a definition and acronym for "Managed Service Provider".

Response: The DoD received numerous comments about the use of ESPs which do not process, store, or transmit CUI. In response to these comments, the DoD modified the rule to reduce the assessment burden on ESPs. An ESP that utilizes staff augmentation, where the OSA provides all processes, technology, and facilities, does not require a CMMC assessment. The rule was also updated to add a definition of "CSP" that is based on the NIST SP 800-145 Sept2011 definition of cloud computing. The term "Managed Service Provider" is not used in the rule; therefore, the acronym was removed from § 170.4.

d. IoT/OT/ICS:

Comment: Several comments recommended DoD clarify the definition of IoT, OT, and ICS. Regarding IoT, one comment requested the rule specify that the exchange of data and information between devices occurs over the internet.

Response: As specified in the rule, IoT, IIoT, and OT, are Specialized Assets, and all requirements associated with Specialized Assets apply to any equipment that processes, stores, or transmits CUI but is unable to be fully secured. The description of Internet of Things (IoT) in the level 2 and level 3 Scoping Guides is consistent with the definition of IOT in § 170.4 and is defined in NIST SP 800-172A Mar2022. Scoping Guide text also provides examples to help clarify what types of devices may be IoT. The definition of OT is from NIST SP 800-60 V2R1 and the definition of ICS is from NIST SP 800-82r3. Requests for revisions to these definitions should be addressed to NIST. OSAs determine the asset categories and assessment scope based on how and where they will process, store, and transmit FCI and CUI. The DoD declined to comment on individual use cases included in the comments.

e. Program and Security Requirements:

Comment: Two comments asked for a definition of "Security Requirements" while another asked for the DoD to define the term "CMMC Program requirements" in the rule. Three comments addressed concerns with the CMMC security practices numbering scheme in §§

170.14(c)(i). One comment requested clarification on what constitutes a "priority" program. Another commenter stated the term "all applicable CMMC security requirements" is ambiguous and many OSAs will only attest to fulfilling the FAR 52.204–21 or NIST SP 800-171 R2 security requirements. The commenter felt this could lead to a significant disconnect at CMMC Level 2 since Level 2 includes security requirements associated with the use of ESPs, as defined in DFARS clause 252.204–7012 paragraphs (e.g., para (b)(2)(ii)(D)) and the DoD CIO FedRAMP Equivalency memorandum.

Response: CMMC Program requirements are all the requirements codified in the 32 CFR part 170 CMMC Program rule. The term "CMMC Security Requirements" is defined in § 170.14(c). The CMMC supplemental guidance documents add clarity; however, they are not authoritative and the rule itself takes precedence. The CMMC numbering scheme in the rule is a key element of the model that must pull together the independent numbering schemes of FAR clause 52.204-21 (for Level 1), NIST SP 800-171 R2 (for Level 2), and NIST SP 800-172 Feb2021 (for Level 3). For the CMMC Program, the numbering scheme must also identify the domain and CMMC Level of each security requirement. The term "priority program" is not used in the rule; therefore, no definition of this term is needed. A commenter incorrectly associated CMMC Program requirements as CMMC security requirements. To address potential confusion, the rule was updated to define "CMMC security requirements" as the 15 Level 1 FAR requirements, the 110 NIST SP 800-171 R2 requirements, and the 24 selected NIST SP 800-172 Feb2021 requirements.

f. OSA and OSC

Comment: Several comments requested clarification of the terms OSA and OSC. One recommended combining them into a single term.

Response: The definitions of Organization Seeking Assessment (OSA) and Organization Seeking Certification (OSC) are provided in § 170.4. It is important to note that OSC is a sub-set of OSA.

g. Process, Store, or Transmit

Comment: Several comments asked about use of the term, "Process, store or transmit". One asked about its application to a turnkey cloud based CMMC solution and whether the intent was to consider "access" a subset of "process". Another recommended using the term "Handle" in lieu of this term and noted that this would also require amendments to DFARS clause 252204-7012. Another comment recommended rephrasing the definition to provide clarity while another asked that the definition of "Process, store, or transmit" (§ 170.4(b)) explicitly include residence of data in memory, which has not previously been identified in this context and could raise interpretation issues.

Response: The phrase "process, store, or transmit" is more specific than the term "handle" and is consistent with DoD contract requirements for Non-Federal Information systems as specified in DFARS clause 252.204-7012. The DoD intended "Access" to be included in the "Process, store, or transmit definition as written in § 170.4(b). An organization offering a turnkey cloud based CMMC solution would be considered an ESP by this rule, and the rule was updated to address assessment and certification requirements of ESPs. The rule definitions are provided for additional clarity of the terms included in the rule and does not nor cannot include every potential instance of the term's application to a contractor's information systems.

h. Clarification of Definitions for FCI and CUI

Comment: Three comments requested clarification of and noted inconsistency between the terms "FCI" and "CUI". One perceived "[FCI]" and "[CUI]" as new acronyms and asked why this rule includes them. One comment noted the inconsistent use of the terms "CUI and FCI" and "sensitive unclassified information" and recommended selecting one term for use throughout the rule. Another comment requested definitions for CMMC be distinguished with formatting or another notation.

Response: FCI is defined in FAR clause 52.204-21. The definition of CUI and general requirements for its safeguarding are included in 32 CFR 2002.4 and 2002.14, respectively. CUI is not a new acronym. The notation "[FCI]" is identified in table 2 to § 170.15(c)(1)(ii) to reflect

its alignment to the requirements of FAR clause 52.204-21 for basic safeguarding of information. Similarly, "[CUI]" has been added to reflect the use of those requirements for CMMC Level 2, which is designed to protect CUI, not FCI. The DoD amended the rule such that "sensitive unclassified information" will consistently be replaced with "FCI and/or CUI" as appropriate.

i. Use of Terms Information and Data

Comment: One comment noted the terms "data", "technical data", and "information" are used synonymously throughout the rule and supplemental documents. They also noted that neither NARA's CUI Registry nor the NIST SP 800-171 R2 define the word "information" and asserted this was a major oversight by NARA ISOO, the CUI Program Executive Agent. The commenter requested this rule adopt the term "Information" throughout the rule and only use "data" when specifically intended based on its definition. Another commenter requested the term "Technical Data" be replaced with the term "Information".

Response: As a commenter stated, both the CUI program and NIST use the term "information". Suggestions that the DoD work with NARA or NIST to define this term are outside the scope of this rule. Within this rule, data generally refers to individual facts, such as those submitted to eMASS or SPRS; however, data and information may be used interchangeably. DoD declined to make requested administrative edits because they would not result in a substantive change.

j. Source Materials Incorporated by Reference

Comment: Four comments asked for clarification of those documents incorporated by reference, or the specific versions of documents referenced in the rule.

Response: The DoD declined to incorporate by reference the Department's role as data owner. NIST SP 800-53 R5 was incorporated by reference only for use with applicable definitions because it provided the latest definitions available.

The OSA is responsible for determining its CMMC Assessment Scope and its relationship to security domains. Assets are out-of-scope when they are physically or logically separated from the assessment scope. Contractor Risk Managed Assets are only applicable within the OSA's assessment scope. Table 3 to § 170.19(c)(1) is used to identify the asset categories within the assessment scope and the associated requirements for each asset category. Contractor's riskbased security policies, procedures, and practices are not used to define the scope of the assessment, they are descriptive of the types of documents an assessor will use to meet the CMMC assessment requirements.

To ensure the source of every definition is accounted for, the terms in § 170.4 either cite a reference or are designated as CMMC-custom using the notation "(CMMC-custom term)." The rule has been updated to eliminate the CNSS Glossary definitions and replaced them with appropriate NIST definitions.

k. Miscellaneous Other Terms, References and Notations

Comment: Three comments asked about references to the DoD Manual 8570, "Information Assurance Workforce Improvement Program," and one asked if the references should be replaced by the newer DoD Manual 8140.

One commenter suggested DoD add an enhanced definition of "Security Domain" domain. to the glossary.

One questioned use of the CNSSI-4009 Glossary instead of the NIST Glossary of Terms. One comment requested a change to text quoted from another source. One commenter asserted that the rule includes no reference to "existing FAR, DFARS, or DoD authoritative sources" and recommended that they be added in instead referencing NIST publications only.

One comment asked if it is necessary to read and understand all FIPS, NIST SP 800, CNSSI, and ISO/IEC documents incorporated by referenced in § 170.2. One comment requested the references for CMMC Assessment Guides in Appendix A be changed to NIST SP 800-171A Jun2018 and NIST SP 800-172A Mar2022. Two comments noted version numbers are not always provided for two specific document sources. Another comment requested references for supporting information, resources, and training for the DIB.

A commenter asked if the term “Government Information Systems” was equivalent to the term “Federal Information Systems” while another expressed that the term, “CMMC Level 2 Final Certification Assessment was confusing given that “Assessment” and “Certification” are two separate and distinct terms. Another comment noted that the Summary Information section states there is a difference between a POA and a POA&M but recommended both terms be defined for clarity.

One comment stated the “CMMC Certified Assessor (CCA)” definition and acronym are not used consistently in the rule and the current CMMC AB’s website. Another comment noted that the term, “related practitioners” under the definition of CAICO in § 170.4 could be confused with the term “Registered Practitioners (RP)” used by the CMMC AB as their designation for consultants.

One comment stated that the DoD must be deliberate in its use of certain terms, especially the words "must" and "shall", which connote legal requirements, versus words like "will", "expected", "can", "may", "should", etc., which are permissive (i.e., optional)

One commenter noted the word “practice” was replaced multiple times based on a comparison of pre-publication drafts with the formal drafts that were published for public comment.

Another comment asserted that the DoD is falsely describing the CMMC program as addressing “basic” cybersecurity requirements when this is the most demanding cybersecurity standard ever produced.

One commenter objected to the CMMC Level 1, 2, and 3 Assessment definitions in § 170.4 referring to the content of corresponding rule sections and suggested that the definitions be deleted from § 170.4 unless they can be succinctly defined without doing so.

Response: The rule has been updated to reference DoD Manual 8140 “Cyberspace Workforce Qualification and Management Program” which replaced DoD Manual 8570, "Information Assurance Workforce Improvement Program." DOD Manual 8140.03 is available at: https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf.

No changes were made to quotations from sources outside the rule. A definition cited from a source must exactly match the source, it cannot be altered. To address a commenter’s misperception that the rule does not reference “existing FAR/DFARS, or other DoD authoritative sources,” it should be noted that the CMMC proposed rule includes 54 mentions each of FAR clause 52.204-21 and DFARS clause 252.204-7012. The DFARS clause 252.204-7012 is added to DoD contracts to implement the requirements of NIST SP 800-171, which is the authoritative reference for adequate safeguarding of CUI.

Contractors complying with CMMC need to be familiar with those documents that are incorporated by reference, which address requirement-related topics. NIST SP 800-53 R5 is incorporated by reference only for applicable definitions because DoD chose to use the latest definitions available. The purpose of a reference listed in § 170.2 should be interpreted based on the context in which it is used. For example, the references provided in § 170.4 specify the source of the definition. The references for the CMMC Assessments Guides listed in Appendix A have been updated. These guides are largely derived from NIST SP 800-171 R2, NIST SP 800-171A Jun2018, NIST SP 800-172 Feb2021, and NIST SP 800-172A Mar2022.

The DoD has updated § 170.3 to align with the FAR terminology and now reflects “Federal Information System” instead of “Government Information System”.

The DoD updated the rule to reference the latest version of “Cloud Security Technical Reference Architecture” and, where appropriate, to identify a revision number for NIST SP 800-171. Specific details of cybersecurity-related resources and training developed to support the DIB are outside the scope of this rule. As it becomes available, supporting resources and training information will be disseminated. Currently, multiple public resources are available to help educate companies on NIST and CMMC requirements.

The DoD declined to respond to comments based on comparison of pre-publication draft versions of the supplemental guidance documents.

A commenter's claim that DoD views the CMMC program as only addressing "basic cybersecurity" is incorrect. Throughout the rule, references to "basic safeguarding" mean the requirements of CMMC Level 1, which align directly to the requirements of FAR clause 52.20421. That FAR clause is titled "Basic Safeguarding of Covered Contractor Information Systems". Similarly, the CMMC program establishes a CMMC Level 3 requirement to comply with a subset of requirements from NIST SP 800-172 Feb2021, titled, "Enhanced Security Requirements for Protecting Controlled Unclassified Information."

Section 170.4 includes acronyms and definitions used in the rule text. Terms from other authoritative sources are listed in § 170.4 and are properly sourced. 1 CFR part 51 governs drafting of this rule.

The DoD updated the rule throughout to reflect new terminology better differentiating between the activity of undergoing an assessment and the CMMC Status that may result from that activity. An OSA undergoes one of the following: Level 1 self-assessment; Level 2 selfassessment; Level 2 certification assessment; or Level 3 certification assessment. The result of that assessment activity is either failure to meet minimum requirements or one of the following CMMC Statuses: Final Level 1 (Self); Conditional Level 2 (Self); Final Level 2 (Self); Conditional Level 2 (C3PAO); Final Level 2 (C3PAO); Conditional Level 3 (DIBCAC); or Final Level 3 (DIBCAC).

The official DoD acronym for CCA is "CMMC Certified Assessor," as addressed in § 170.4. All CMMC terms and definitions provided in this 32 CFR part 170 CMMC Program rule are codified and therefore take precedence over definitions and acronym usage from the CMMC website or other sources.

To avoid confusion in the ecosystem with the term "practitioner", the DoD modified the definition in § 170.4 to replace the word "practitioners" with "professionals."
While "must" is a more commonly used term than "shall", both terms impose a requirement as defined in FAR 2.101 Definitions.

33. Rule Text Modifications

a. Changes to the Preamble

Comment: One commenter recommended that the supplemental Assessment Guides be consolidated with and cross referenced to requirements for the CMMC Levels in the same document. Eighty-three comments requested changes to the preamble section of the rule text. Of those, 17 were incorporated and are summarized below.

Writing Style: Multiple commenters wanted shorter, simpler, and more focused wording starting with changes to the first sentence in the Summary section.
Word Choices: In the "CMMC 2.0 Overview as Proposed by this Rule" section several comments objected to the description of FAR clause 52.204-21 requirements as "elementary" or "basic". One comment asserted that "may" is not the correct verb for "Defense contracts … may include applicable requirements …,". One comment suggested the preamble sentence "Once CMMC is implemented, the required CMMC level for contractors will be specified in the solicitation," be revised to use wording that is more consistent with other parts of the preamble and rule text. One commenter proposed edits to remove passive voice from a sentence in the preamble description of Key Changes Incorporated in the Revised CMMC Program. One commenter requested a change to reference the relevant DFARS clause 252.204-7012, rather than the DFARS subpart 204.73.

Clarifications: Two comments asserted that the description of affirmations requirement could be mis-interpreted as suggesting that primes and subcontractors all submit a single affirmation or that one contractor must affirm another's continuing compliance. One comment requested clarification about FedRAMP requirements for Cloud Service Providers. Some comments asked whether POA&Ms must be documented in the System Security Plan. One comment recommended punctuation and grammatical edits and asked for clarification of rule text that discusses the impact of not

logically or physically separating contractor-owned information systems that process, store, or transmit FCI (or CUI) from those that do not.

Response: This rule follows the format and includes all sections required in OMB guidelines for formal rulemaking. The DoD lacks authority to modify the template or omit required sections, as requested by some commenters. In addition, one commenter recommended that the supplemental Assessment Guides be consolidated with and cross referenced to requirements for the CMMC Levels in the same document. The DoD interpreted this recommendation as a request to integrate all information in the supplemental guidance into the rule text, which does not align with rulemaking guidelines (1 CFR part 51). No changes were made to consolidate or integrate the supplemental guidance documents, which are not codified and are provided as optional resources to assist OSAs. The regulatory content in the 32 CFR part 170 CMMC Program rule takes precedence.

Some commenters criticized the preamble summary paragraph, and one submitted a preferred rewrite that oversimplified the content so far as to alter the intended meaning. For that reason, the specific revisions were not incorporated. However, the DoD has revised the final rule to begin with a simplified statement of its purpose, as follows: "With this final rule, DoD establishes a scalable way to verify, through assessment, that contractors have implemented required security measures necessary to safeguard DoD's Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)".

The DoD strove to streamline the writing style. Note that the preamble is not part of the regulatory text, however, it is a required part of the rulemaking template. The DoD made the following changes to the preamble based on requests for text modifications.

The preamble is updated to change the verb "will" to "should", where appropriate. The preamble and regulatory text have been updated to clarify that a Plan of Action need not be part of the System Security Plan. The sentence in the preamble overview about FAR clause 52.20421 requirements has been rewritten to describe them as "the minimum necessary" to receive FCI, rather than describing them as "elementary" for "basic" cybersecurity. Note that the title of the FAR clause 52.204-21 clause is Basic Safeguarding Requirements.

A preamble overview paragraph about Affirming Officials is revised to clarify that CMMC affirmations shall be submitted by the OSA and apply only to the information systems of that organization. DoD's use of the term OSA within the affirmations section is deliberate and conveys that each organization is responsible for affirmations pertaining to their own assessments. A preamble overview paragraph about Cloud Service Providers has been aligned to DFARS clause 252.204-7012 language and specifies that defense contractors must confirm that any CSPs they use to handle CUI must meet FedRAMP Moderate Baseline standards. Wording in the preamble overview of the rule has been edited from "may include" to "require", to clarify a statement about when DFARS clause 252.204-7012 applies. One sentence in the preamble about the regulatory impact of CMMC Requirements has been edited into two sentences to make clear that solicitations identify CMMC contract requirements, rather than "for contractors", and that only contractors handling FCI or CUI must meet the specified CMMC requirements.

The DoD has incorporated a suggested re-wording to simplify the description of CMMC Level 2 assessments in the preamble paragraph describing Key Changes Incorporated in the Revised CMMC Program.

b. Changes to the Regulatory Text

Comment: Of the 52 comments that requested changes to the regulatory text (§§ 170.1 through 170.24), the nine which DoD incorporated are summarized below.

Word choices: In § 170.1(b), two comments posited that the word "enhance" is inaccurate in the phrase "The CMMC Program is designed to enhance protection of FCI and CUI…". In § 170.9(a) one comment noted that C3PAOs do not "grant" assessments, they "conduct" them. Another asked why, in table 3 to § 170.19(c)(1), the CUI Asset category needs to be assessed against "CMMC security requirements" but in table 5 to § 170.19(d)(1), the same category is assessed against "all CMMC security requirements." For § 170.4(b) One comment requested appending "and to the DoD" to the definition of Assessment Findings Report.

Paragraph Organization: For Applicability, a comment recommended changing the order of paragraphs in § 170.3 and other text changes to improve clarity.

Reference: One comment noted that the § 170.6(b) phrase "as provided for under DFARS clauses 252.204-7012 and 7020…" is in error because the section describes CMMC PMO responsibilities and only DFARS clause 252.204-7020 references DIBCAC assessments of OSAs.

Redundancy: One comment asserted that § 170.9(b)(9) and § 170.9(b)(20) are redundant as both describe that assessment appeals and results are entered into eMASS.

Consistency: One comment pointed out an inconsistency between the text in § 170.18(c)(1)(i) and the Scoping Guide related to whether a CMMC Level 3 Assessment Scope must be the same as, or may be a subset of, the Assessment Scope of the prerequisite CMMC Level 2 certification.

Clarifications: One comment asked whether the stipulation that CCIs must not disclose CMMC data or metrics applies to all data or only "non-public" data.
Consistency: One commenter asked for clarification regarding templates and formats required for information uploaded into the CMMC instantiation of eMASS.

Response: The DoD has incorporated a request to delete the word "enhance" from § 170.1(b), and the purpose of the CMMC Program now reads that the CMMC Program is designed as a compliance assessment to assist in DoD's enforcement of information safeguarding requirements. Lower level paragraphs in § 170.3 have been reordered for added clarity.
The words "and to the DoD via CMMC eMASS" have been added to the end of the Assessment Findings Report definition in § 170.4(b). In addition, § 170.9(b)(17) has been rephrased to stipulate that all assessment data and information uploaded into the CMMC instantiation of eMASS must be compliant with the data standard provided in the eMASS CMMC Assessment Import Templates available on the CMMC eMASS website.

The DoD replaced the word "granting" with the word "conducting" in the description of C3PAO assessments in § 170.9(a). Sections 170.9(b)(9) and (b)(20) have been modified to eliminate redundancy between the two paragraphs, however the DoD did not concur that §§ 170.9(b)(17) and (18) are redundant and made no change.

Section 170.18(c)(1)(i) was revised to clarify that the CMMC Assessment Scope for Level 3 must be equal to or a subset of the CMMC Assessment Scope for the Level 2 certification assessment of the system in question. Section 170.19 was revised to clarify that, for CMMC Level 2, OSAs will be assessed against all Level 2 requirements. For CMMC Level 3, OSAs will be assessed against all Level 2 and Level 3 requirements.

Section 170.1 has been revised to correct punctuation and improve grammar. The section now conveys more clearly that the CMMC Program is designed as a compliance assessment to assist in DoD's enforcement of information safeguarding requirements. No changes were made regarding use of "not logically or physically isolated from all such CUI systems". Specifying a CMMC Assessment Scope is a necessary preparatory step for a CMMC assessment. Assessment requirements are specified in § 170.19. At Levels 2 and 3, logical or physical isolation is the primary mechanism used to separate in-scope from out-of-scope assets. CRMA and Specialized Asset categories only apply to assets that are within the Assessment Scope or boundary.

§ 170.6(b) has been revised to reference DFARS clause 252.204-7020 rather than DFARS clause 252.204-7012. In addition, § 170.05 was revised to reference DFARS clause 252.2047012, rather than DFARS 204.73, for consistency and clarity.
The title of § 170.16(c)(1) has been updated to specify self-assessment of the OSA. DoD declined to make other administrative changes because they would not result in a substantive change.

§ 170.12(b)(8) has been revised to clarify that CCIs must not disclose CMMC data or metrics that are PPI, FCI, or CUI without prior coordination with and approval from DoD.

c. Changes Recommended but Not Incorporated

Comment: Many comments addressed non-substantive administrative changes or writing style and were not incorporated. Many comments requested substantive changes that were not incorporated, and which are described more fully in the response below.

Response: In addition, thirty-eight other recommendations were not incorporated because they did not result in substantive changes. The DoD declines to delete references or convert narrative text explanations into tables, bullets, or other truncated formats because the intent is to facilitate reader understanding of complex requirements. Other recommended administrative changes which did not result in a substantive change were also not incorporated.

Other changes were not incorporated because the revisions would result in unintended or inaccurate meaning of the text. The following explanation is provided for those unincorporated but substantive recommendations.

The DoD did not change content in the Discussion of Public Comments section that addressed responses to the original 48 CFR CMMC interim final rule, because intervening rule changes made in response to public comments received about the more recent proposed rule(s) supersede text of the earlier rule.

Section 170.3(a)(1) applies to contract awardees. While the rule may impact External Service Providers and Cloud Service providers, the rule is not directly applicable to them. CMMC requirements apply at the time of contract award and thereafter.

DoD declined to change the program name as it is well known in the community, and the tiered approach to the model still embodies a concept of cybersecurity maturity.
OSA responsibilities for complying with CMMC are provided throughout the rule and do not need to be repeated.

CMMC is a program that validates implementation via assessment, the rule does not prescribe how to implement.

In the first sentence of the Summary, this rule describes that the CMMC assessment mechanism will cover both existing security requirements for CUI, and new security requirements for certain programs. No additional reference is necessary in the introductory summary because the specific NIST reference documents are mentioned shortly after the summary and throughout the rule text.

DoD declined to revise § 170.2 to use the word "competent" because "competence" is the word included in the referenced ISO/IEC 17011:2017(E) Abstract.

The rule retains requirements to provide all documentation and records in English because it is necessary for adequate program management and specifying this requirement is required to ensure clarity of interpretation.

The DoD has reviewed § 170.17(c)(2)(ii) and does not agree that a noun is missing. The lead-in paragraph provides the noun, and it is not necessary to repeat the phrase.
The DoD disagrees that portions of § 170.18(c)(1) are redundant and therefore did not delete the lower level paragraphs, however revisions were made to clarify that a Level 2 certification assessment is needed prior to Level 3 certification assessment.

Recommended edits to § 170.24(9) that would change the meaning were not accepted. During the assessment process, the Lead Assessor/Assessor must view any prior DoD CIO adjudication of proposed variances to security requirements in the system security plan to ensure correct implementation and render a determination of MET if there have been no changes in the environment.

The DoD did not modify § 170.10 to permit CCAs, CCPs, and CCIs to retrain "or" recertify, instead of both, upon significant change to DoD's CMMC Program requirements under this rule.
The DoD disagreed with one commenter's assertion that the summary within the preamble to the rule implies CMMC assessments address all DFARS clause 252.204-7012 requirements, therefore no edits were necessary. The rule indicates that the applicable CMMC Level 2 security requirements are those in NIST SP 800-171 R2 as implemented in DFARS clause 252.204-7012.

Revisions suggesting that all objectives identified in NIST SP 800-171A Jun2018 need not be met are not accurate and not incorporated. Each assessment objective in NIST SP 800-171A

Jun2018 must yield a finding of MET or NOT APPLICABLE for the overall security requirement to be scored as MET. Assessors exercise judgment in determining when sufficient and adequate evidence has been presented to make an assessment finding. This is consistent with current DIBCAC High Assessments and assessments conducted under the Joint Surveillance Voluntary Assessment Program (JSVAP). A security requirement can be applicable, even with assessment objectives that are N/A. The security requirement is NOT MET when one or more applicable assessment objectives is NOT MET.

Recommendations to address specific contractual matters were not addressed, because this is a 32 CFR part 170 CMMC Program rule and not an acquisition regulation. Any comments related to contract requirements should be provided in response to the 48 CFR part 204 CMMC Acquisition rule.

The CMMC rule does not specify the number of POA&Ms that may be used to address one or more CMMC security requirement that were NOT MET during a CMMC assessment. The OSA may choose to use a single POA&M or multiple POA&Ms.

No edits were made to reference CCAs in § 170.7, which covers responsibilities for only the DIBCAC, and not CCAs. § 170.11 covers responsibilities for CCAs.

DoD declined to add verbiage to address the potential revision or cancellation of an ISO/IEC standard because § 170.8 adequately reflects that the Accreditation Body shall achieve full compliance with revised ISO/IEC 17011:2017(E) standards. Standards are not effective until published as final.

The DoD declined to adopt one commenter's suggestion to submit all appeals investigation materials with the final decision into eMASS, however, an updated assessment result, if any, will be input into eMASS. In addition, C3PAOs are required to retain assessment artifacts for 6 years.

DoD did not agree with one commenter's assertion that the preamble description of the CMMC Program is incomplete or inaccurate, or that the rule makes implicit changes to DFARS clause 252.204-7010 reporting requirements for activities subject to the U.S.-International Atomic Energy Agency Additional Protocol. The referenced paragraph, which appears both in the preamble background section and in an overview paragraph of the supplemental documents, accurately portrays the CMMC Program as a compliance assessment model to assist in DoD's enforcement of FCI and CUI safeguarding requirements. No change has been made in either location.

The DoD also declines to specify in the rule the DoD offices that review Tier 3 background investigations or equivalency determinations.

No language related to Cloud Service Offerings (CSO) was added in § 170.19 column two. Assets that process, store, or transmit CUI are handled the same way regardless of whether they are from a CSO or otherwise. Therefore, there is no need to call out CSOs in the table.

The DoD minimized use of the passive voice to an extent in this final rule; however, in some places the passive voice is used to emphasize the action occurring rather than the individual or entity performing the action.

There is no version number in the title of the CMMC Program. Terms such as versions 1.0 or 2.0 have previously been used in DoD's public engagements as a colloquial way to communicate differences in content as the program has evolved. This final rule codifies the program and does include changes from the proposed rule. Only those public comments received during the 60-day comment period following the December 26, 2023 publication (88 FR 89058) are addressed in this final rule.

34. Error Corrections

Comment: Numerous administrative comments were received that addressed formatting grammar, punctuation, and typographical errors as well as word usage and acronym errors: Wording discrepancies, redundancies, and inaccuracies were also reported by multiple comments.

Several comments identified inconsistencies between FedRAMP equivalency as stated § 170.16(c)(2)(ii) and as described in the DOD CIO's December 21, 2023, Federal Risk and

Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings memorandum. One comment requested moving the phrase "in accordance with all applicable policies, procedures, and requirements" in § 170.5(d) to an earlier part of the sentence to be grammatically correct.

One comment noted that DFARS provision 252.204-7019 does not stipulate assessments must be a "self-assessment" as stated in the CMMC 2.0 Overview as Proposed by this Rule section. Also in the same section, one comment indicated the SSP description should not direct the user to explain how each requirement is implemented, monitored, and enforced.

One comment asked if the reference to NIST SP 900-171A refers to the current version or if a version number should be specified. Three comments indicated issues using embedded links to websites. One comment noted that "inspection activities" should be changed to "assessment activities" in 170.9(b)(10). One comment asserted that in 170.17(a)(1) the word "obtaining" should be deleted in the phrase "…the OSC must achieve either CMMC Level 2 Conditional Certification or Final Certification through obtaining a CMMC Level 2 Certification Assessment…"

Response:

Typographical, Grammatical, and Punctuation Errors, and Formatting

The DOD reviewed all reported grammatical, punctuation, typographical, and acronym-related errors and the preamble, RIA, and rule have been updated to address all confirmed errors. Additionally, the formatting errors in the CMMC Level 2 Asset Categories and Associated Requirements row of table 1 of § 170.19(c)(1), have been corrected. The final rule has been revised to correct document titles as needed.

A commenter provided feedback on the PRA and identified incorrect markings in information collection samples. DoD will work with DISA to ensure the final versions of the eMASS templates contain the proper markings. An OSA's CMMC certification assessment results will be ingested into DoD's CMMC instance using the eMASS CMMC Assessment Import Templates published at https://cmmc.emass.apps.mil. The requirements for C3PAOs and DCMA DIBCAC and what is submitted into CMMC eMASS is described in §§ 170.7, 170. 9, 170.17(a)(1)(i), 170.18(a)(1)(i), and 170.19. The documents accompanying the PRA were intended to serve as samples. The comment also contained an incorrect assumption that commercial privileged information "is not CUI because it is incidental to the performance of the contract." The commenter has confused CDI with CUI and is incorrect in the assumption that commercial privileged information is not CUI because of it being incidental to the performance of the contract.

Word usage

Incorrect uses of "tri-annually" have been corrected. Where appropriate the wording has been changed to "every three years" for clarity. In the preamble to the rule, the statement "...and triennial affirmation..." has been corrected to indicate the affirmations are an "annual" requirement. - DoD has updated the preamble to the rule to the correct certification assessment terminology.

The link on the *Federal Register* web site has been corrected and now resolves to the website indicated.

Incorrect or Incomplete References

Several incorrect or incomplete references have also been corrected. § 170.9(b)(1) has been corrected to refer to the authorization in § 170.8(a). One comment asserted that there is no section (c) associated with the reference "§ 170.17(a)(1) and (c)" which is in § 170.9(b)(6). The section "§ 170.17(c) Procedures" does exist and addresses the procedures associated with a CMMC Level 2 Certification Assessment. Section 170.17(a)(1) addresses the Level 2 Certification Assessment requirements for an OSC. The rule has been updated in § 170.9(b)(6) for clarity.

Commenters accurately noted that § 170.17(a)(1) should refer to the Level 2 requirements in § 170.14(c)(3), and this has been corrected. The reference in § 170.18(c)(5)(ii) has been updated

to say, “that maps to the NIST SP 800–171 R2 and a subset of the NIST SP 800-172 Feb2021 requirements”. The rule is updated to replace the instruction “(insert references L1-3)” with “§ 170.19 CMMC scoping.”

Wording discrepancies, redundancies, and inaccuracies

To address a discrepancy between the rule and scoping guidance, the Level 2 Scoping Guide has been updated for clarity and alignment with § 170.16(a) which states that meeting the CMMC Level 2 Self-Assessment requirements also satisfies the CMMC Level 1 SelfAssessment requirements for the same CMMC Assessment Scope. Additionally, the preamble to this rule has been updated to clarify that not all affirmations will occur prior to contract award because POA&M closeout affirmations may occur after contract award.

To address a discrepancy about Level 1 scoring, in § 170.24 the phrase “; therefore, no score is calculated, and no scoring methodology is needed," has been deleted.

The regulatory text was updated to require FedRAMP moderate or FedRAMP moderate equivalency in accordance with DoD Policy. CMMC Program Requirements make no change to existing policies for information security requirements implemented by DoD. The preamble was modified to indicate DFARS provision 252.204-7019 requires an assessment (basic, medium, or high) and not just a self-assessment (basic).

The data input at § 170.17(a)(1)(i)(F) for CMMC eMASS is redundant so it has been removed. In the preamble, the DoD has also removed the inaccurate phrase, "certified by DoD", from the statement "Under CMMC, compliance will be checked by independent third-party assessors certified by DoD."

DoD has updated language in § 170.18(a)(1)(i)(B) to reflect for each DCMA DIBCAC Assessor conducting the assessment, “name and government organization information” will be required for the CMMC instantiation of eMASS.

The DoD has considered the recommendation to change the description of what an SSP should contain and declines to revise the rule text. The NIST SP 800-171 R2 requirement states that an SSP must describe “…how security requirements are implemented…” which is equivalent to going “…through each NIST SP 800-171 security requirement and explain how the requirement is implemented, monitored, and enforced.”

Perceived Errors

DoD declines to make the edit to change “shall” to “will” in § 170.9(b). The existing language is consistent with standard rulemaking usage. The title for NIST SP 800-171A Jun2018 is the current title used by NIST and does not have a version number, so no change was needed. While not used in the rule text, the term enterprise is used in the description of the CMMC Program in the preamble’s Statement of Need for This Rule section: Defense contractors can achieve a specific CMMC Level for its entire enterprise network or an enclave(s), depending upon where the information to protected is processed, stored, or transmitted, therefore enterprise remains in the definitions list.

DoD verified links by clicking on them in the PDF and by copying and pasting the links into a web browser. In both cases links resolved correctly.

The DoD has changed "all personnel involved in inspection activities" to "all personnel involved in assessment activities" in § 170.9(b)(9).

A comment asserted that there was a rulemaking formatting error in § 170.4(b). DoD is following the Office of the Federal Register standards for this section. In sections or paragraphs containing only definitions, paragraph designations are not used, and the terms are listed in alphabetical order. The definition paragraph begins with the term being defined. If a definition contains subordinate paragraphs, these paragraphs are numbered with paragraph designations beginning with the next appropriate level based on the dedicated definitions section.

The 2nd sentence of § 170.17(a)(1) includes the word “obtaining” for clarity.

35. Comments in Favor of the CMMC Program

Comment: Some commenters expressed favorable opinions about the CMMC program as a viable long-term solution to ensure cybersecurity controls are in place. Others commented about specific content of the 32 CFR part 170 CMMC Program proposed rule and the supplemental

documents. For example, two commenters specifically complimented the inclusion of an Affirmation requirement and another supported CMMC implementation as a pre-award requirement. Another commenter appreciated the regulatory text which "encourages" contractors to consult with the Government for additional guidance if or when unsure of appropriate CMMC Level to assign a subcontract solicitation. Two commenters applauded the use of already established workforce qualifications while another concurred with the regulatory text permitting CMMC Certified Professionals (CCPs) to participate in assessments with oversight of a CMMC Certified Assessor (CCA). A commenter also expressed appreciation for the regulatory text's alignment to a specific version of the guidelines (i.e., NIST SP 800-171 R2). One commenter appreciated the video that DoD published to accompany and explain the proposed rule. Several comments cited the longstanding requirements of DFARS clause 252.204-7012 and cybersecurity risks of not implementing NIST SP 800-171 R2 as reasons that the 32 CFR part 170 CMMC Program final rule should be implemented as soon as possible.
Response: The Department appreciates that several commenters expressed agreement to and encouragement for the CMMC Program requirement and its associated specific rule text. The DoD recognizes that not all entities impacted by these regulations hold the same view of its requirements and appreciates those that took the time to express both positive and constructive feedback.

Applicability

Once CMMC is implemented in the 48 CFR part 204 CMMC Acquisition rule, the CMMC Program will require DoD to identify the CMMC Level and assessment type as a solicitation requirement and in the resulting contract for any effort that will cause a contractor or subcontractor to process, store, or transmit FCI or CUI on its unclassified information system(s). Once CMMC is implemented in the 48 CFR part 204 CMMC Acquisition rule, contractors handling FCI or CUI will be required to meet the CMMC Level and assessment type specified in the solicitation and resulting contract.

Summary of Program Changes: DFARS Case 2019-D041 implemented DoD's original model for assessing contractor information security protections. The initial CMMC Program was comprised of five progressively advanced levels of cybersecurity standards and required defense contractors and subcontractors to undergo a certification process to demonstrate compliance with the cybersecurity standards associated with a given CMMC Level.

In March 2021, the Department initiated an internal review of CMMC's implementation that engaged DoD's cybersecurity and acquisition leaders to refine policy and program implementation, focusing on the need to reduce costs for small businesses and align cybersecurity requirements to other Federal standards and guidelines. This review resulted in the revised CMMC Program, which streamlines assessment and certification requirements and improves implementation of the CMMC Program. These changes include:

- Eliminating Levels 2 and 4, and renaming the remaining three CMMC Levels as follows:
- Level 1 will remain the same as the initial CMMC Program Level 1;
- Level 2 will be similar to the initial CMMC Program Level 3; • Level 3 will be similar to the initial CMMC Program Level 5.
- Removing CMMC-unique requirements and maturity processes from all levels;
- For CMMC Level 1, allowing annual self-assessments with an annual affirmation by company leadership;
- Allowing a subset of companies at Level 2 to demonstrate compliance through selfassessment rather than C3PAO assessment.
- For CMMC Level 3, requiring Department-conducted assessments; and
- Developing a time-bound and enforceable POA&M process.

In December 2023, the Department published a proposed rule to amend 32 CFR part 170 in the *Federal Register* (Docket ID DOD-2023-OS-0063, 88 FR 89058), which implemented the DoD's vision for the revised CMMC Program outlined in November 2021. The comment period for the proposed rule concluded on February 26, 2024. Changes have been made to the CMMC Program based on public comment. Significant changes include:

- The Implementation Phase 1 has been extended by an additional six months.
- A new taxonomy was created differentiating the level and type of assessment conducted from the CMMC Status achieved as a result.
- Clarification was added regarding the DoD's role in achievement or loss of CMMC Statuses.
- CMMC Status will be automatically updated in SPRS for OSAs who have met standards acceptance.
- Requirements regarding conflict of interest were updated to expand the cooling-off period for the CMMC Accreditation Body to one year and bounded the timeframe between consulting and assessing for the CMMC Ecosystem to three years.
- A requirement was added for the CMMC Ecosystem members to report adverse information to the CAICO.
- A Provisional Instructor role was added to cover the transitional period that ends 18 months after the effective date of this rule.
- A CCI requirement was added to clarify that a CCI must be certified at the same or higher level than the classes they are instructing.
- A requirement for artifact retention was added to Level 1 self-assessments and Level 2 self-assessments.
- The assessment requirements for ESPs have been reduced.
- The definition of CSP has been narrowed and is now based on NIST SP 800-145 Sept2011.
- The assessment requirements for Security Protection Assets and Security Protection Data have been reduced.
- References to FedRAMP equivalency have been tied to DoD policy.
- Clarified the requirements for CSPs for an OSC seeking a CMMC Status of Level 3 (DIBCAC).
- Clarified that DCMA DIBCAC has the authority to perform limited checks of compliance of assets that changed asset category or changed assessment requirements between the Level 2 and Level 3 certification assessment.
- Clarification was added around the use of VDI clients.
- Provided clarification to distinguish between Plan of Action & Milestones (POA&Ms) and operational plan of action.
- Definitions have been added for: Affirming Official, Assessment objective, Asset, CMMC security requirement, CMMC Status, DoD Assessment Methodology, Enduring Exception, Operational plan of action, Personally Identifiable Information, Security Protection Data (SPD), and Temporary deficiency. Some definitions were also changed to source from NIST documentation instead of Committee on National Security Systems (CNSS) Instruction No. 4009.

Background

A. Statement of Need for This Rule

The Department of Defense (DoD) requires defense contractors to protect FCI and CUI. To verify contractor and subcontractor implementation of DoD's cybersecurity information protection requirements, the Department developed the Cybersecurity Maturity Model Certification (CMMC) Program as a means of assessing and verifying adequate protection of contractor information systems that process, store, or transmit either FCI or CUI.

The CMMC Program is intended to: (1) align cybersecurity requirements to the sensitivity of unclassified information to be protected, (2) add a self-assessment element to affirm implementation of applicable cybersecurity requirements, (3) add a certification element to verify implementation of cybersecurity requirements, and (4) add an affirmation to attest to continued compliance with assessed requirements. As part of the program, DoD also intends to provide supporting resources and training to the DIB, to help support companies who are working to achieve the required CMMC Status. The CMMC Program provides for assessment at

three levels, starting with basic safeguarding of FCI at CMMC Level 1, moving to the broad protection of CUI at CMMC Level 2, and culminating with higher-level protection of CUI against risk from Advanced Persistent Threats (APTs) at CMMC Level 3.

The CMMC Program addresses DoD's need to protect FCI and CUI during the acquisition and sustainment of products and services from the DIB. This effort is instrumental in establishing cybersecurity as a foundation for DoD acquisitions.

Although DoD contract requirements to provide adequate security for covered defense information (reflected in DFARS clause 252.204-7012) predate CMMC by many years, a verification requirement for the handling of CUI to assess a contractor or subcontractor's implementation of those required information security controls is new with the CMMC Program. The theft of intellectual property and sensitive information from all U.S. industrial sectors from malicious cyber activity threatens economic security and national security. The Council of Economic Advisers estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016[25]. The Center for Strategic and International Studies estimates that the total global cost of cybercrime was as high as $600 billion in 2017.[26]

Malicious cyber actors have targeted and continue to target defense contractors and the DoD supply chain. These attacks not only focus on the large prime contractors, but also target subcontractors that make up the lower tiers of the DoD supply chain. Many of these subcontractors are small entities that provide critical support and innovation. Overall, the DIB sector consists of over 220,000 companies[27] that process, store, or transmit CUI or FCI in support of the warfighter and contribute towards the research, engineering, development, acquisition, production, delivery, sustainment, and operations of DoD systems, networks, installations, capabilities, and services. The aggregate loss of intellectual property and controlled unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation, as well as significantly increase the risk to national security. As part of multiple lines of effort focused on the security and resiliency of the DIB, the Department is working with industry to enhance the protection of FCI and CUI within the DoD supply chain. Toward this end, DoD has developed the CMMC Program.

Cybersecurity Maturity Model Certification Program

The CMMC Program provides a comprehensive and scalable certification approach to verify the implementation of requirements associated with the achievement of a cybersecurity level. CMMC is designed to provide increased assurance to the Department that defense contractors can adequately protect FCI and CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. Defense contractors can achieve a specific CMMC Status for their entire enterprise network or an enclave(s), depending upon where the information to be protected is processed, stored, or transmitted. The CMMC Program assesses implementation of cybersecurity requirements. The CMMC requirements for safeguarding and security are the same as those required by FAR Subpart 4.19 and DFARS clause 252.204-7012, as well as selected NIST SP 800-172 Feb201 requirements. CMMC Level 1 requires implementation of the safeguarding requirements set forth in FAR clause 52.204-21. CMMC Level 2 requires implementation of the security requirements in NIST SP 800-171 R2. CMMC Level 3 requires implementation of the security requirements in NIST SP 800-171 R2 as well as selected NIST SP 800-172 Feb2021 requirements, with DoD specified parameters. The CMMC security requirements for all three Levels are provided in § 170.14. In general, CMMC assessments do not duplicate efforts from existing DoD assessments. In rare

---

[25] Based on information from the Council of Economic Advisors report: The Cost of Malicious Cyber Activity to the U.S. Economy, 2018.

[26] Based on information from the Center for Strategic and International Studies report on the Economic Impact of Cybercrime; www.csis.org/analysis/economic-impact-cybercrime.

[27] Based on information from the Federal Procurement Data System, the average number of unique prime contractors is approximately 212,650 and the number of known unique subcontractors is approximately 8,300. (FPDS from FY18-FY21).

circumstances a re-assessment may be necessary when cybersecurity risks, threats, or awareness have changed.

Under the CMMC Program, CMMC contract requirements include self-assessments and third-party assessments for CMMC Level 2, predicated on program criticality, information sensitivity, and the severity of cyber threat. Based on the type and sensitivity of the information to be protected, a defense contractor must achieve the appropriate CMMC Status and demonstrate implementation of the associated set of information protection requirements. If the CMMC Status of Level 1 (Self) or Level 2 (Self) is a contract requirement, the defense contractor will be required to self-assess its compliance with the CMMC Level 1 or Level 2 security requirements and submit both the self-assessment results and an affirmation of conformance in SPRS. Level 1 self-assessment and associated affirmation is required annually. Level 2 self-assessment is required every three years with an affirmation following the selfassessment and annually after the Final CMMC Status Date.

If the CMMC Status of Level 2 (C3PAO) is a contract requirement, the Level 2 certification assessment must be performed by an authorized or accredited CMMC Third Party Assessment Organization (C3PAO). When the CMMC Status of Level 3 (DIBCAC) is a contract requirement, the Level 3 certification assessment by DCMA DIBCAC is required following the achievement of the CMMC Status of Final Level 2 (C3PAO). Upon achievement of the CMMC Status of Level 2 (C3PAO) or Level 3 (DIBCAC), the offeror will be issued a Certificate of CMMC Status. The assessment results are documented in SPRS to enable contracting officers to verify the CMMC Status and CMMC Status Date (i.e., not more than three years old) of an offeror prior to contract award. The offeror must also submit an affirmation of conformance in SPRS following the assessment and annually after the Final CMMC Status Date.

CMMC allows the use of a Plan of Action and Milestones (POA&Ms) for specified CMMC Level 2 and Level 3 security requirements. Each POA&M must be closed (i.e., all requirements completed), within 180 days of the initial assessment.

The details of the requirements for self-assessment, certification assessment, and affirmation for each CMMC Level, are provided in §§ 170.15 through 170.18. POA&M requirements and affirmation requirements are provided in §§ 170.21 and 170.22.

DoD's phased implementation of the CMMC Status requirements is described in § 170.3(e). Once CMMC requirements have been implemented in the DFARS, the solicitation and resulting contract will identify the specific CMMC Status required for that procurement. Selection of a CMMC Status will be based upon careful consideration of market research and the likelihood of a robust competitive market of prospective offerors capable of meeting the requirement. In some scenarios, DoD may elect to waive application of CMMC Status requirements to a particular procurement. In such cases, the solicitation will not include a CMMC Status requirement. Such waivers may be requested and approved by the Department in accordance with DoD's internal policies and procedures. For a DoD solicitation or contract that does include CMMC requirements, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, contracting officers will not make award, or exercise an option on a contract, if the offeror or contractor does not meet the requirements for the required CMMC Status. Furthermore, CMMC requirements are required to flow down to subcontractors as prescribed in the solicitation and resulting contract at all tiers, commensurate with the sensitivity of the unclassified information flowed down to each subcontractor.

B. Legal Authority

5 U.S.C. 301 authorizes the head of an Executive department or military department to prescribe regulations for the government of his or her department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property (www.govinfo.gov/content/pkg/USCODE-2009title5/pdf/USCODE-2009-title5-partI-chap3-sec301.pdf).

Section 1648 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 11692)[28] directs the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. Defense Industrial Base (DIB). The CMMC Program is an important part of this framework.

C. Community Impact

This final rule impacts all prospective and actual DoD contractors and subcontractors that are handling or will handle DoD information that meets the standards for FCI or CUI on a contractor information system during performance of the DoD contract or subcontract. This final rule also impacts all companies who are performing or will perform accreditation, training, certification, or assessment functions in connection with implementation of the CMMC Program.

D. Regulatory History

The CMMC Program verifies defense contractor compliance with DoD's cybersecurity information protection requirements. It is designed to protect FCI and CUI that is shared by the Department with, or generated by, its contractors and subcontractors. The cybersecurity standards required by the program are the same as those set forth in FAR clause 52.204-21 (CMMC Level 1), the NIST SP 800-171 R2 guidelines, which is presently required by DFARS clause 252.204-7012 (CMMC Level 2), and additional selected requirements from the NIST SP 800-172 Feb2021 guidelines (CMMC Level 3). The program adds a robust assessment element and provides the Department increased assurance that contractors and subcontractors are meeting these requirements.

In September 2020, the DoD published the 48 CFR CMMC interim final rule to the DFARS in the *Federal Register* (DFARS Case 2019-D041, 85 FR 48513, September 9, 2020), which implemented the DoD's vision for the initial CMMC Program and outlined the basic features of the program (tiered model, required assessments, and implementation through contracts). The 48 CFR CMMC interim final rule became effective on November 30, 2020, establishing a five-year phase-in period.

In March 2021, the Department initiated an internal review of CMMC's implementation, informed by more than 750 CMMC-related public comments in response to the 48 CFR CMMC interim final rule. This comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

In November 2021, the Department announced plans for a revised CMMC Program, which incorporates an updated program structure and requirements designed to achieve the primary goals of an internal DoD review of the CMMC Program. With the implementation of the CMMC Program, the Department introduced several key changes that build on and refine the original program requirements. These include:

- Streamlining the model from five to three certification levels;
- Allowing all companies at Level 1 and a subset of companies at Level 2 to demonstrate compliance through self-assessments;
- Increased oversight of professional and ethical standards of third-party assessors; and
- Allowing companies, under certain limited circumstances, to make POA&Ms to achieve certification.

In December 2023, the Department published a proposed rule to amend 32 CFR part 170 in the *Federal Register* (Docket ID 2023-OS-0063, 88 FR 89058, December 26, 2023), which implemented the DoD's vision for the revised CMMC Program outlined in November 2021. The comment period for the proposed rule concluded on February 26, 2024.

The CMMC requirements established pursuant to DFARS Case 2019-D041 have not been revised as of the date of publication of this final rule. However, the CMMC Program requirements in this final rule will be implemented in the DFARS, as needed, which may result in changes to the current DFARS text, solicitation provisions, and contract clauses relating to DoD's cybersecurity protection requirements, including DFARS subpart 204.75 and DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification (CMMC) Requirements.

---

[28] www.govinfo.gov/content/pkg/PLAW-116publ92/pdf/PLAW-116publ92.pdf

Context of the CMMC Program In Light of Other DoD-Related Work

At present, and prior to the DFARS CMMC Acquisition rule becoming effective, the Department is using the DCMA DIBCAC to conduct CMMC Level 2-like assessments. To date, the DCMA DIBCAC has assessed 357 entities including DoD's major prime contractors. The CMMC Program's assessment phase-in plan, as described in § 170.3 Applicability, does not preclude entities from immediately and voluntarily seeking a CMMC certification assessment prior to the DFARS CMMC Acquisition rule being finalized and the clause being added to new or existing DoD contracts.

The Department estimates 8,350 medium and large entities will require CMMC Level 2 certification assessments. Once the CMMC DFARS coverage is effective, the Department will contractually mandate CMMC Level 2 certification assessments on these entities. It is estimated that 135 CMMC Third-Party Assessment Organization (C3PAO)-led assessments will be completed in the first year. The Department estimates 673 C3PAO-led assessments in year 2 followed by 2,252 C3PAO-led assessments in year 3. During the fourth year, the Department estimates,4,452 C3PAO-led assessments will be completed. The DCMA DIBCAC will perform assessments upon DoD's request.

Additionally, the Department may include CMMC Level 2 certification requirements on contracts awarded prior to the CMMC DFARS coverage becoming effective, but doing so will require bilateral contract modification after negotiations.

The CMMC Program has been incorporated in the Department's 2024 Defense Industrial Base Cybersecurity Strategy[28]. The strategy requires the Department to coordinate and collaborate across components to identify and close gaps in protecting DoD networks, supply chains, and other critical resources. Other prongs of the Department's cybersecurity strategy are described in the Department's National Industrial Security Program Operating Manual (NISPOM) which address implementation of the Security Executive Agent Directive (SEAD) 3 [29], including clarifications on procedures for the protection and reproduction of classified information; controlled unclassified information (CUI); National Interest Determination (NID) requirements for cleared contractors operating under a Special Security Agreement for Foreign Ownership, Control, or Influence; and eligibility determinations for personnel security clearance processes and requirements[29].

In addition, DCMA DIBCAC is responsible for leading the Department's contractor cybersecurity risk mitigation efforts. As part of this work, the DIBCAC assesses the defense industrial base companies to ensure they are meeting contractually required cybersecurity standards. The DIBCAC team ensures contractors have the ability to protect controlled unclassified information for government contracts they are awarded. DIBCAC conducts NIST SP 800-171 assessments in support of DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reportin*g, and DFARS clause 204.204-7020, *NIST SP 800-171 DoD Assessment Requirements*. The DFARS 204.204-7020 DIBCAC prioritization process is designed to adjust as DoD's cyber priorities evolve based on ongoing threats. DIBCAC analysts collect and analyze data on DoD contractors to include:

- Mission critical programs, technologies, and infrastructure and the contractors (prime or lower tier) that support DoD capabilities.
- Cyber threats, vulnerabilities, or incidents.
- DoD Leadership requests.

Regulatory Impact Analysis

FAR Subpart 4.19 and DFARS clause 252.204-7012 address safeguarding of FCI and CUI in contractor information systems and prescribe contract clauses requiring protection of FCI and

[28] https://media.defense.gov/2024/Mar/28/2003424523/-1/-1/1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF [29] www.govinfo.gov/content/pkg/FR-2020-12-21/pdf/2020-27698.pdf

[29] www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/32-CFR-Part-117-NISPOM-Rule/

CUI within the supply chain. The FAR and DFARS requirements for safeguarding FCI and CUI predate the CMMC Program by many years, and baseline costs for their implementation are assumed to vary widely based on factors including, but not limited to, company size and complexity of the information systems to be secured. FAR clause 52.204-21 is prescribed at FAR section 4.1903 for use in solicitations and contracts when the contractor or subcontractor at any tier may have FCI residing in or transiting through its information system. This clause requires contractors and subcontractors to apply basic safeguarding requirements and procedures to protect applicable contractor information systems that process, store, or transmit FCI. In addition, DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, is prescribed at DFARS section 204.7304(c) for use by DoD in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of commercially available off-the-shelf items. This clause applies when a contractor information system processes, stores, or transmits covered defense information and requires contractors and subcontractors to provide "adequate security" to safeguard that information when it resides on or transits through a contractor information system, and to report cyber incidents that affect that system or network. The clause states that to provide adequate security, the contractor shall implement, at a minimum, the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 R2, *Protecting CUI in Nonfederal Systems and Organizations*. Contractors are also required to flow down DFARS clause 252.204-7012 to all subcontracts for operationally critical support or for which subcontractor performance will involve covered defense information.

However, neither FAR clause 52.204-21 nor DFARS clause 252.204-7012 provide for DoD assessment of a contractor's implementation of the information protection requirements required by those clauses. The Department developed the CMMC Program to verify implementation of cybersecurity requirements in DoD contracts and subcontracts, by assessing adequacy of contractor information system security compliance prior to award and during performance of the contract. With limited exceptions, the Department intends to require compliance with CMMC as a condition of contract award. Once CMMC is implemented, the required CMMC Status will be specified in the solicitation and resulting contract. Contractors handling FCI or CUI will be required to meet the CMMC Status specified in the contract.

There are three different levels of CMMC assessment, starting with basic safeguarding of FCI at Level 1, moving to the broad protection of CUI at Level 2, and culminating with higher level protection of CUI against risk from Advanced Persistent Threats (APTs) at Level 3. The benefits and costs associated with implementing this final rule, as well as alternative approaches considered, are as follows:

Costs

A Regulatory Impact Analysis (RIA) that includes a detailed discussion and explanation about the assumptions and methodology used to estimate the cost of this regulatory action follows and is available at www.regulations.gov (search for "DoD-2023-OS-0063," click "Open Docket," and view "Supporting Documents").

Background

The Department of Defense (DoD or Department) requires a secure and resilient supply chain to ensure the development, production, and sustainment of capabilities critical to national security. The DoD supply chain is targeted by adversaries with increasing frequency and sophistication, and to devastating effect. Therefore, implementation of cybersecurity standards and enforcement mechanisms are critically important. Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," emphasizes the need to strengthen cybersecurity protections for both the Federal Government and the private sector.

Nation-state adversaries attack the U.S. supply chain for a myriad of reasons, including exfiltration of valuable technical data (a form of industrial espionage); disruption to control systems used for critical infrastructure, manufacturing, and weapons systems; corruption of quality and assurance across a broad range of product types and categories; and manipulation of

software to achieve unauthorized access to connected systems and to degrade the integrity of system operations. For example, since September 2020, major cyber-attacks such as the SolarWinds[30], Colonial Pipeline, Hafnium[31], and Kaseya[32] attacks, have been spearheaded or influenced by nation-state actors[33] and resulted in significant failures and disruption. In context of this threat, the size and complexity of defense procurement activities provide numerous pathways for adversaries to access DoD's sensitive systems and information. Moreover, adversaries continue to evolve their tactics, techniques, and procedures. For example, on April 28, 2022, CISA and the FBI issued an advisory on destructive "wiperware," a form of malware which can destroy valuable information [34]. Protection of FCI and CUI is critically important, and the DoD needs assurance that contactor information systems are adequately secured to protect such information when it resides on or transits those systems.

The Department is committed to working with defense contractors to protect FCI and CUI.

- Federal Contract Information (FCI): As defined in section 4.1901 of the FAR, 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, but not including information provided by the Government to the public, such as that on public Web sites, or simple transactional information, such as that necessary to process payments.
- Controlled Unclassified Information (CUI): 32 CFR 2002.4(h) defines CUI, in part, as information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls, including FCI.

In September 2020, the DoD published 48 CFR CMMC interim final rule (DFARS Case 2019-D041, 85 FR 48513, September 9, 2020), which implemented DoD's vision for the initial Cybersecurity Maturity Model Certification (CMMC) Program and outlined basic program features, to include: 5-level tiered model, CMMC Certified Third Party Assessment Organization (C3PAO) assessments in support of contractor and subcontractor certification, with no allowance for a Plan of Action and Milestones (POA&Ms), and implementation of all security requirements by the time of a contract award. A total of 750 comments were received on the 48 CFR CMMC interim final rule during the public comment period that ended on November 30, 2020. These comments highlighted a variety of industry concerns including concerns relating to the costs for a C3PAO certification, and the costs and burden associated with implementing, prior to award, the required process maturity and 20 additional cybersecurity practices that were included in the initial CMMC Program. The Small Business Administration Office of Advocacy also raised similar concerns on the impact the rule would have on small businesses in the DIB.

Pursuant to DFARS clause 252.204-7012, DoD has required certain defense contractors and subcontractors to implement the security protections set forth in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 R2 to provide adequate security for CUI that is processed, stored, or transmitted on contractor information systems. The CMMC Program provides the Department the mechanism needed to verify that a defense contractor or subcontractor has implemented the security requirements at each CMMC Level and is maintaining that status across the contract period of performance, as required.

In calendar year (CY) 2021 DoD paused the planned CMMC rollout to conduct an internal review of the CMMC Program. The internal review resulted in a refined and streamlined set of

---

[30] www.gao.gov/assets/gao-22-104746.pdf

[31] www.ic3.gov/Media/News/2021/210310.pdf

[32] www.cisa.gov/uscert/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affectedkaseya-vsa

[33] www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study26AUG2019.pdf

[34] www.cisa.gov/uscert/ncas/alerts/aa22-057a

requirements that addressed many of the concerns identified in the public comments received relating to the initial CMMC Program. These changes have been incorporated into the revised CMMC Program structure and policies. In July 2022, the CMMC PMO met with the Office of Advocacy for the United States Small Business Administration (SBA) to address the revisions planned to the CMMC Program that are responsive to prior SBA concerns.

The CMMC Program will enhance the ability of the DoD to safely share FCI and CUI with defense contractors and know the information will be suitably safeguarded. Once fully implemented, CMMC will incorporate a set of cybersecurity requirements into acquisition contracts to provide verification that applicable cyber protections have been implemented. Under the CMMC Program, defense contractors and subcontractors will be required to implement certain cybersecurity protection requirements tied to a designated CMMC level and either perform a self-assessment or obtain an independent assessment from either a C3PAO or DCMA DIBCAC as a condition of a DoD contract award. CMMC is designed to validate the protection of FCI and CUI that is shared with and generated by the Department's contractors and subcontractors. Through protection of information by adherence to the requirements verified in the revised CMMC Program, the Department and its contractors will prevent disruption in service and the loss of intellectual property and assets, and thwart access to FCI and CUI by the nation's adversaries.

The CMMC Program is intended to: (1) align cybersecurity requirements to the sensitivity of unclassified information to be protected, and (2) add a certification element, where appropriate, to verify implementation of cybersecurity requirements. As part of the program, DoD also intends to provide supporting resources and training to defense contractors to help support companies who are working to achieve the required CMMC Status. The CMMC Program provides for assessment at three levels: basic safeguarding of FCI at CMMC Level 1, broad protection of CUI at CMMC Level 2, and enhanced protection of CUI against risk from Advanced Persistent Threats (APTs) at CMMC Level 3. The CMMC Program is designed to provide increased assurance to the Department that a defense contractor can adequately protect FCI and CUI in accordance with prescribed security requirements, accounting for information flow down to its subcontractors in a multi-tier supply chain.

The CMMC Program addresses DoD's need to protect FCI and CUI during the acquisition and sustainment of products and services from the DIB. This effort is instrumental in establishing cybersecurity as a foundation for future DoD acquisition.

Although DoD contract requirements to provide adequate security for covered defense information (reflected in DFARS clause 252.204-7012) predate CMMC by many years, a certification requirement for the handling of CUI to assess a contractor or subcontractor's compliance of those required information security controls is new with the CMMC Program. Findings from DoD Inspector General report[35] indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. The report emphasizes that malicious actors can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies.

Currently, the FAR and DFARS prescribe contract clauses intended to protect FCI and CUI. Specifically, the clause at FAR 52.204–21, *Basic Safeguarding of Covered Contractor Information Systems*, is prescribed at FAR 4.1903 for use in Government solicitations and contracts when the contractor or a subcontractor at any tier may have FCI residing in or transiting through its information system(s). This clause requires contractors and subcontractors to implement basic safeguarding requirements and procedures to protect FCI being processed, stored, or transmitted on contractor information systems. In addition, DFARS clause 252.2047012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, is prescribed at DFARS 204.7304(c) for use in all solicitations and contracts except for solicitations

[35] DODIG-2019-105 "Audit of Protection of DoD CUI on Contractor-Owned Networks and Systems"

and contracts solely for the acquisition of commercially available off-the-shelf (COTS) items. This clause requires contractors and subcontractors to provide "adequate security" to process, store or transmit covered defense information when it resides on or transits a contractor information system, and to report cyber incidents that affect that system or network. The clause states that to provide adequate security, the contractor shall implement, at a minimum, the security requirements in NIST Special Publication (SP) 800-171 R2, *Protecting CUI in Nonfederal Systems and Organizations*. Contractors are also required to flow down DFARS clause 252.204-7012 to all subcontracts that require processing, storing, or transmitting of covered defense information.

However, neither FAR clause 52.204-21 nor DFARS clause 252.204-7012 provide for DoD verification of a contractor's implementation of the basic safeguarding requirements specified in FAR clause 52.204-21 nor the security requirements specified in NIST SP 800-171 R2, implementation of which is required by DFARS clause 252.204-7012, prior to contract award. As part of multiple lines of effort focused on the security and resilience of the DIB, the Department is working with industry to enhance the protection of FCI and CUI within the DoD supply chain. Toward this end, DoD has developed the CMMC Program.

Revised CMMC Program Requirements

The CMMC Program requirements will be implemented through the DoD acquisition and contracting process. With limited exceptions, the Department intends to require compliance with CMMC as a condition of contract award. Once CMMC is implemented, the required CMMC Status will be specified in the solicitation and resulting contract. Contractors handling FCI or CUI will be required to meet the CMMC Status specified in the contract. In accordance with the implementation plan described in § 170.3(e), CMMC Status requirements will apply to new DoD solicitations and contracts, and shall flow down to subcontractors, based on the sensitivity of the FCI and CUI to be processed, stored or transmitted to or by the subcontractor. Before contract award, the offeror must achieve the specified CMMC Status for the contractor information system (e.g., enterprise network, network enclave) that will process, store, or transmit the information to be protected. The contractor or subcontractor will also submit affirmations in the Supplier Performance Risk System (SPRS). An overview of requirements at each level is shown:

Level 1 self-assessment

- Level 1 self-assessment requires compliance with basic safeguarding requirements to protect FCI are set forth in FAR clause 52.204-21. CMMC Level 1 does not add any additional security requirements to those identified in FAR clause 52.204-21.
- OSAs will submit the following information in SPRS:
    1. the results of a self-assessment of the OSA's implementation of the basic safeguarding requirements set forth in § 170.15 associated with the contractor information system(s) used in performance of the contract; and
    2. an initial affirmation of compliance, and then annually thereafter, an affirmation of continued compliance as set forth in § 170.22.
    3. the Level 1 self-assessment cost burden will be addressed as part of the 48 CFR part 204 CMMC Acquisition final rule.

Level 2 self-assessment

- Level 2 self-assessment requires compliance with the security requirements set forth in NIST SP 800-171 R2 to protect CUI. CMMC Level 2 does not add any additional security requirements to those identified in NIST SP 800-171 R2.
- OSAs will submit the following information in SPRS:
    1. the results of a self-assessment of the OSA's implementation of the NIST SP 800-171 R2 requirements set forth in § 170.16 associated with the covered contractor information system(s) used in performance of the applicable contract.
    2. an initial affirmation of compliance, and, if applicable, a POA&M closeout affirmation, and then annually thereafter, an affirmation of continued compliance set forth in

§ 170.22.

3. the Level 2 self-assessment cost burden will be addressed as part of the 48 CFR part 204 CMMC Acquisition final rule.

Level 2 certification assessment

- Level 2 certification assessment requires compliance with the security requirements set forth in in § 170.17 to protect CUI. CMMC Level 2 does not add any additional security requirements to those selected in NIST SP 800-171 R2.
- A Level 2 certification assessment of the applicable contractor information system(s) provided by an authorized or accredited C3PAO is required to validate implementation of the NIST SP 800-171 R2 security requirements prior to award of any prime contract or subcontract and exercise of option.
- The C3PAO will upload the Level 2 certification assessment results in the CMMC instantiation of eMASS which will feed the information into SPRS.
- OSCs will submit in SPRS an initial affirmation of compliance, and, if necessary, a POA&M closeout affirmation, and then annually following the Final CMMC Status Date, an affirmation of continued compliance as set forth in § 170.22.

The Level 2 certification assessment cost burdens are included in this part with the exception of the requirement for the OSC to upload the affirmation in SPRS that is included in the 48 CFR part 204 CMMC Acquisition final rule and an update to DFARS collection approved under OMB Control Number 0750-0004, *Assessing Contractor Implementation of Cybersecurity Requirements*. Additionally, the information collection reporting requirements for the CMMC instantiation of eMASS are included in a separate ICR for this part and cover only those requirements pertaining to the CMMC process.

Level 3 certification assessment

- Level 3 certification assessment requires the CMMC Status of Final Level 2 (C3PAO) and compliance with the security requirements set forth in § 170.18 to protect CUI. CMMC Level 3 adds additional security requirements to those required by existing acquisition regulations as specified in this rule.
- A Level 3 certification assessment of the applicable contractor information system(s) provided by the DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) is required to validate implementation of the DoD-defined selected security requirements set forth in NIST SP 800-172 Feb2021. A CMMC Status of Final Level 2 (C3PAO) is a prerequisite to schedule a DCMA DIBCAC Level 3 certification assessment.
- DCMA DIBCAC will upload the Level 3 certification assessment results into the CMMC instantiation of eMASS, which will feed the information into SPRS.
- OSCs will submit in SPRS an initial affirmation of compliance, and, if necessary, a POA&M closeout affirmation, and then annually following the Final CMMC Status Date, an affirmation of continued compliance as set forth in § 170.22.

The Level 3 certification assessment cost burdens are included in this part with the exception of the requirement for the OSC to upload the affirmation in SPRS that is included in the 48 CFR part 204 CMMC Acquisition rule and an update to DFARS collection approved under OMB Control Number 0750-0004, Assessing Contractor Implementation of Cybersecurity Requirements. Additionally, the information collection reporting requirements for the CMMC instantiation of eMASS are included in a separate ICR for this part and cover only those requirements pertaining to the CMMC process. As described, the CMMC Program couples an affirmation of compliance with certification assessment requirements to verify OSA implementation of cybersecurity requirements, as applicable.

The CMMC Program addresses DoD's need to protect FCI and CUI during the acquisition and sustainment of products and services from the DIB. This effort is instrumental in ensuring cybersecurity is the foundation of future DoD acquisitions.

Policy Problems Addressed by the revised CMMC Program

Implementation of the CMMC Program is intended to solve the following policy problems:

Lack of Verification of Contractor Compliance with Cybersecurity Requirements

Neither FAR clause 52.204-21 nor DFARS clause 252.204-7012 provide for DoD assessment of a defense contractor or subcontractor's implementation of the information protection requirements within those clauses. Defense contractors represent that they will implement the requirements in NIST SP 800-171 R2 upon submission of their offer. Findings from DoD Inspector General report (DODIG-2019-105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. CMMC adds new assessment requirements for contractor implementation of underlying information security requirements, to allow DoD to assess a defense contractor's cybersecurity posture using authorized or accredited C3PAOs. The contractor and subcontractor must achieve the required CMMC Level as a condition of contract award.

Inadequate Implementation of Cybersecurity Requirements

Under DFARS clause 252.204-7012 and DFARS clause 252.204-7020, defense contractors and subcontractors must document implementation of the security requirements in NIST SP 800171 R2 in a system security plan and may use a plan of action to describe how and when any unimplemented security requirements will be met. For the CMMC Program, the solicitation and resulting contract, will specify the required CMMC Status, which will be determined considering program criticality, information sensitivity, and severity of cyber threat. Although the security requirements in NIST SP 800-171 R2 address a range of threats, additional requirements are needed to significantly reduce the risk posed by APTs. An APT is an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). CMMC Level 3 requires implementation of selected security requirements from NIST SP 800172 Feb2021 to reduce the risk of APT threats.

The CMMC Program will require prime contractors to flow the appropriate CMMC Status requirement down throughout the entire supply chain relevant to a particular contract. Defense contractors or subcontractors that handle FCI, must meet the requirements for CMMC Level 1. Defense contractors that handle CUI must meet the requirements for CMMC Level 2 or higher, depending on the sensitivity of the information associated with a program or technology being developed.

Insufficient Scale and Depth of Resources to Verify Compliance

Today, DoD prime contractors must include DFARS clause 252.204-7012 in subcontracts for which performance will involve covered defense information, but this does not provide the Department with sufficient insights with respect to the cybersecurity posture of all members of a multi-tier supply chain for any given program or technology development effort. The revised CMMC Program requires prime contractors to flow down appropriate CMMC Status requirements, as applicable, to subcontractors throughout their supply chain(s).

Given the size and scale of the DIB, the Department cannot scale its existing cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors and subcontractors every three years. The Department's existing assessment capability is best suited for conducting targeted assessments for the relatively small subset of DoD contractors and subcontractors that support designated high-priority programs involving CUI. CMMC addresses the Department's scaling challenges by utilizing a private-sector accreditation structure. A DoD-authorized Accreditation Body will authorize, accredit, and provide oversight of C3PAOs which in turn will conduct Level 2 certification assessments of actual and prospective DoD contractors and subcontractors. Defense contractors will directly contract with an authorized or accredited C3PAO to obtain a Level 2 certification assessment.

The cost of Level 2 certification assessment activities is driven by multiple factors, including market forces that govern availability of C3PAOs and the size and complexity of the enterprise or enclave under assessment. The Government will perform Level 3 certification assessments.

Government resource limitations may affect schedule availability.

Reduces Duplicate or Respective Assessments of Our Industry Partners

CMMC assessment results will be posted in SPRS, DoD's authoritative source for supplier and product performance information. Posting CMMC assessment results in SPRS precludes the need to validate CMMC implementation on a contract-by-contract basis. This enables DoD to identify whether the CMMC requirements have been met for relevant contractor information systems, avoids duplicative assessments, and eliminates the need for program level assessments, all of which decreases costs to both DoD and industry.

Revised CMMC Program Implementation

The DoD is implementing a phased implementation for the revised CMMC Program and intends to introduce CMMC Status requirements in solicitations over a three-year period to provide appropriate ramp-up time. This phased implementation is intended to minimize the financial impacts to defense contractors, especially small businesses, and disruption to the existing DoD supply chain. After CMMC is implemented in acquisition regulation, DoD will include CMMC self-assessment requirements in solicitations and resulting contracts when warranted by the type of information that will be handled by the contractor of subcontractor(s). CMMC Status requirements for Levels 1, 2, and 3 will be included in solicitations and resulting contracts issued after the phase-in period when warranted by any FCI and/or CUI information protection requirements for the contract effort. In the intervening period, Government Program Managers will have discretion to include CMMC Status requirements or exclude them and rely upon existing DFARS clause 252.204-7012 requirements, in accordance with DoD policy. As stated in § 170.20(a), there is qualified standards acceptance between DCMA DIBCAC High Assessment and the CMMC Status of Level 2(C3PAO), which will result in staggering of the dates for new Level 2 certification assessments. The implementation period will consist of four (4) phases as set forth in § 170.3(e), during which time the Government will include CMMC requirements in certain solicitations and contracts. During the CMMC phase-in period, program managers and requiring activities will be required to include CMMC Status requirements in certain solicitations and contracts and will have discretion to include in others.

A purpose of the phased implementation is to ensure adequate availability of authorized or accredited C3PAOs and assessors to meet the demand.

Revised CMMC Program Flow Down

CMMC Level requirements will be flowed down to subcontractors at all tiers as set forth in § 170.23; however, the specific CMMC Status required for a subcontractor will be based on the type of unclassified information and the priority of the acquisition program and/or technology being developed.

Key Changes Incorporated in the Revised CMMC Program

In November 2021, the Department announced the revised CMMC Program, which is an updated program structure with revised requirements. In the revised CMMC Program, the Department has introduced several key changes that build on and refine the original program requirements. These include:

- Streamlining the model from five levels to three levels.
- Exclusively implementing National Institute of Standards and Technology (NIST) cybersecurity standards and guidelines.
- Allowing all companies subject to Level 1, and a subset of companies subject to Level 2 to demonstrate compliance through self-assessments.
- Increased oversight of professional and ethical standards of CMMC third-party assessors.
- Allowing Plans of Action & Milestones (POA&M) under limited circumstances to achieve conditional certification.

As a result of the alignment of the revised CMMC Program to NIST guidelines, the Department's requirements will continue to evolve as changes are made to the underlying NIST SP 800-171 R2, NIST SP 800-171A Jun2018, NIST SP 800-172 Feb2021, and NIST SP 800-172A Mar2022 requirements.

CMMC Assessment

Assessment Criteria

CMMC requires that defense contractors and subcontractors entrusted with FCI and CUI implement cybersecurity standards at progressively more secure levels, depending on the type and sensitivity of the information.

Level 1 self-assessment

An annual Level 1 self-assessment and annual affirmation asserts that an OSA has implemented all the basic safeguarding requirements to protect FCI as set forth in § 170.14(c)(2). An OSA can choose to perform the annual self-assessment internally or engage a third-party to assist with evaluating its Level 1 compliance. Use of a third party to assist with the assessment process is still considered a self-assessment and results in a CMMC Status of Final Level 1 (Self). An OSA achieve the CMMC Status of Level 1 (Self) for an entire enterprise network or for a particular enclave(s), depending upon where the FCI is or will be processed, stored, or transmitted.

Level 2 self-assessment

A Level 2 self-assessment and annual affirmation attests that an OSA has implemented all the security requirements to protect CUI as specified in § 170.14(c)(3).

Level 2 certification assessment

A Level 2 certification assessment, conducted by a C3PAO, verifies that an OSC is conforming to the security requirements to protect CUI as specified in § 170.14(c)(3). Each OSC information system that will process, store, or transmit CUI in the execution of the contract is subject to the corresponding CMMC Status requirements set forth in the contract.

Level 3 certification assessment

Achievement of the CMMC Status of Final Level 2 (C3PAO) for information systems within the Level 3 CMMC Assessment Scope is a prerequisite for initiating a Level 3 certification assessment. A Level 3 certification assessment, conducted by DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), verifies that an OSC has implemented the CMMC Level 3 security requirements to protect CUI as specified in § 170.14(c)(4). A Level 3 certification assessment must be conducted for each OSC information system that will be used in the execution of the contract that will process, store, or transmit CUI.

Impact and Cost Analysis of the Revised CMMC Program

Summary of Impact

Public comment feedback on the initial CMMC Program indicated that cost estimates were too low. The revised CMMC Program cost estimates account for that feedback with the following improvements:

- Allowance for outsourced IT services
- Increased total time for the contractor to prepare for the assessment, including limited time for learning the reporting and affirmation processes
- Allowance for use of consulting firms to assist with the assessment process • Time for a senior level manager to review the assessment and affirmation before submitting the results in SPRS
- Updated government and contractor labor rates that include applicable burden costs

As a result, some costs of the revised CMMC Program may be higher than those included in the initial CMMC Program.

The revised CMMC Program impact analysis includes estimated costs for implementation of the revised CMMC Program requirements across Level 1, Level 2, and Level 3 for the Public (small and other than small entities, including the CMMC Ecosystem as set forth in 32 CFR subpart C) and the Government. In summary, the total estimated Public and Government costs associated with this rule, calculated for a 20-year horizon in 2023 dollars at a 7 percent discount rate and a 3 percent discount rate are provided as follows:

Table 3 - Total Estimated Costs of CMMC Requirements for the Public and the Government
(7 percent discount)

Total cost	Public	Government	Total
Annualized Costs	$3,989,182,374	$9,508,593	$3,998,690,967
Present Value Costs	$42,261,454,899	$100,734,168	$42,362,189,067

Table 4 - Total Estimated Costs of CMMC Requirements for the Public and the Government
(3 percent discount)

Total cost	Public	Government	Total
Annualized Costs	$4,219,513,555	$9,953,205	$4,229,466,760
Present Value Costs	$62,775,706,830	$148,078,564	$62,923,785,394

Estimating the number of CMMC assessments for unique entities per level per year is complicated by the fact that companies may serve as a prime contractor on one effort but a subcontractor on others, and may also enter into subcontract agreements with more than one prime contractor for various opportunities.

In addition, the CMMC Program relies upon free market influences of supply and demand to propel implementation. Specifically, the Department does not control which defense contractors aspire to compete for which business opportunities, nor does it control access to the assessment services offered by C3PAOs. OSAs may elect to complete a self-assessment or pursue a certification assessment at any time after issuance of the rule, in an effort to distinguish themselves as competitive for efforts that require an ability to adequately protect CUI. For that reason, the number of CMMC assessments for unique entities per level per year may vary significantly from the assumptions used in generating the cost estimate. The estimates represent the best estimates at this time based on internal expertise and public feedback.

DoD utilized historical metrics gathered for the initial CMMC Program and subject matter expertise from Defense Pricing and Contracting (DPC) and DCMA DIBCAC to estimate the number of entities by type and by assessment level for this analysis. The following table summarizes the estimated profile used in this analysis.

Table 5 - Estimated Number of Entities by Type and Level

Assessment Level	Small	Other than Small	Total	Percent
Level 1 self-assessment	103,010	36,191	139,201	63%
Level 2 self-assessment	2,961	1,039	4,000	2%
Level 2 certification assessment	56,689	19,909	76,598	35%
Level 3 certification assessment	1,327	160	1,487	1%
Total	**163,987**	**57,299**	**221,286**	100%
Percent	74%	26%	100%	

DoD is planning for a phased roll-out of each assessment level across 7 years with the entity numbers reaching a maximum by Year 4 as shown in the tables. The target of Year 4 was selected based on the projected capacity of the CMMC Ecosystem to grow to efficiently support the entities in the pipeline. For modeling efficiency, a similar roll-out is assumed regardless of entity size or assessment level. It is assumed that by year 7 the maximum number of entities is reached. Beyond year 7, the number of entities entering and exiting are expected to net to zero. The following tables reflect the number of new entities in each year and for each level.

Table 6 - *Number of Small Entities Over Phase-In Period

	Level 1	Level 2	Level 2	Level 3	

Yr	Self-Assess	Self-Assess	Certification	Certification	Total
1	699	20	382	3	1,104
2	3,493	101	1,926	45	5,565
3	11,654	335	6,414	151	18,554
4	22,336	642	12,293	289	35,560
5	22,333	642	12,289	289	35,553
6	22,333	642	12,289	289	35,553
7	20,162	579	11,096	261	32,098
Tot	**103,010**	**2,961**	**56,689**	**1,327**	**163,987**

Table 7 - *Number of Other than Small Entities Over Phase-In Period

	Level 1	Level 2	Level 2	Level 3	
Yr	Self-Assess	Self-Assess	Certification	Certification	Total
1	246	7	135	1	389
2	1,227	35	673	5	1,940
3	4,094	118	2,252	18	6,482
4	7,848	225	4,317	34	12,424
5	7,846	225	4,317	34	12,422
6	7,846	225	4,317	34	12,422
7	7,084	204	3,898	34	11,220
Tot	**36,191**	**1,039**	**19,909**	**160**	**57,299**

Table 8 - *Number of Total Entities Over Phase-In Period

	Level 1	Level 2	Level 2	Level 3	
Yr	Self-Assess	Self-Assess	Certification	Certification	Total
1	945	27	517	4	1,493
2	4,720	136	2,599	50	7,505
3	15,748	453	8,666	169	25,036
4	30,184	867	16,610	323	47,984
5	30,179	867	16,606	323	47,975
6	30,179	867	16,606	323	47,975
7	27,246	783	14,994	295	43,318
Tot	**139,201**	**4,000**	**76,598**	**1,487**	**221,286**

Public Costs

Summary of Impacted Awardee Entities

According to data available in the Electronic Data Access system for fiscal years (FYs) 2019,

2020, and 2021, DoD awards an average of 1,366,262 contracts and orders per year that contain DFARS clause 252.204-7012, to 31,338 unique awardees, of which 683,718 awards (50%) are made to 23,475 small entities (75%).[36]

Public Cost Analysis

The following is a summary of the estimated Public costs the revised CMMC Program for other than small[37] entities, per assessment of a contractor information system, at the required periodicity for each CMMC level.

Table 9 - Other Than Small Entities (per Assessment)

Assessment Phase ($)	Level 1 selfassessment[39]	Level 2 selfassessment[39]	Level 2 certification assessment	Level 3 certification assessment
Periodicity	Annual	Triennial	Triennial	Triennial
Plan and Prepare the Assessment	$1,146	$18,015	$26,264	$7,066
Conduct the Assessment	$1,728	$19,964	$80,656	$23,136
Report Assessment Results	$584	$2,712	$2,712	$2,712
Annual Affirmation(s)	$584	*$8,136	*$8,136	*$8,136
Subtotal	$4,042	$48,827	$117,768	$41,050
** POA&M	$0	$0	$0	$3,394
Total (across 3 years)	**$4,042**	**$48,827**	**$117,768**	**$44,444**

*Reflects the 3-year cost to match the periodicity.

**Requirements NOT MET (if needed and when allowed) will be documented in a Plan of Action and Milestones.

The following is a summary of the estimated Public costs of the revised CMMC Program for Small Entities, per assessment of each contractor information system, estimated at one per entity, at the required periodicity for each CMMC level.

Table 10 - Small Entities (per Assessment)

Assessment Phase ($)	Level 1 selfassessment[40]	Level 2 selfassessment[40]	Level 2 certification assessment	Level 3 certification assessment
Periodicity	Annual	Triennial	Triennial	Triennial
Plan and Prepare the Assessment	$1,803	$14,426	$20,699	$1,905
Conduct the Assessment	$2,705	$15,542	$76,743	$1,524
Report Assessment Results	$909	$2,851	$2,851	$1,876
Affirmations	$560	*$4,377	*$4,377	*$5,628
Subtotal	$5,977	$37,196	$104,670	$10,933
**POA&M	$0	$0	$0	$1,869
Total	**$5,977**	**$37,196**	**$104,670**	**$12,802**

[36] The number of unique awardees impacted each year is 1/3 of the average number of annual awardees according to the Electronic Data Access system (31,338/3 = 10,446). This estimate does not address new entrants or awardees who discontinue doing business with DoD.

[37] Includes all businesses with the exception of those defined under the small business criteria and size standards provided in 13 CFR 121.201 (See FAR Part 19.102)

*Reflects the 3-year cost to match the periodicity.

[39] The Level 1 self-assessment and Level 2 self-assessment information collection reporting and recordkeeping requirements will be included in a modification of an existing DFARS collection approved under OMB Control Number 0750-0004, Assessing Contractor Implementation of Cybersecurity Requirements. Modifications to this DFARS collection will be addressed as part of the 48 CFR part 204 CMMC Acquisition rule.

[40] The Level 1 self-assessment and Level 2 self-assessment information collection reporting and recordkeeping requirements will be included in a modification of an existing DFARS collection approved under OMB Control Number 0750-0004, Assessing Contractor Implementation of Cybersecurity Requirements. Modifications to this DFARS collection will be addressed as part of the 48 CFR part 204 CMMC Acquisition rule.

**Requirements "NOT MET" (if needed and when allowed) will be documented in a Plan of Action and Milestones.

The total estimated Public (large and small entities) costs associated with this rule, calculated for a 20-year horizon in 2023 dollars at a 7 percent and 3 percent discount rate, per OMB guidance, is provided as follows:

Table 11 - Total Estimated Costs of CMMC Requirements for Large and Small Entities

Public Costs	7% Discount	3% Discount
Annualized Costs	$3,989,182,374	$4,219,513,555
Present Value Costs	$42,261,454,899	$62,775,706,830

Assumptions

In estimating the Public costs, DoD considered applicable nonrecurring engineering costs, recurring engineering costs[38], assessment costs, and affirmation costs for each CMMC Level. For CMMC Levels 1 and 2, the cost estimates are based only upon the self-assessment, certification assessment, and affirmation activities that a defense contractor, subcontractor, or ecosystem member must take to allow DoD to verify implementation of the relevant underlying security requirements, i.e., for CMMC Level 1, the security requirements set forth in FAR clause 52.204-21, and for CMMC Level 2, the security requirements set forth in NIST SP 800-171 R2. DoD did not consider the cost of implementing the security requirements themselves because implementation is already required by FAR clause 52.204-21, effective June 15, 2016, and by DFARS clause 252.204-7012, requiring implementation by Dec. 31, 2017, respectively; therefore, the costs of implementing the security requirements for CMMC Levels 1 and 2 should already have been incurred and are not attributed to this rule. As such, the nonrecurring engineering and recurring engineering costs to implement the security requirements defined for CMMC Level 1 and Level 2 are not included in this economic analysis. However, cost estimates to implement CMMC Level 3, are included, as that CMMC level will require defense contractors and subcontractors, as applicable, to implement a DoD-defined subset of the security requirements set forth in NIST SP 800-172 Feb2021, a new addition to current security protection requirements.

In estimating the public cost for a defense contractor small entity to comply with CMMC Program requirements for each CMMC level, DoD considered non-recurring engineering costs, recurring engineering costs, assessment costs, and affirmation costs for each CMMC Level. These costs include labor and consulting.

Estimates include size and complexity assumptions to account for typical organizational differences between small entities and other than small entities with respect to the handling of Information Technology (IT) and cybersecurity:

- small entities are likely to have a less complex, less expansive operating environment and IT / Cybersecurity infrastructure compared to larger defense contractors
- small entities are likely to outsource IT and cybersecurity to an External Service Provider (ESP)

[38] The terms nonrecurring engineering costs and recurring engineering costs are terms of art and do not only encompass actual engineering costs.

- entities (small and other than small) pursuing Level 2 self-assessment are likely to seek consulting or implementation assistance from an ESP to either help them prepare for the assessment technically or participate in the assessment with the C3PAOs.

Estimates do not include the cost to implement (Non-recurring Engineering Costs (NRE)) or maintenance costs (Recurring Engineering (RE)) associated with the security requirements prescribed in current regulations.

For CMMC Levels 1 and 2, cost estimates are based upon assessment, reporting, and affirmation activities that a contractor or subcontractor will need to take to verify implementation of existing security requirements set forth in FAR clause 52.204-21, effective June 15, 2016, to protect FCI, and DFARS clause 252.204-7012 which required implementation of NIST SP 800171 requirements not later than December 31, 2017, to protect CUI. As such, cost estimates are not included for an entity to implement the CMMC Level 1 or 2 security requirements, maintain implementation of these existing security requirements, or remediate a plan of action for unimplemented requirements.

For CMMC Level 3, the cost estimates factor in the assessment, reporting, and affirmation activities in addition to estimates for NRE and RE to implement and maintain CMMC Level 3 security requirements. In addition to implementing the CMMC Level 2 security requirements, CMMC Level 3 requires implementing selected security requirement set forth in NIST SP 800-172 Feb2021 as described in § 170.14(c)(4) which are not currently required through other regulations. CMMC Level 3 is expected to apply only to a small subset of defense contractors and subcontractors.

The Cost Categories used for each CMMC Level are described:

1. ***Nonrecurring Engineering Costs:*** Estimates consist of hardware, software, and the associated labor to implement the same. Costs associated with implementing the requirements set forth in FAR clause 52.204-21 and NIST SP 800-171 R2 are assumed to have been already implemented and, therefore, are not accounted for in this cost estimate. As such, these costs only appear in CMMC Level 3. If nonrecurring engineering costs are referenced, they are only accounted for as a one-time occurrence and are reflected in the year of the initial assessment.

2. ***Recurring Engineering Costs:*** Estimates consist of annually recurring fees and associated labor for technology refresh. Costs associated with implementing the requirements set forth in FAR clause 52.204-21 and NIST SP 800-171 R2 are assumed to have been already implemented and, therefore, are not accounted for in this cost estimate. As such, these costs only appear in CMMC Level 3.

3. ***Assessment Costs****:* Estimates consist of activities for pre-assessment preparations (which includes gathering and/or developing evidence that the assessment objectives for each requirement have been satisfied), conducting and/or participating in the actual assessment, and completion of any post-assessment work. Assessment costs are represented by notional phases. Assessment costs assume the OSA passes the assessment on the first attempt (conditional – with an allowable POA&M or final). Each phase includes an estimate of hours to conduct the assessment activities including:

(a) Labor hour estimates for a company (and any ESP support) to prepare for and participate in the assessment.

(b) C3PAO cost estimates for companies pursuing a certification

- labor hour estimates for authorized or certified assessors to work with the business to conduct the actual assessment
- Assessment Costs broken down into phases
- Phase 1: Planning and preparing for the assessment
- Phase 2: Conducting the assessment (self or C3PAO)
- Phase 3: Reporting of Assessment Results
- Phase 4: POA&M Closeout (for CMMC Level 3 only, if applicable and allowed)
- CMMC allows a limited open Plan of Action and Milestones (POA&M) for a period of 180 days to remediate the POA&M, see § 170.21.

4. ***Affirmations:*** Estimates consist of costs for an OSA to submit to SPRS an initial and, as applicable, any subsequent affirmations of compliance that the contractor information system is compliant with and will maintain compliance with the security requirements of the applicable CMMC Level. If POA&Ms are allowed, an affirmation must be submitted with the POA&M closeout. With the exception of Small Entities for Level 1 and Level 2, it is assumed the task requires the same labor categories and estimated hours as the final reporting phase of the assessment.

The categories and rates used for estimating purposes were compiled by subject matter experts based on current data available from within the DoD contractor database for comparable labor categories. A factor estimate of 30 percent was added to the labor rate per hour to include but are not limited to company-sponsored benefits (fringe) and limited employee-related expenses such as training and certifications. This estimate is based on labor performed by indirect personnel (i.e., personnel who are part of overhead expense); therefore, the 30 percent factor represents an estimate for fringe expense and G&A expenses versus full overhead expense. The categories and rates inclusive of the labor cost plus the additional factor are defined in the table.

Table 12 - Other than Small Entities - Labor Rates Used for Estimate

Code[39]	Rate per Hour[40]	Description	Background / Years' Experience[41]	With Master's Degree[44]
IT5	$ 116.87	Senior Staff IT Specialist	Cyber Background, 10 + years	
IT4	$ 97.49	Staff IT Specialist	Cyber Background, 7-10 years	5-7 years
IT3	$ 81.96	Senior IT Specialist	Cyber Background, 5-7 years	2-5 years
IT2	$ 54.27	IT Specialist	Cyber Background, 2-5 years	0-2 years
IT1	$ 36.32	Associate IT Specialist	Cyber Background, 0-2 years	
MGMT5	$ 190.52	Director	Chief Info. Systems Officer/ Chief Info. Officer	
MGMT4	$ 143.50	Staff Manager	Vice President	
MGMT3	$ 128.64	Senior Manager	Program Manager	
MGMT2	$ 95.96	Manager	5-7 years	
MGMT1	$ 82.75	Associate Manager	1-5 years	
C3PAO[45]	$ 260.28	Cyber Subject Matter Expert	4 years	

Table 13 - Small Entities – Labor Rates Used for Estimate

Code[42]	Rate per Hour[43]	Description	Background / Years' Experience[44]	Master's Degree[44]
MGMT5	$ 190.52	Director	Chief Info. Systems Officer / Chief Info. Officer	

[39] IT = Information Technology, MGMT = Management

[40] IT and MGMT rates represent an estimate for in-house labor and includes the labor rate plus fringe and employeerelated expenses

[41] Background assumes a Bachelor's degree as the minimum education level, additional requirements are noted including required years of experience. A Master's degree may reduce the required years of experience as noted. [45] The ESP / C3PAO rate represents an estimate for outsourced labor and includes the labor rate, overhead expense, G&A expense, and profit.

IT4-SB	$ 86.24	Staff IT Specialist	Cyber Background, 7-10 years	5-7 years
ESP / C3PAO[45]	$ 260.28	Cyber Subject Matter Expert	4 years	

CMMC Level 1 Self-Assessment and Affirmation Costs

Other Than Small Entities

- ***Nonrecurring and recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with CMMC Level 1, since it is assumed that the contractor or subcontractor has already implemented the applicable security requirements.[42]
- ***Assessments Costs****:* It is estimated that the cost to support a CMMC Level 1 selfassessment and affirmation is ***$4,042** (as summarized in 4.1.2, table 9). A Level 1 selfassessment is conducted annually, and is based on the assumptions detailed:
  - **Phase 1: Planning and preparing for the self-assessment: $1,146**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
  - **Phase 2: Conducting the self-assessment**: **$1,728**
    - A director (MGMT5) for 6 hours ($190.52/hr x 6hrs = $1,143)
    - A staff IT specialist (IT4) for 6 hours ($97.49/hrs x 6hrs = $585)
  - **Phase 3: Reporting of self-assessment results** into SPRS: **$584**
    - A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
    - A staff IT specialist (IT4) for 2.08 hours ($97.49/hrs x 2.08hrs = $203)
    - **Affirmations**: It is estimated that the costs to perform an initial and annual affirmation of compliance with CMMC Level 1 for an "other than small" entity is **$584**
    - A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
    - A staff IT specialist (IT4) for 2.08 hours ($97.49/hrs x 2.08hrs = $203)
    - The Level 1 self-assessment and affirmations cost burden will be addressed as part of the 48 CFR part 204 CMMC Acquisition rule.
    - **Summary:** The following is the annual other than small entities total cost summary for Level

1 self-assessments and affirmations over a ten-year period: (Example calculation, Year 1: ***$4,042** per entity x 246 entities (cumulative) = $994,233)

Table 14 –Level 1: Self-Assessment for Other Than Small Entities

Year	Other than Small Entities Per Year	Cumulative Other Than Small Entities	Annual Total Cost (self-assess, affirm)
1	246	246	$994,233
2	1,227	1,473	$5,953,271
3	4,094	5,567	$22,499,565
4	7,848	13,415	$54,218,010
5	7,846	21,261	$85,928,372
6	7,846	29,107	$117,638,733
7	7,084	36,191	$146,269,399
8		36,191	$146,269,399
9		36,191	$146,269,399
10		36,191	$146,269,399

[42] CMMC Level 1 consists of the same 15 basic safeguarding requirements specified in FAR clause 52.204-21. This cost analysis assumes that defense contractors and subcontractors already have contracts with FAR clause 52.204-21 and, therefore, have already implemented the 15 basic safeguarding requirements.

Total	**36,191**		**$872,309,779**

Small Entities

- ***Nonrecurring and recurring engineering costs***: There are no nonrecurring or recurring engineering costs associated with CMMC Level 1 since it is assumed the contractor or subcontractor has implemented the applicable security requirements.[43]
- ***Assessment Costs and Initial Affirmation Costs:*** It is estimated that the cost to support a CMMC Level 1 self-assessment and affirmation is ***$5,977** (as summarized in 4.1.2, table 10). A Level 1 self-assessment is conducted annually, and is based on the assumptions detailed:
  - **Phase 1: Planning and preparing for the self-assessment**: **$1,803**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - An external service provider (ESP) for 4 hours ($260.28 x 4hrs = $1,041)
  - **Phase 2: Conducting the self-assessment: $2,705**
    - A director (MGMT5) for 6 hours ($190.52/hr x 6hrs = $1,143)
    - An external service provider (ESP) for 6 hours ($260.28 x 6hrs = $1,562)
  - **Phase 3: Reporting of assessment results into SPRS: $909**
    - A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
    - An external service provider (ESP) for 2 hours ($260.28/hr * 2hrs = $521)
    - A staff IT specialist (IT4-SB) for 0.08 hours48 ($86.24/hr x 0.08hrs = $7)
    - **Affirmation:** initial affirmation post assessment: **$ 560**
    - ***Reaffirmations:*** It is estimated that the costs to reaffirm a CMMC Level 1 annually for a small entity is **$560**
    - A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
    - A staff IT specialist (IT4-SB) for 2.08 hours ($86.24/hr x 2.08hrs = $179)
    - The Level 1 self-assessment and affirmations cost burden will be addressed as part of the 48 CFR part 204 CMMC Acquisition rule.
    - ***Summary:*** The following is the annual small entities total cost summary for Level 1 selfassessments and affirmations over a ten-year period: (Example calculation, Year 1: *$5,977 per entity x 699 entities (cumulative) = $4,177,845)

Table 15 – Level 1: Self-Assessment for Small Entities

Year	Small Entities Per Year	Cumulative Small Entities	Annual Total Cost (self-assess, affirm)
1	699	699	$4,177,845
2	3,493	4,192	$25,055,116
3	11,654	15,846	$94,709,771
4	22,336	38,182	$228,209,547
5	22,333	60,515	$361,691,392
6	22,333	82,848	$495,173,237
7	20,162	103,010	$615,679,258
8		103,010	$615,679,258
9		103,010	$615,679,258
10		103,010	$615,679,258
Total	**103,010**		**$3,671,733,942**

[48] A person needs to enter the information into SPRS, which should only take five minutes.

All Entities Summary

[43] Again, it is assumed that that defense contractors and subcontractors have already implemented the 15 basic safeguarding requirements in FAR clause 52.204-21.

The following is a summary of the combined costs for both small and other than small entities for Level 1 self-assessments and affirmations over a ten-year period:

Table 16 – Level 1: Self-Assessment for All Entities

Year	Entities Per Year	Cumulative Entities	Total Cost (Self-Assess and Affirmation)
1	945	945	$5,172,077
2	4,720	5,665	$31,008,386
3	15,748	21,413	$117,209,336
4	30,184	51,597	$282,427,557
5	30,179	81,776	$447,619,764
6	30,179	111,955	$612,811,971
7	27,246	139,201	$761,948,657
8	0	139,201	$761,948,657
9	0	139,201	$761,948,657
10	0	139,201	$761,948,657
Total	**139,201**		**4,544,043,721**

CMMC Level 2 Self-Assessment and Affirmation Costs

Other Than Small Entities

- ***Nonrecurring and Recurring Engineering Costs:*** There are no nonrecurring or recurring engineering costs associated with Level 2 self-assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 R2 security requirements.
- ***Self-Assessment Costs and Initial Affirmation Costs:*** It is estimated that the cost to support a Level 2 self-assessment and affirmation is *$43,403. The three-year cost is $48,827 (as summarized in 4.1.2, table 9), which includes the triennial assessment + affirmation, and two additional annual affirmations ($43,403 + $2,712 + $2,712).

- **Phase 1: Planning and preparing for the self-assessment: $18,015**
  - A director (MGMT5) for 30 hours ($190.52/hr x 30hrs = $5,716)
  - A manager (MGMT2) for 40 hours ($95.96/hr x 40hrs = $3,838)
  - A staff IT specialist (IT4) for 46 hours ($97.49/hr x 46hrs = $4,485)
  - A senior IT specialist (IT3) for 26 hours ($81.96/hr x 26hrs = $2,131)
  - An IT specialist (IT2) for 34 hours ($54.27/hr x 34hrs = $1,845)
- **Phase 2: Conducting the self-assessment: $19,964**
  - A director (MGMT5) for 24 hours ($190.52/hr x 24hrs = $4,572)
  - A manager (MGMT2) for 24 hours ($95.96/hr x 24hrs = $2,303)
  - A staff IT specialist (IT4) for 56 hours ($97.49/hr x 56hrs = $5,460)
  - A senior IT specialist (IT3) for 56 hours ($81.96/hr x 56hrs = $4,590)
  - An IT specialist (IT2) for 56 hours ($54.27/hr x 56hrs = $3,039)
- **Phase 3: Reporting of self-assessment results into SPRS: $2,712**
  - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
  - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
  - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
  - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
  - **Affirmation:** initial affirmation post assessment: **$ 2,712**
  - **Reaffirmations:** It is estimated that the cost to perform an annual affirmation for CMMC

  Level 2 self-assessment is **$2,712** (three-year cost is $8,136, or $2,712 x 3):
  - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)

- A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
- A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
- A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
- The Level 2 self-assessment and affirmations cost burden will be addressed as part of the 48

CFR part 204 CMMC Acquisition rule.

- **Summary:** The following is the annual other than small entities total cost summary for CMMC Level 2 self-assessments and affirmations over a ten-year period: (Example calculation, Year 2: **(*$43,403** assessment per entity x 35 entities) + **($2,712** annual affirmation per entity x 7 entities) = $1,538,092

Table 17 - Level 2: Self-Assessment for Other Than Small Entities

Year	Entities Performing Triennial Self-Assessments including initial affirmation	Entities Performing Annual Affirmation Actions Only	Total Cost
1	7	0	$303,821
2	35	7	$1,538,092
3	118	42	$5,235,473
4	232	153	$10,484,485
5	260	350	$12,234,099
6	343	492	$16,221,701
7	436	603	$20,559,249
8	260	779	$13,397,691
9	343	696	$16,775,017
10	436	603	$20,559,249
Total	**2,470**	**3,725**	**$117,308,877**

Small Entities

- ***Nonrecurring and recurring engineering costs:*** There are no nonrecurring or recurring engineering costs associated with Level 2 self-assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 R2 security requirements.
- ***Self-Assessment Costs and Initial Affirmation Costs:*** It is estimated that the cost to support a Level 2 self-assessment and affirmation for a small entity is ***$34,277**. The three-year cost is $37,196 (as summarized in 4.1.2, table 10), which includes the triennial assessment + affirmation, plus two additional annual affirmations ($34,277 + $1,459 + $1,459).
  - **Phase 1: Planning and preparing for the self-assessment: $14,426**
  - A director (MGMT5) for 32 hours ($190.52/hr x* 32hrs = $6,097)
  - An external service provider (ESP) for 32 hours ($260.28/hr x 32hrs = $8,329)
  - **Phase 2: Conducting the self-assessment: $15,542**
  - A director (MGMT5) for 16 hours ($190.52/hr x 16hrs = $3,048)
  - An external service provider (ESP) for 48 hours ($260.28/hr x 48hrs = $12,493)
  - **Phase 3: Reporting of self-assessment results into SPRS: $2,851**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - An external service provider (ESP) for 8 hours ($260.28/hr x 8hrs = $2,082)
    - A staff IT specialist (IT4-SB) for 0.08 hours ($86.24/hr x 0.08hrs = $7)
    - **Affirmation:** initial affirmation post assessment: **$ 1,459**

- **Reaffirmations:** It is estimated that the costs to reaffirm a Level 2 self-assessment annually is **$1,459** (three-year costs to reaffirm a Level 2 self-assessment annually is

$4,377, or $1,459 x 3):

- A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
- A staff IT specialist (IT4-SB) for 8.08 hours ($86.24/hr x 8.08hrs = $697)
- The Level 2 self-assessment and affirmations cost burden will be addressed as part of the 48 CFR part 204 CMMC Acquisition rule.
- ***Summary****:* The following is the annual small entities total cost summary for Level 2 selfassessments and affirmations over a ten-year period: (Example calculation, Year 2: **(*$34,277** self-assessment per entity x 101 entities) + (**$1,459** annual affirmation per entity x 20 entities) = $3,491,193)

Table 18 - Level 2: Self-Assessment for Small Entities

Year	Entities Performing Triennial Self-Assessments including initial affirmation	Entities Performing Annual Affirmation Actions Only	Total Cost
1	20	0	$685,547
2	101	20	$3,491,193
3	335	121	$11,659,448
4	662	436	$23,327,706
5	743	997	$26,922,622
6	977	1,405	$35,538,762
7	1,241	1,720	$45,047,546
8	743	2,218	$28,703,951
9	977	1,984	$36,383,471
10	1,241	1,720	$45,047,546
Total	**7,040**	**10,621**	**$256,807,792**

All Entities Summary

The following is a summary of the cost to all entities regardless of size for Level 2 selfassessments and affirmations over a ten-year period:

Table 19 - Level 2: Self-Assessment for All Entities

Year	Entities Performing Triennial Self-Assessments and initial affirmation	Entities Performing Annual Reaffirmations Actions Only	Total Cost
1	27	0	$989,369
2	136	27	$5,029,285
3	453	163	$16,894,921
4	894	589	$33,812,191
5	1,003	1,347	$39,156,721
6	1,320	1,897	$51,760,463
7	1,677	2,323	$65,606,795
8	1,003	2,997	$42,101,642
9	1,320	2,680	$53,158,488
10	1,677	2,323	$65,606,795

Total	**9,510**	**14,346**	**$374,116,669**

CMMC Level 2 Certification Assessment and Affirmation Costs

Other Than Small Entities

- ***Nonrecurring and recurring engineering costs**:* There are no nonrecurring or recurring engineering costs associated with Level 2 certification assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 R2 security requirements.
- ***Assessment and Initial Affirmation Costs:*** It is estimated that the cost to support a Level 2 certification assessment and annual affirmation for an "other than small" entity is *$112,345. The three-year cost is $117,768 (as summarized in 4.1.2, table 9), and includes a triennial assessment + affirmation, plus two additional annual affirmations ($112,345 + $2,712 + $2,712, with a minor rounding difference.)
  - **Phase 1: Planning and preparing for the certification assessment: $26,264**
    - A director (MGMT5) for 32 hours ($190.52/hr x 32hrs = $6,097)
    - A manager (MGMT2) for 64 hours ($95.96/hr x 64hrs = $6,141)
    - A staff IT specialist (IT4) for 72 hours ($97.49/hr x 72hrs = $7,019)
    - A senior IT specialist (IT3) for 40 hours ($81.96/hr x 40hrs = $3,278)
    - An IT specialist (IT2) for 58 hours ($54.27/hr x 58hrs = $3,148)
    - An associate IT specialist (IT1) for 16 hours ($36.32/hr x 16hrs = $581)
  - **Phase 2: Conducting the certification assessment: $28,600**
    - A director (MGMT5) for 32 hours ($190.52/hr x 32hrs = $6,097)
    - A manager (MGMT2) for 32 hours ($95.96/hr x 32hrs = $3,071)
    - A staff IT specialist (IT4) for 72 hours ($97.49/hr x 72hrs = $7,019)
    - A senior IT specialist (IT3) for 72 hours ($81.96/hr x 72hrs = $5,901)
    - An IT specialist (IT2) for 120 hours ($54.27/hr x 120hrs = $6,512)
  - **Phase 3: Reporting of certification assessment results: $2,712**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
    - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
    - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
    - **Affirmations:** initial affirmation post assessment: **$2,712**
  - **C3PAO Costs: C3PAO engagement inclusive of Phases 1, 2, and 3 (5-person** team) for 200 hours ($260.28/hr x 200hrs = **$52,056**)
  - **Reaffirmations:** It is estimated that the costs to reaffirm a Level 2 certification assessment annually is **$2,712** (three-year cost is $8,136 or $2,712 x 3)
  - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
  - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
  - A staff IT specialist (IT4) for 8 hours ($97.49/hr x 8hrs = $1,560)
  - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
  - The Level 2 affirmations cost burden will be addressed as part of the 48 CFR part 204 CMMC

  Acquisition rule.
- ***Summary**:* The following is the annual other than small entities total cost summary for Level 2 certification assessments and affirmations over a ten-year period: (Example calculation, Year 2: (***$112,345** assessment per entity x 673 entities) + (**$2,712** annual affirmation per entity x 135 entities) = $75,974,425)

Table 20 - Level 2: Certification Assessment for Other Than Small Entities

Year	Entities Performing Triennial Certifications and initial affirmation	Entities Performing Annual Reaffirmation Actions Only	Total Cost
1	135	0	$15,166,590

2	673	135	$75,974,425
3	2,252	808	$255,192,758
4	4,452	2,925	$508,094,016
5	4,990	6,704	$578,785,599
6	6,569	9,442	$763,604,903
7	8,350	11,559	$969,433,559
8	4,990	14,919	$601,067,429
9	6,569	13,340	$774,177,583
10	8,350	11,559	$969,433,559
Total	**47,330**	**71,391**	**$5,510,930,421**

Small Entities

- ***Nonrecurring or recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with Level 2 certification assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 R2 security requirements.
- ***Assessment Costs and Initial Affirmation Costs****:* It is estimated that the cost to support a Level 2 certification assessment and affirmation for a small entity is ***$101,752.** The threeyear cost is $104,670 (as summarized in 4.1.2, table 10), and includes the triennial assessment + affirmation plus two additional annual affirmations ($101,752 + $1,459 + $1,459).
  - **Phase 1: Planning and preparing for the certification assessment: $20,699**
  - A director (MGMT5) for 54 hours ($190.52/hr x 54hrs = $10,288)
  - An external service provider (ESP) for 40 hours ($260.28/hr x 40hrs = $10,411)
  - **Phase 2: Conducting the certification assessment: $45,509**
    - A director (MGMT5) for 64 hours ($190.52/hr x 64hrs = $12,193)
    - An external service provider (ESP) for 128 hours ($260.28/hr x 128hrs = $33,316)
  - **Phase 3: Reporting of certification assessment results: $2,851**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - An ESP for 8 hours ($260.28/hr x 8hrs = $2,082)
    - A staff IT specialist (IT4-SB) for 0.08 hours ($86.24/hr x 0.08hrs = $7)
  - **Affirmations: cost to post initial affirmation $1,459**
- **C3PAO Costs:** C3PAO engagement inclusive of Phases 1, 2, and 3 (3-person team) for 120 hours ($260.28/hr x 120hrs = **$31,234**)
- ***Reaffirmations****:* It is estimated that the costs to reaffirm a Level 2 certification assessment annually is **$1,459** (three-year cost is $4,377, or $1,459 x 3)
- A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
- A staff IT specialist (IT4-SB) for 8.08 hours ($86.24/hr x 8.08hrs = $697) • The Level 2 affirmations cost burden will be addressed as part of the 48 CFR part 204 CMMC Acquisition rule.
- ***Summary****:* The following is the annual small entities total cost summary for Level 2 certification assessments and affirmations over a ten-year period: (Example calculation, Year 2: (***$101,752** assessment per entity x 1,926 entities) + (**$1,459** annual affirmation per entity x 382 entities) = $196,531,451)

Table 21 - Level 2: Certification Assessment for Small Entities

Year	Entities Performing Triennial Certifications and initial affirmation	Entities Performing Annual Reaffirmation Actions Only	Total Cost

1	382	0	$38,869,223
2	1,926	382	$196,531,451
3	6,414	2,308	$656,003,811
4	12,675	8,340	$1,301,872,564
5	14,215	19,089	$1,474,252,306
6	18,703	26,890	$1,942,295,763
7	23,771	32,918	$2,466,768,671
8	14,215	42,474	$1,508,368,920
9	18,703	37,986	$1,958,483,830
10	23,771	32,918	$2,466,768,671
Total	**134,775**	**203,305**	**$14,010,215,209**

All Entities Summary

The following is a summary of the cost to all entities regardless of size for Level 2 certification assessment and affirmation costs over a ten-year period:

Table 22 - Level 2: Certification Assessment for All Entities

Year	Entities Performing Triennial Certifications and initial affirmation	Entities Performing Reaffirmation Actions Only	Total Cost
1	517	0	$54,035,813
2	2,599	517	$272,505,876
3	8,666	3,116	$911,196,569
4	17,127	11,265	$1,809,966,579
5	19,205	25,793	$2,053,037,904
6	25,272	36,332	$2,705,900,665
7	32,121	44,477	$3,436,202,230
8	19,205	57,393	$2,109,436,349
9	25,272	51,326	$2,732,661,414
10	32,121	44,477	$3,436,202,230
Total	**182,105**	**274,696**	**$19,521,145,630**

CMMC Level 3 Certification Assessment and Affirmation Costs

An OSC pursuing Level 3 certification assessment must have a CMMC Status of Final Level 2 (C3PAO), and also must demonstrate compliance with CMMC Level 3, which includes implementation of selected security requirements from NIST SP 800-172 Feb2021 not required in prior rules. Therefore, the Nonrecurring Engineering and Recurring Engineering cost estimates have been included for the initial implementation and maintenance of the required selected NIST SP 800-172 Feb2021 security requirements. The cost estimates account for time for an OSC to implement these security requirements and prepare for, support, participate in, and closeout a Level 3 certification assessment conducted by DCMA DIBCAC. The OSC should keep in mind that the total cost of a Level 3 certification assessment includes the cost of a Level 2 certification assessment as well as the costs to implement and assess the security requirements specific to Level 3. CMMC Level 3 is expected to affect a small subset of the DIB.

Other Than Small Entities, Per Entity

- ***Nonrecurring Engineering Costs:*** **$21,100,000**[44]
- **Recurring Engineering Costs: $4,120,000**
- ***Assessment Costs and Initial Affirmation Costs:*** It is estimated that the cost to support a Level 3 certification assessment and affirmation for an other than small entity is ***$39,021.** The three-year cost is $44,445 (as summarized in 4.1.2, table 23), and includes the triennial assessment + affirmation, plus two additional annual affirmations ($39,021 + $2,712 + $2,712)
    - **Phase 1: Planning and preparing for the certification assessment: $7,066**
        - A director (MGMT5) for 12 hours ($190.52/hr x 12hrs = $2,286)
        - A manager (MGMT2) for 12 hours ($95.96/hr x 12hrs = $1,152)
        - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
        - A senior IT specialist (IT3) for 12 hours ($81.96/hr x 12hrs = $984)
        - An IT specialist (IT2) for 20 hours ($54.27/hr x 20hrs = $1,085)
    - **Phase 2: Conducting the certification assessment: $23,136**
        - A director (MGMT5) for 24 hours ($190.52/hr x 24hrs = $4,572)
        - A manager (MGMT2) for 24 hours ($95.96/hr x 24hrs = $2,303)
        - A staff IT specialist (IT4) for 64 hours ($97.49/hr x 64hrs = $6,239)
        - A senior IT specialist (IT3) for 64 hours ($81.96/hr x 64hrs = $5,245)
        - An IT specialist (IT2) for 88 hours ($54.27/hr x 88hrs = $4,776)
    - **Phase 3: Reporting of certification assessment results: $2,712**
        - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
        - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
        - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
        - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
        - **Phase 4: Closing out POA&Ms**[45] **(for CMMC Level 3 if necessary and allowed):**

        $3,394
    - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
    - A senior staff IT specialist (IT5) for 16 hours ($116.87/hr x 16hrs = $1,870)
    - **Affirmations:** initial affirmation post assessment: **$2,712**
    - **Reaffirmations:** It is estimated that the costs to reaffirm a Level 3 certification assessment annually is **$2,712** (three-year cost is $8,136, or $2,712 x 3)
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
    - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
    - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7) The Level 3 affirmations cost burden will be addressed as part of the 48 CFR part 204 CMMC Acquisition rule.
    - ***Summary:*** The following is the annual other than small entities total cost summary for Level 3 certification assessments and affirmations over a ten-year period. Example calculation, Year 2 (reference per entity amounts shown):
    - ***(**$39,021 Certification per entity x 5 entities) + ($2,712 Annual Affirmation per entity x 1 entity) = **$197,818**, and
    - **$105,500,000** Nonrecurring Engineering cost ($21,100,000 per entity x 5 entities being certified), and
    - **$24,720,000** Recurring Engineering cost ($4,120,000 per entity x 5 entities being certified) + ($4,120,000 per entity x 1 entity performing affirmations)
    - **$130,417,818** Total Cost = Certification and Affirmation Cost ($197,818) +

[44] DoD utilized subject matter expertise from Defense Pricing and Contracting (DPC) and DCMA DIBCAC to estimate the Nonrecurring and Recurring Engineering Costs.

[45] Costs for closing out POA&Ms are included at Level 3 because the requirement to implement a subset of NIST SP 800-172 Feb2021 security requirements is new with the CMMC rule. These costs are not included at Level 2 because the implementation of all NIST SP 800-171 R2 security requirements are already required.

Nonrecurring Engineering cost ($105,500,000) + Recurring Engineering cost ($24,720,000), or $145,432,897.

Table 23 - Level 3: Certification Assessment for Other Than Small Entities

Yr	Entities Performing Triennial Certification Including Initial Affirmation	Entities Performing Reaffirmation Actions Only	Triennial Certification and Affirmations Total Cost	Nonrecurring Engineering Cost	Recurring Engineering Cost	Total Cost
1	1	0	$39,021	$21,100,000	$4,120,000	$25,259,021
2	5	1	$197,818	$105,500,000	$24,720,000	$130,417,818
3	18	6	$718,654	$379,800,000	$98,880,000	$479,398,654
4	35	23	$1,428,123	$717,400,000	$238,960,000	$957,788,123
5	39	53	$1,665,578	$717,400,000	$379,040,000	$1,098,105,578
6	52	74	$2,229,811	$717,400,000	$519,120,000	$1,238,749,811
7	69	91	$2,939,280	$717,400,000	$659,200,000	$1,379,539,280
8	39	121	$1,850,016		$659,200,000	$661,050,016
9	52	108	$2,322,031		$659,200,000	$661,522,031
10	69	91	$2,939,280		$659,200,000	$662,139,280
Tot	**379**	**568**	**$16,329,613**	**$3,376,000,000**	**$3,901,640,000**	**$7,293,969,613**

Small Entities

- ***Nonrecurring Engineering Costs*: $2,700,000**
- ***Recurring Engineering Costs:* $490,000**
- ***Assessment Costs and Initial Affirmation Costs:*** It is estimated that the cost to support a Level 3 certification assessment for a small entity is ***$9,050** The three-year cost is $12,802 (summarized in 4.1.2, table 10), and includes the triennial assessment + affirmation, plus two additional annual affirmations ($9,050 + $1,876 + $1,876):
  - **Phase 1: Planning and preparing for the certification assessment: $1,905**
  - A director (MGMT5) for 10 hours ($190.52/hr x 10hrs = $1,905)
  - **Phase 2: Conducting the certification assessment: $1,524**
  - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
  - **Phase 3: Reporting of certification assessment results: $1,876**
    - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
    - A staff IT specialist (IT4-SB) for 4.08 hours ($86.24/hr x 4.08hrs = $352)
    - **Phase 4: Closing out POA&Ms[46] (for CMMC Level 3 if necessary and allowed):**

    $1,869
  - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
  - A staff IT specialist (IT4-SB) for 48 hours ($86.24/hr x 48hrs = $345)
  - **Reaffirmations**: It is estimated that the costs to reaffirm a Level 3 certification assessment annually is **$1,876** (three-year cost is $5,628, or $1,876 x 3)
  - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
  - A staff IT specialist (IT4-SB) for 4.08 hours ($86.24/hr x 4.08hrs = $352)

[46] Costs for closing out POA&Ms are included at Level 3 because the requirement to implement a subset of NIST SP 800-172 Feb2021 security requirements is new with the CMMC rule. These costs are not included at Level 2 because the implementation of all NIST SP 800-171 R2 security requirements is already required.

- The Level 3 affirmations cost burden will be addressed as part of the 48 CFR part 204 CMMC Acquisition rule.

Summary: The following is the annual small entities total cost summary for Level 3 certification assessments and affirmations over a ten-year period. Example calculation, Year 2 (reference per entity amounts shown):

- *($9,050 Certification per entity x 45 entities) + ($1,876 Annual Affirmation per entity x 3 entities) = **$412,897**, and
- $121,500,000 Nonrecurring Engineering cost ($2,700,000 per entity x 45 entities being certified), and
- $23,520,000 Recurring Engineering cost ($490,000 per entity x 45 entities being certified) + ($490,000 per entity x 3 entities performing affirmations)
- $145,432,897 Total Cost = Certification and Affirmation Cost ($412,897) + Nonrecurring Engineering cost ($121,500,000) + Recurring Engineering cost ($23,520,000), or $145,432,897.

Table 24 - Level 3: Certification Assessment for Small Entities

Yr	Entities Performing Triennial Certification Including Initial Affirmation	Entities Performing Reaffirmation Actions Only	Triennial Certification and Affirmations Total Cost	Nonrecurring Engineering Cost	Recurring Engineering Cost	Total Cost
1	3	0	$27,151	$8,100,000	$1,470,000	$9,597,151
2	45	3	$412,897	$121,500,000	$23,520,000	$145,432,897
3	151	48	$1,456,663	$407,700,000	$97,510,000	$506,666,663
4	292	196	$3,010,423	$780,300,000	$239,120,000	$1,022,430,423
5	334	443	$3,853,914	$780,300,000	$380,730,000	$1,164,883,914
6	440	626	$5,156,569	$780,300,000	$522,340,000	$1,307,796,569
7	553	774	$6,456,917	$704,700,000	$650,230,000	$1,361,386,917
8	334	993	$4,885,718		$650,230,000	$655,115,718
9	440	887	$5,646,207		$650,230,000	$655,876,207
10	553	774	$6,456,917		$650,230,000	$656,686,917
Tot	**3,145**	**4,744**	**$37,363,377**	**$3,582,900,000**	**$3,865,610,000**	**$7,485,873,377**

All Entities Summary

The following is a summary of the cost to all entities regardless of size for Level 3 certification assessments and affirmations over a ten-year period:

Table 25 - Level 3: Certification Assessment for All Entities

Yr	Entities Performing Triennial Certification	Entities Performing Reaffirmation	Triennial Certs and Affirmation Total Cost	Nonrecurring Engineering Cost	Recurring Engineering Cost	Total Cost
	Including Initial Affirmation	Actions Only				
1	4	0	$66,172	$29,200,000	$5,590,000	$34,856,172
2	50	4	$610,715	$227,000,000	$48,240,000	$275,850,715
3	169	54	$2,175,317	$787,500,000	$196,390,000	$986,065,317
4	327	219	$4,438,546	$1,497,700,000	$478,080,000	$1,980,218,546

5	373	496	$5,519,492	$1,497,700,000	$759,770,000	$2,262,989,492
6	492	700	$7,386,381	$1,497,700,000	$1,041,460,000	$2,546,546,381
7	622	865	$9,396,197	$1,422,100,000	$1,309,430,000	$2,740,926,197
8	373	1,114	$6,735,735	$-	$1,309,430,000	$1,316,165,735
9	492	995	$7,968,238	$-	$1,309,430,000	$1,317,398,238
10	622	865	$9,396,197	$-	$1,309,430,000	$1,318,826,197
Tot	**3,524**	**5,312**	**$53,692,990**	**$6,958,900,000**	**$7,767,250,000**	**$14,779,842,990**

Government Costs

Summary of Impact

The following is a summary of the estimated Government costs calculated for a 20-year horizon in 2023 dollars at a 7 percent and 3 percent discount rate. The Government costs include conducting Level 3 certification assessments, uploading results into the CMMC instantiation of eMASS, and the CMMC PMO costs.

Table 26 – Total Estimated Government Costs of CMMC Requirements for All Entities

Government Costs	7% Discount	3% Discount
Annualized Costs	$9,508,593	$9,953,205
Present Value Costs	$100,734,168	$148,078,564

Government Costs (All Levels)

The estimated Government costs utilize the entity numbers and phased roll-out detailed in the Public cost section. The DIBCAC estimated the detailed hours for all activities and other costs in a manner similar to the details shown in the Public cost section. Labor efforts for the Government are focused on Level 3. For purposes of the cost estimate, Government labor is based on the average of step one, five, and ten for GS-11 through GS-15 labor elements for the Washington D.C. area. The cost of labor was increased by a factor of approximately 51 percent which includes an estimated fringe factor (fringe factor includes estimated average insurance and pension benefits) plus overhead (overhead factor represents supervision and management of the labor) to arrive at the estimated labor rates. The Government labor in this estimate is performed by DCMA, which is a labor-intensive agency with limited overhead expenses. Therefore, the overall added factor of 51 percent is appropriate versus a typical full overhead factor of 100 percent.

CMMC Database Infrastructure Costs

The Government will develop the operational CMMC instantiation of eMASS. The cost analysis assumes that the nonrecurring engineering (NRE) cost includes the requirements development, architecture design, security, prototyping and testing, and approvals or certifications.[47] Nonrecurring engineering costs is a one-time fee of **$4,631,213** and is reflected here as incurred in the initial year of the estimate. The Year 1 amount is based on the actual cost incurred in FY2020 with adjustment for inflation to arrive at base year (BY) 1 dollars (2023). The recurring engineering (RE) cost includes database management, data analysis, cybersecurity, storage and backups, licensing, and infrastructure.[48][49]

[47] Nonrecurring engineering costs were first incurred in FY20. The cost has inflation applied to put the value in 2023 base year (BY) dollars.

[48] The cost for the recurring engineering cost is based on the costs incurred in FY20 and FY21. The values for Year [49] (FY20) and Year 2 ((FY21) are actual historic values that have inflation applied to them to put them in base year 2023 dollars. Every proceeding years' recurring engineering cost is based on the average of the two historic actual values.

The cost for recurring engineering in Year 1 **($2,336,038)** and Year 2 **($1,804,480)** are based on historical amounts incurred for FY 2020 and FY 2021 with adjustment for inflation to arrive at base year 1 and Year 2 dollars (2023 and 2024). The estimated recurring engineering for Year 3 forward is calculated as the average of the Year 1 and Year 2 amounts (($2,336,038 + $1,804,480)/2 = **$2,070,259**).

The table summarizes the nonrecurring engineering (NRE) and recurring engineering (RE) costs for Year 1 through Year 5:

Table 27 - Government Costs for CMMC Database Infrastructure (BY23$)

	NRE	RE	Sub-Total Per Year
Year 1	$4,631,213	$2,336,038.92	$6,967,252
Year 2	0	$1,804,480	$1,804,480
Year 3	0	$2,070,259	$2,070,259
Year 4	0	$2,070,259	$2,070,259
Year 5	0	$2,070,259	$2,070,259
Total	**$4,631,213**	**$10,351,296**	**$14,982,509**

Total Government Costs

The following is a summary of the total Government costs over a ten-year period:

Table 28 – Estimated CMMC Costs –Government (BY23$)

Year	Government Costs (All Levels**)	CMMC Database Infrastructure (CMMC Instantiation of eMASS)	Total
1	$79,698	$6,967,252	$7,046,950
2	$826,063	$1,804,480	$2,630,543
3	$2,871,167	$2,070,259	$4,941,426
4	$5,713,930	$2,070,259	$7,784,189
5	$6,830,268	$2,070,259	$8,900,527
6	$9,083,729	$2,070,259	$11,153,988
7	$11,533,002	$2,070,259	$13,603,261
8	$7,670,055	$2,070,259	$9,740,314
9	$9,486,082	$2,070,259	$11,556,342
10	$11,533,002	$2,070,259	$13,603,261

**Government activities associated with all Government costs associated with the CMMC Program.

Total Public and Government Costs

The following is a summary of the total estimated annual Public and Government cost associated with implementation of the CMMC Program over a ten-year period:

Table 29 - Estimated CMMC Costs – Public and Government (BY23$)

Year	Public	Government	Total
1	$95,053,432	$7,046,950	$102,100,382
2	$584,394,262	$2,630,543	$587,024,805
3	$2,031,366,143	$4,941,427	$2,036,307,570
4	$4,106,424,873	$7,784,189	$4,114,209,062
5	$4,802,803,881	$8,900,527	$4,811,704,408

6	$5,917,019,480	$11,153,988	$5,928,173,468
7	$7,004,683,879	$13,603,261	$7,018,287,140
8	$4,229,652,383	$9,740,314	$4,239,392,697
9	$4,865,166,797	$11,556,342	$4,876,723,139
10	$5,582,583,879	$13,603,261	$5,596,187,140

Alternatives

DoD considered and adopted several alternatives during the development of this rule that reduce the burden on defense contractors and still meet the objectives of the rule. These alternatives include: (1) maintaining status quo and leveraging only the current requirements implemented in DFARS provision 252.204-7019 and DFARS clause 252.204-7020 requiring defense contractors and offerors to self-assess utilizing the DoD Assessment Methodology and entering a Basic Summary Score; (2) revising CMMC to reduce the burden for small businesses and contractors who do not process, store, or transmit critical CUI by eliminating the requirement to hire a C3PAO and instead allow self-assessment with affirmation to maintain compliance at CMMC Level 1, and allowing triennial self-assessment with an annual affirmation to maintain compliance for some CMMC Level 2 programs; (3) exempting contracts and orders exclusively for the acquisition of commercially available off-the-shelf items; and (4) implementing a phased implementation for CMMC.

In addition, the Department took into consideration the timing of the requirement to achieve a specified CMMC Status: (1) at time of proposal or offer submission, (2) after contract award, (3) at the time of contract award, or (4) permitting government Program Managers to seek approval to waive inclusion of CMMC Status requirements in solicitations that involve disclosure or creation of FCI or CUI as part of the contract effort. Such waivers will be requested and approved by DoD in accordance with internal policies, procedures, and approval requirements. The Department ultimately adopted alternatives 3 and 4. The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC Status after the release of the solicitation. The drawback of alternative 2 (after contract award) is the increased risk to the Department with respect to the costs, program schedule, and uncertainty in the event the contractor is unable to achieve the required CMMC Status in a reasonable amount of time given their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI.

Benefits

The Department of Defense expects this final rule to protect DoD and industry from the loss of FCI and CUI, including intellectual property. The theft of intellectual property and FCI and CUI due to malicious cyber activity threatens U.S. economic security and national security. In 2010, the Commander of the U.S. Cyber Command and Director of the National Security Agency estimated the value of U.S. intellectual property to be $5 trillion and that $300 billion is stolen over networks annually[50]. The 2013 Intellectual Property Commission Report provided concurrence and noted that the ongoing theft represents "the greatest transfer of wealth in history." The report also highlighted the challenges of generating an exact figure because Government and private studies tend to understate the impacts due to inadequate data or scope, which is evidenced in subsequent analyses[51].

The responsibility of Federal agencies to protect FCI or CUI does not change when such information is shared with defense contractors. A comparable level of protection is needed when FCI or CUI is processed, stored, or transmitted on contractor information systems.[52] The protection of FCI, CUI, and intellectual property on defense contractor systems can directly

[50] www.govinfo.gov/content/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm

[51] www.nbr.org/program/commission-on-the-theft-of-intellectual-property/

[52] www.cybernc.us/fci-cui/

impact the ability of the Federal Government to successfully conduct its essential missions and functions[53].

Malicious cyber actors have targeted and continue to target the DIB sector that consists of approximately 220,000 small-to-large sized entities that support the warfighter. In particular, actors ranging from cyber criminals to nation-states continue to attack companies and organizations that comprise the Department's multi-tier supply chain including smaller entities at the lower tiers. From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted sensitive, unclassified information, as well as proprietary and export-controlled technology. The acquired information provides significant insight into U.S. weapons platforms development and deployment timelines, vehicle specifications, and plans for communications infrastructure and IT. By acquiring proprietary internal documents and email communications, adversaries may be able to adjust their own military plans and priorities, hasten technological development efforts, inform foreign policymakers of U.S. intentions, and target potential sources for recruitment[54].

In addition to stealing intellectual property for military gains, Russia may conduct cyberattacks against the U.S. for retaliatory purposes. On March 21, 2022, the Biden-Harris Administration stated intelligence indicates that the Russian Government and Russian-aligned cybercrime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian Government or the Russian people[55].

The aggregate loss of intellectual property and CUI from the DoD supply chain severely undercuts U.S. technical advantage, limits and disrupts business opportunities associated with technological superiority, and ultimately threatens our national defenses and economy. By incorporating heightened cybersecurity into acquisition programs, the CMMC Program provides the Department assurance that contractors and subcontractors are meeting DoD's cybersecurity requirements and provides a key mechanism to adapt to an evolving threat landscape. This is critically important to the Department because defense contractors are the target of increasingly frequent and complex cyberattacks by adversaries and non-state actors. Dynamically enhancing DIB cybersecurity to meet these evolving threats and safeguarding the information that supports and enables our warfighters is a top priority for the Department. The CMMC Program is a key component of the Department's DIB cybersecurity effort.

CMMC provides uniform and improved DoD cybersecurity requirements in three (3) levels, using the security requirements in NIST SP 800-171 R2 and a selected subset of those in NIST SP 800-172 Feb2021. With this rule, the Department is publishing supplemental guidance documents to assist the public and in particular, small businesses, with CMMC implementation, increasing the likelihood of successful implementation and strengthening cybersecurity across the DIB. CMMC decreases the burden and cost on companies protecting FCI by allowing all companies at Level 1, and a subset of companies at Level 2, to demonstrate compliance through self-assessments. CMMC allows companies, under certain limited circumstances, to make a Plan of Action & Milestones (POA&M) to provide additional time to achieve a Final CMMC Status. These key updates to CMMC benefit the DoD and our national interest by providing:

- improved safeguarding of competitive advantages through requirements flow-down to the defense contractor supply chain and protections for proprietary information and capabilities, and

[53] GAO Report to Congress, Defense Contractor Cybersecurity Stakeholder Communication and Performance Goals Could Improve Certification Framework, December 2021.

[54] www.cisa.gov/news-events/cybersecurity-advisories/aa22-047a

[55] www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-ournations-cybersecurity/

- increased efficiency in the economy and private markets as a result of the streamlining of cybersecurity requirements, the resulting improvements in cybersecurity, and accountability across the supply chain.

In summary, the CMMC Program enforces and validates implementation of DoD's required cyber protection standards for companies in the DIB, preserving U.S. technical advantage. In addition, CMMC increases security for the most sensitive CUI by applying additional requirements at Level 3. Implementation of CMMC will help protect FCI and CUI upon which DoD systems and critical infrastructure rely, making it vital to national security. CMMC is focused on securing the Department's supply chain, including the smallest, most vulnerable innovative companies. The security risks that result from the significant loss of FCI and CUI, including intellectual property and proprietary data, make implementation of the CMMC Program vital, practical, and in the public interest.

III. Regulatory Compliance Analysis

A. Executive Order 12866, "Regulatory Planning and Review" and Executive Order 13563, "Improving Regulation and Regulatory Review," as amended by Executive Order 14094, "Modernizing Regulatory Review"

These Executive Orders direct agencies to assess all costs, benefits, and available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health, safety effects, distributive impacts, and equity). These Executive Orders emphasize the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. The Office of Management and Budget (OMB) has determined this final rule is significant as defined by Section 3(f)(1) for purposes of Executive Order 12866, as amended by Executive Order 14094.

B. Congressional Review Act (5 U.S.C. 801 et seq.)

As defined by 5 U.S.C. 804(2), a major rule is a rule that the Administrator of the Office of Information and Regulatory Affairs of the Office of Management and Budget finds has resulted in or is likely to result in— (a) an annual effect on the economy of $100,000,000 or more; (b) a major increase in costs or prices for consumers, individual industries, Federal, State, or local government agencies, or geographic regions; or (c) significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and export markets. This rule has been designated a major rule as it is expected to have annual effect on the economy of $100M dollars or more.

C. Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C. 601)

The Department of Defense Chief Information Officer certified that this rule is subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would, if promulgated, have a significant economic impact on a substantial number of small entities.

DoD has considered previous comments from Small Business Administration (SBA) regarding the impact and cost to small businesses to implement CMMC. In July 2022, the CMMC PMO met with the Office of Advocacy for the U.S. SBA to address the revisions planned in CMMC that are responsive to prior SBA concerns, with which the SBA was satisfied. An Initial Regulatory Flexibility Analysis that includes a detailed discussion and explanation about the assumptions and methodology used to estimate the cost of this regulatory action on small entities follows and is available at www.regulations.gov (search for "DoD-2023-OS-0063," click "Open Docket," and view "Supporting Documents").

This final regulatory flexibility analysis has been prepared consistent with 5 U.S.C. 603.

D. FINAL REGULATORY FLEXIBILITY ANALYSIS

This final regulatory flexibility analysis has been prepared consistent with 5 U.S.C. 604(a).

Reasons for the Action

This final rule is necessary to create a secure and resilient supply chain, by addressing threats to the U.S. economy and national security from ongoing malicious cyber activities and preventing theft of hundreds of billions of dollars of U.S. intellectual property. The President's

Executive Order (EO) 14028, "Improving the Nation's Cybersecurity,"[56] emphasized that industrial security needs strengthening to ensure investments are not lost through intellectual property theft or among other supply chain risks.

Currently, the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) prescribe contract clauses intended to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the Department of Defense (DoD) supply chain. Specifically, the clause at FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, is prescribed at FAR 4.1903 for use in Government solicitations and contracts when the contractor or a subcontractor at any tier may have FCI residing in or transiting through its information system. The FAR clause focuses on ensuring a basic level of cybersecurity hygiene and is reflective of actions that a prudent businessperson would employ.

In addition, DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is prescribed in DFARS 204.7304 (c) for use in DoD solicitations and contracts that require processing, storing, or transmitting of CUI in contractor owned information systems. DFARS clause 252.204-7012 requires defense contractors and subcontractors to provide "adequate security" to process, store or transmit CUI on information systems or networks, and to report cyber incidents that affect these systems or networks. The clause states that to provide adequate security, the contractor shall implement, at a minimum, the security requirements in "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 R2, Protecting CUI in Nonfederal Systems and Organizations." Contractors are also required to flow down DFARS clause 252.204-7012 to all subcontracts that involve CUI. However, neither FAR clause 52.204-21 nor DFARS clause 252.204-7012, provide for DoD verification of a contractor's implementation of basic safeguarding requirements specified in those clauses prior to contract award. DFARS clause 252.204-7020, *NIST SP 800-171 DoD Assessment Requirements,* applies to contractor information systems that are subject to NIST SP 800-171 requirements pursuant to DFARS clause 252.204-7012. DFARS provision 252.2047019 and DFARS clause 7020 require offerors and contractors (including subcontractors) respectively to score their implementation of NIST SP 800-171 requirements for each contractor information system that is relevant to the offer or contract and to submit, at minimum, summary level self-assessment scores in the Supplier Performance Risk System (SPRS) for a minimum of a Basic Assessment, which is a contractor self-assessment. The SPRS submission includes the NIST SP 800-171 version against which the assessment was conducted, all industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the required system security plan, the date of assessment, the summary level score, and the date all NIST SP 800-171 R2 requirements are expected to be implemented based on the associated plan(s) of action in accordance with NIST SP 800-171 R2. Accordingly, and upon submission of an offer, when applicable, the contractor must verify that a summary level score(s) of a current NIST SP 800-171 DoD Assessment is posted in SPRS for all contractor information systems relevant to the offer to signify appropriate implementation of NIST SP 800-171 R2 requirements.

Findings from DoD Inspector General report (DODIG-2019-105 "Audit of Protection of DoD CUI on Contractor-Owned Networks and Systems") indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI. That report included recommendations for DoD take steps to assess a contractor's ability to protect this information. The report emphasizes that malicious actors can exploit vulnerabilities in contractors' information systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies. Due to these shortcomings and the associated risks to national security, the Department developed the Cybersecurity Maturity Model Certification (CMMC) Program to assess contractor and subcontractor implementation of DoD's required cybersecurity standards.

---

[56] www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/technology-products-services/itsecurity/executive-order-14028

The CMMC Program verifies compliance with DoD cyber protection standards by defense contractors and subcontractors and is designed to protect FCI and CUI that is shared by the Department with its contractors and subcontractors, and when developed by a contractor in the course of contract performance but not shared. The program incorporates a set of cybersecurity requirements into acquisition contracts and provides the Department increased assurance that contractors and subcontractors are meeting these requirements. The CMMC Program has three key features:

- **Tiered Model:** CMMC requires that companies demonstrate, through assessment that they have implemented cybersecurity requirements. The type of assessment and requirements against which it is conducted are selected based on the information that must be safeguarded. The program also sets forth the requirements for flow down of CMMC requirements to subcontractors.
- **Assessment Requirement:** CMMC assessments allow the Department to verify the implementation of cybersecurity requirements.
- **Implementation through Contracts:** Once CMMC is fully implemented, DoD contractors that handle FCI and CUI on their non-Federal information systems will be required to achieve a particular CMMC Status as a condition of contract award.

In September 2020, the DoD published the 48 CFR CMMC interim final rule in the *Federal Register* (DFARS Case 2019-D041) that implemented the DoD's initial vision for the CMMC Program and outlined the key features of the program. The 48 CFR CMMC interim final rule became effective on November 30, 2020.

In March 2021, the Department initiated an internal review of CMMC's implementation, informed by more than 750 public comments in response to the 48 CFR CMMC interim final rule. This comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

In November 2021, the Department announced an updated program structure with revised requirements designed to achieve the primary goals identified by DoD's internal review of the CMMC Program. With the implementation of the revised CMMC program, the Department introduced several key changes that build on and refine the original program requirements. These include:

- Streamlining the CMMC model from five levels to three levels.
- Exclusively implementing National Institute of Standards and Technology (NIST) cybersecurity guidelines.
- Allowing all companies subject to CMMC Level 1 requirements and subset of companies subject to CMMC Level 2 requirements to demonstrate CMMC compliance through self-assessments.
- Increased oversight of professional and ethical standards of third-party assessors.
- Allowing Plans of Action & Milestones (POA&M) under limited circumstances to achieve conditional certification.

In July 2022, the CMMC Program Management Office (PMO) met with the Office of Advocacy for the U.S. SBA to address the revisions planned for CMMC and again met in July 2023 to review the proposed 32 CFR part 170 CMMC Program rule updates that are responsive to prior SBA concerns. As a result of the alignment of CMMC requirements to NIST guidelines, the Department's requirements continue to evolve as changes are made to the underlying NIST SP 800-171 R2 and NIST SP 800-172 Feb2021 requirements. Such changes will not be effective as CMMC requirements unless and until made effective through rulemaking.

Objectives of, and Legal Basis for, the Rule

Legal Basis: 5 U.S.C. 301; Sec. 1648, Pub. L. 116-92, 133 Stat. 1198.

The objective of this final CMMC Program rule is to provide the Department with increased assurance that a defense contractor can adequately protect FCI and CUI commensurate with the risk, also accounting for information flow down to its subcontractors in a multi-tier supply chain. This rule meets the objective by providing a mechanism to assess contractor and subcontractor implementation of DoD's cyber security protection requirements for FCI and CUI.

Implementation of the CMMC Program is intended to address the following policy issues:

(a) ***Verification of a contractor's cybersecurity posture***

Effective June 2016, FAR clause 52.204-21 Basic Safeguarding of Contractor Information Systems, requires Federal contractors and subcontractors to implement 15 basic safeguarding requirements, as applicable, to protect contractor information systems that process, store, or transmit FCI.

December 31, 2017, was the DoD deadline for contractors to implement, as applicable, the cybersecurity protection requirements set forth in NIST SP 800-171 Re2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, in accordance with requirements of DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. NIST SP 800-171A Jun2018 states, "For the CUI security requirements in NIST Special Publication 800-171 Rev 2, nonfederal organizations describe in a system security plan, how the specified requirements are met or how organizations plan to meet the requirements.[57]" The NIST process provides contractors with a tool to assess their security posture and decide if or when to mitigate the risks based upon the organizational risk tolerance. When the DoD implemented the NIST SP 800-171 requirements with a not-later-than date of December 2017, the policy intent was to permit contractors some flexibility to remediate lagging NIST requirements, and document them in plans of action, and resolve those deficiencies within a reasonable period. An unintended consequence of this flexibility was that some contractors far exceeded the intention to secure systems that must adequately safeguard CUI in a timely manner and instead created open-ended plans of action with undefined closure dates. The effect was to delay full compliance with safeguarding requirements for years. As a result, the DoD's implementation of the NIST SP 800-171 requirements, as mandated by 32 CFR part 2002, has not been fully effective or validated. This necessitates implementation of the CMMC Program to enforce a finite timeline for full compliance of contractual requirements.

Findings from DoD Inspector General report (DODIG-2019-105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicated that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information.

CMMC adds an assessment requirement to verify defense contractors and subcontractors have implemented the applicable security requirements prior to award. CMMC also adds requirements at each CMMC level for contractors and subcontractors to affirm initial compliance with the specified CMMC security requirements and provide annual affirmations thereafter.

(b) ***Comprehensive implementation of cybersecurity requirements***

Although the security requirements in NIST SP 800-171 R2 address a range of threats, they do not sufficiently address Advanced Persistent Threats (APTs). An APT is an adversary that possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). To address APTs, NIST has published NIST SP 800-172 Feb2022. CMMC Level 3 certification assessment provides for government assessment of a contractor's implementation of a defined subset of NIST SP 800-172 Feb2021 Enhanced Security Requirements with DoD predefined parameters and specifications.

(c) ***Scale and Depth***

Today, DoD prime contractors must include DFARS clause 252.204-7012 in subcontracts for which performance will involve covered defense information, but this does not provide the Department with sufficient insights with respect to the cybersecurity posture of all members of a multi-tier supply chain for any given program or technology development effort. The revised CMMC Program requires prime contractors to flow down CMMC requirements, as applicable, to subcontractors throughout their supply chain(s).

---

[57] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf

Given the size of the Defense Industrial Base (DIB), the Department cannot scale its existing cybersecurity assessment workforce to conduct on-site assessments of approximately 220,000 DoD contractors and subcontractors every three years. The Department's existing assessment capability is best suited for conducting targeted assessments for the relatively small subset of DoD contractors and subcontractors that support designated high-priority programs.

CMMC addresses the Department's scaling challenges by utilizing a private-sector accreditation structure. The DoD-recognized Accreditation Body will authorize, accredit, and provide oversight of CMMC Third-Party Assessment Organizations (C3PAO) which in turn will conduct CMMC Level 2 certification assessments of actual and prospective DoD contractors and subcontractors. Organizations Seeking Certification (OSCs) will directly contract with an authorized or accredited C3PAO to undergo a Level 2 certification assessment to achieve a CMMC Status of Conditional and Final Level 2 (C3PAO). The cost of CMMC Level 2 activities is driven by multiple factors, including market forces that govern availability of C3PAOs and the size and complexity of the enterprise or enclave under assessment. The Government will perform Level 3 certification assessments. Government resource limitations may affect schedule availability.

(d) ***Reduces Duplicate or Repetitive Assessments of our Industry Partners****:*

CMMC assessment results and contractor affirmations of compliance will be posted in Supplier Performance Risk System (SPRS), DoD's authoritative source for supplier and product performance information. Posting CMMC assessment results in SPRS precludes the need to validate CMMC implementation on a contract-by-contract basis. This enables DoD to identify whether the CMMC assessment requirements have been met for relevant contractor information system(s), avoids duplicative assessments, and eliminates the need for program level assessments, all of which results in decreased costs to both DoD and industry.

Significant Issues Raised by Public Comments

The CMMC proposed rule was published in the *Federal Register* on December 26, 2023, to initiate the mandatory 60-day public review and comment period for this rule and the supporting documents that ended on 26 February 2024. From the volume of comments received on the CMMC rule documents, from or concerning Small Businesses, the following significant issues were raised.

1. Cost. Some comments identified that the proposed rule does not address how the CMMC Program will be funded, or how the costs of certification and compliance will be shared between the DoD and the contractors. This may raise questions about the affordability and sustainability of the CMMC program, especially for small businesses. Commenters suggested that the DoD conduct and publish a comprehensive cost assessment for each level of CMMC certification and explore ways to reduce the financial burden on the contractors, such as providing incentives, subsidies, loans, grants, tax credits or reimbursements. Several comments presented the opinion that the cost estimates in the preamble/rule did not adequately address all possible costs to become compliant with regulations and attain a certification i.e., ongoing Recurring Engineering and Non-Recurring Engineering costs. Others commented that the mandate to comply with requirements, attain verification of compliance, and the inability to recoup costs prior to completing compliance will be barriers to entry and will drive many small businesses out of the DoD market. Concern was also expressed regarding the cost of failing an assessment and not being able to recoup costs fast enough, through increased Overhead and G&A [General and Administrative] rates. Another concern was raised that IR&D [Independent Research and Development] spending will be negatively impacted due to the diversion of funds to Cybersecurity compliance. Some shared concerns about the potential for overmarking CUI data, that will drive a higher than necessary demand for CMMC certification and create an overburdened Ecosystem, thereby preventing timely certification and incentivizing "price gouging" by assessors. Several suggested that the Government regulate the prices for assessment services. Many commenters also suggested the DoD needed to find ways to reduce the financial burdens on small businesses through direct payment for compliance, tax incentives, increased profits, or increased flexibility to comply with requirements, i.e., by reducing requirements for

small businesses or providing more time to comply after contract award. Commenters also felt the handling of CUI by small businesses was too difficult, and recommended prime contractors should be responsible for handling all CUI. If a small business needs CUI to execute its work, the prime or the Government should provide an environment for the small business to complete its work.

DoD Response. In recognition of the pervasive cyber threat both to DoD and to the DIB, CMMC Program requirements are designed to ensure compliance with existing standards for protection of FCI and CUI. These cybersecurity requirements align directly to NIST guidelines (NIST SP 800-171 R2 and NIST SP 800-172 Feb2021) and the basic safeguarding requirements in FAR clause 52.204-21 that apply to all executive agencies. Since December 2017, DFARS clause 252.204-7012 has required contractors to implement the NIST SP 800-171 security requirements to provide *adequate security* as applicable for processing, storing, or transmitting CUI on non-Federal information systems, as needed in support of the performance of a DoD contract.

The executive branch's CUI Program is codified in 32 CFR part 2002 and establishes policy for designating, handling, and decontrolling information that qualifies as CUI. The definition of CUI and general requirements for its safeguarding are included in 32 CFR 2002.4 and 2002.14. 32 CFR 2002.14(h)(2) specifically requires that Agencies must use NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems..." Contractually, DFARS clause 252.204-7012 requires contractors to implement the NIST SP 800-171 R2 security requirements, and that requirement applies, regardless of the number of computers or components in a non-Federal information system or the size of the contractor or subcontractor, as applicable. DoD's original implementation of security requirements for adequate safeguarding of CUI relied upon self-attestation by contractors. Since that time, the DoD Inspector General and the DCMA found contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended DoD take steps to assess a contractor's ability to protect this information. The DoD has streamlined requirements to reduce the burden of compliance on contractors. Analysis of costs to meet CMMC requirements is provided in the regulatory impact analysis for this rule. As described in the estimate included with the rule, the major cost categories for compliance with CMMC requirements include costs for completing a self-assessment (e.g., Level 1 or 2); costs to prepare for and undergo Level 2 certification assessment; and costs required to implement the Level 3 security requirements and for preparing to undergo DCMA DIBCAC assessment (Level 3). CMMC Level 3 certification assessments against the NIST SP 800-172 Feb2021 baseline are performed free of cost by DoD assessors, which reduces the overall cost of achieving CMMC Status of Level 3 (DIBCAC). Notably, certification is never required for CMMC Level 1, and the requirement can be satisfied through self-assessment. When CMMC Level 2 requirements apply, they may be met via self-assessment, or a certification assessment conducted by a C3PAO, depending on the specific CMMC requirement cited in the solicitation or resulting contract. When the CMMC Program requirements are effective, solicitations for DoD contracts that will involve the processing, storing, or transmitting of FCI or CUI on any non-Federal system, notwithstanding the size or configuration of the non-Federal system, will specify the required CMMC Level (1, 2 or 3) and assessment type (self-assessment or certification assessment). An assumption for the cost estimates is that Non-Small Entities have a full-time team of cybersecurity professionals on staff while Small Entities do not. The assumptions, explained in the regulatory impact analysis, reflect Small Entities will likely obtain support from External Service Providers and have a staff member submit affirmations and SPRS scores for self-assessments. All these costs, except the open market cost of a C3PAO, are directly controllable by the organization seeking assessment. The CMMC rule does not make any change to cost allowability as defined in FAR 31.201-2 Determining Allowability. The DoD declined to modify the estimates, which are intended to be representative and to inform rulemaking. The cost estimates represent average derived estimates based on internal expertise and public feedback in accordance with OMB Circular A-4 and represent average costs for companies to comply with

the CMMC requirements. This rule does not provide the cost analysis for all actions, personnel, and security measures required to protect CUI information, data, systems, and technical products through the life cycle of the work and data generated. The size and complexity of the network within scope of the assessment impacts the costs as well. As required by rulemaking guidance, the DoD provided cost estimates and impact analyses. An analysis of profit margins is not required. Additionally, this rule and the required cost analysis and resulting cost estimates were reviewed by DoD cost analysts and OMB economists for realism and completeness.

Some public comments received reflect a misinterpretation of the cost estimates that accompany this rule, which are representative of average assessment efforts, and do not include actual prices of C3PAO services available in the marketplace. Market forces of supply and demand will determine C3PAO pricing for CMMC Level 2 certification assessments.

Costs associated with meeting the requirements of existing DFARS clause 252.204-7012 are not captured in the CMMC rule documentation. Please refer to 81 FR 72990, October 21, 2016, for DoD's final rule implementing the DoD's requirement that "contractors shall implement NIST SP 800-171 as soon as practical, but not later than December 31, 2017." Public comments related to implementation costs were published with that final rule, along with DoD's responses. Within the limitations of section § 170.21 Plan of Action and Milestones Requirements, offerors may bid on contract opportunities while continuing to work towards full compliance.

Verifying compliance with applicable security requirements may increase costs and is necessary for the adequate protection of DoD FCI and CUI. The cost of lost technological advantage over potential adversaries is far greater than the costs of such enforcement. The value of information and impact of its loss does not diminish when the information is shared with contractors.

At the time of contract award, the DoD may not have visibility into whether the prime contractor's decision to further disseminate DoD FCI and CUI. However, FAR clause 52-20421, DFARS clause 252.204-7012, and DFARS clause 252.204-7021 require the prime contractor to flow down these clauses and the included information security requirement to any subcontractor that will process, store, or transmit FCI or CUI, as applicable. Decisions regarding DoD's information that must be shared to support completion of the contract tasks, including those performed by subcontractors, takes place between the prime contractor and their subcontractors. The DoD cannot dictate business practices between prime contractors and their subcontractors, who should work together to determine the necessary flow down of FCI and CUI, only as needed in performance of the contract, and ensuring compliance with the CMMC security requirements and in consideration of minimizing the burden. While DoD understands the burden on small business, it must enforce CMMC requirements uniformly across the Defense Industrial Base for all contractors who process, store, or transmit FCI and CUI. The requirements necessary to protect a single document are the same as to protect many documents.

Although CMMC compliance may add to an organization's cost, no member of the DIB can assume the status-quo in today's ever-changing cybersecurity environment. Increasing costs to protect the nation's data and industries from emerging threats is simply a component of doing business anywhere in the world. Processing, storing, or transmitting sensitive Government information comes with a handling cost that needs to be built into each organization's business model. All contractors or sub-contractors with access to CUI need to be capable of protecting that information to the standards specified in 32 CFR part 2002. If a small business cannot comply with the requirements of DFARS clause 252.204-7012 and NIST SP 800-171 R2, then that business should not receive CUI or process, store, or transmit CUI. If the DoD information flowed by the prime to a subcontractor is only FCI, then only a CMMC Level 1 self-assessment is required for the subcontractor prior to the flow of information under contract. DoD's programs, technological superiority, and best interests are not served if FCI and CUI are not consistently and adequately safeguarded by all who process, store, or transmit it.

2. Cost Benefit. Some commenters suggested it would be more cost effective for DoD to provide an environment or a DoD managed portal for the handling of CUI. A significant concern

expressed was that companies have delayed complying with DoD cybersecurity standards until the CMMC rule was released and they could understand what level of compliance they will require. Several commenters felt DoD underestimated the costs and should have include the implementation cost of the requirements in this rule as well. One commenter was confused about how the discount rates were applied. Another commenter suggested that DoD provide flexibility to allow small businesses to not meet all the requirements and still be allowed to handle CUI and another expressed concerns regarding the cost of compliance and the degradation of the DIB that will be unable to afford compliance.

DoD Response: The DoD declined to adopt the alternatives suggested in the comments, such as policy-based solutions that lack a rigorous assessment component or sharing CUI only through DoD-hosted secure platforms. The current DFARS clause 252.204-7012 requires protection of Security Protection Assets (SPA) and Security Protection Data (SPD). Section 1.1 of NIST SP 800-171 R2 states: "The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components." There is therefore no increase in the scope because of the CMMC Program as described in the rule.

SPD requires protection commensurate with the CUI it protects and is based on how and where the SPD is stored. The FedRAMP requirements for handling SPD are therefore the same as that for handling CUI.

The CMMC rule made no change to the FAR cost allowability or cost accounting standards. The 7% discount rate is not a discount for organizations; it is a part of a formula used in the regulatory impact analysis (RIA) calculations. When calculating 20 years in the future, a discount rate is used to determine the net present value of money. The cost estimate represents derived estimates based on internal expertise and public feedback in accordance with OMB Circular A-4: Regulatory Impact Analysis: A Primer. Step 7 in the manual explains discount rates.

As written, this rule amply provides for the flexibility sought by the commenter. Rule section § 170.21 specifically addresses the flexibility to have a Plan of Action and Milestones (POA&M) to delay meeting certain requirements subject to CMMC assessment for up to 180 days.

In addition, DFARS clause 252.204-7012 already permits contractors to request DoD CIO permission to utilize alternative security measures to those prescribed by NIST SP 800-171. If an OSC previously received a favorable adjudication from the DoD CIO for an alternative security measure, the DoD CIO adjudication must be included in the system security plan to receive consideration during an assessment. Implemented security measures adjudicated by the DoD CIO as equally effective are assessed as MET if there have been no changes in the environment.

3. CMMC Model. Some commenters claimed that the requirement for all subcontractors of Level 3 prime contractors to be at least Level 2 certified, regardless of what work they do, will generate more demand for Level 2 assessments than the Department is anticipating. Since much of DoD's contract dollars flow through a relatively small number of companies, it is likely those companies will have at least one CMMC Level 3 project. The result would be Level 2 certification requirements being flowed down to nearly the entirety of the DIB. Some commenters believed this to be an unintended consequence of implementing the enhanced protection of CMMC Level 3.

DoD Response: It is possible the commenters misunderstood § 170.23 Application to subcontractors in the rule. § 170.23(a)(4) states: "If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contractor has a requirement for the CMMC Status of Level 3 (DIBCAC), then the CMMC Status of Level 2

(C3PAO) is the minimum requirement for the subcontractor." The commenter's phrase "regardless of what work they do" does not acknowledge the fact that the Level 2 certification assessment is required for subcontractors who process, store, or transmit CUI.

It is also possible that the commenter interpreted that a Level 2 self-assessment is adequate for subcontractors working with a prime that has a contractual requirement for a Level 3 certification assessment. In this case, a CMMC Status of Final Level 2 (Self) is not adequate. A CMMC Status of Final Level 3 (DIBCAC) signifies that the prime first achieved a CMMC Status of Final Level 2 (C3PAO) as the risk to their CUI was deemed high enough to require Level 2 certification assessment. Since this same information may be shared with subcontractors who process, store, or transmit CUI, the subcontractor must also achieve CMMC Status of Final Level 2 (C3PAO).

The decision to rely upon a CMMC Level 2 self-assessment in lieu of a certification assessment is a Government risk-based decision based upon the nature of the effort to be performed and CUI to be shared. The size of the company with access to the CUI is not a basis for this determination. The value of information and impact of its loss does not diminish when the information moves to contractors of smaller size.

4. Assessment. Commenters questioned whether CMMC will accept reciprocity with other compliance methodologies. Another questioned what would drive a company to seek a reassessment of their environment. Other commenters suggested that we allow small businesses 365 days to close their POA&M requirements, as well as suggesting that pre-assessment materials do not need to be uploaded into eMASS, and that the hashing requirements should be simplified. Other suggestions made were to allow Program Managers to relax requirements based on a risk decision and allow assessors to make judgement calls on what evidence constitutes compliance with the requirement. One commenter requested the DoD publish an overview of the assessment methodology that includes the defined frequency guidelines. Additionally, one commenter requested that access to Procurement Integrated Enterprise Environment (PIEE)and Supplier Performance Risk System (SPRS) be made easier for small contractors.

DoD Response: CMMC requirements apply to DoD contracts, and not to contracts issued by other agencies. Flow down of CMMC requirements from a prime contractor to its subcontractors shall apply, as addressed in § 170.23(a) of this rule.

DoD intends to allow qualified standards acceptance of a DIBCAC High Assessment using NIST SP 800–171 R2 for CMMC Status of Final Level 2 (C3PAO) as addressed in § 170.20.

CMMC Level 2 self-assessment, Level 2 certification assessment, and Level 3 certification assessment are valid for a defined CMMC Assessment Scope as outlined in § 170.19 CMMC Scoping. A new CMMC assessment may be required if significant architectural or boundary changes are made to the previous Assessment Scope. Examples include, but are not limited to, expansions of networks or mergers and acquisitions. Operational changes within an Assessment Scope, such as adding or subtracting resources within the existing assessment boundary that follow the existing SSP do not require a new assessment, but rather are covered by the annual affirmations to the continuing compliance with requirements.

The DoD did not accept the recommendation to change the criteria for POA&Ms or the timeline allowed to remediate open POA&M items. The 180-day timeline and the determination of the weighted practices that may be included in a POA&M were risk-based decisions. The determination factored the relative risk DoD is willing to accept when a particular practice is Not Met and the amount of risk the DoD is willing to accept for those security practices that remain "NOT MET" for an extended period. Unlike the original CMMC Program, the revised CMMC Program accepts some risk with the use of limited POA&Ms.

There is value to the DoD in having the pre-assessment information in CMMC eMASS for overall program management and oversight. The information indicates that an assessment is either scheduled or in-process. The CMMC PMO seeks to track CMMC Program adoption, and the pre-assessment information allows reporting on upcoming assessments. Based on the DoD's cost analysis, the cost to upload pre-assessment material is minimal. The rule and Hashing Guide have been updated to add clarity that only reporting a single hash is required, and the name of the hash algorithm used needs to be stored in CMMC eMASS. Each Assessment

Objective in NIST SP 800-171A Jun2018 must yield a finding of MET or NOT APPLICABLE for the overall security requirement to be scored as MET. Assessors exercise judgment in determining when sufficient and adequate evidence has been presented to make an assessment finding. This is consistent with current DIBCAC High Assessments and assessments conducted under the Joint Surveillance Voluntary Assessment (JSVA) program.

A security requirement can be applicable, even with assessment objectives that are N/A. The security requirement is NOT MET when one or more applicable assessment objectives is NOT MET. The requirements of each Level of the CMMC Model are defined in sections §§ 170.15 through 170.18 and the scoring of assessments is described in § 170.24. The assessment frequency required is every year for a CMMC Status of Final Level 1 (Self), and every 3 years for a CMMC Statuses of Final Level 2 (Self), Final Level 2 (C3PAO), and Final Level 3 (DIBCAC), or when changes within the CMMC Assessment Scope invalidate the assessment.

The phased implementation plan for CMMC described in § 170.3(e) is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements. The rule has been updated to add an additional six months to the Phase 1 timeline. Phase 2 will start one calendar year after the start of Phase 1.

5. Scoping. Commenters expressed concerns about how External Service Providers (ESP) and SPA and SPD are handled with regard to certification. Another commenter expressed concern about the lack of FedRAMP Moderate certified capabilities in the market as well as requesting clarification on the definition of "Specialized Assets", specifically regarding equipment in manufacturing that may not fall under the conventional categories of IoT, IIoT, and OT. Another commenter expressed concerns about how Contractor Risk Managed Assets (CRMA) are handled, along with concerns about available FedRAMP certified capabilities. Other comments identified concerns with the responsibility of a company that adopts an ESP and their adherence to security requirements, and the lack of time given in Phase 2 of the CMMC roll-out to garner certification. A question was also asked regarding the Department's assumptions on the rigor a Certifying Officer [Affirming Official in the rule] would require before signing an attestation and the methodology used to determine the resultant actions that must be taken. Another raised a concern regarding how sub-environments are handled as well as end-to-end encryption in handling CUI. Another expressed concern regarding the marking of data as CUI and the potential for overmarking. Some commenters made suggestions that all CUI be held in a special appendix for contracts and only be allowed to be accessed at the prime's facility or through a government hosted secure portal. A commenter also suggested that small businesses should not be made to meet the CMMC Level 3 requirements. Another commenter raised questions about the alternatives that the Department considered in developing the CMMC Program. Another suggestion was to provide uniform web-based training on cybersecurity and that the definition of CUI was unclear, and CUI should stay under the control of the Federal Government and be maintained in a government owned secure portal. A suggestion was also made that DoD establish a Cyber Protection Program that monitors DIB companies and provides real time health reports on the DIB and dynamic intelligence security alerts and recommended actions. A suggestion that NIST establish a special standard for micro-organizations was also provided. Commenters also suggested that the rule was too stringent, and CUI was not marked well or flowed down to subcontractors appropriately.

DoD Response: The Department is committed to overseeing the CMMC Program and will take appropriate measures to ensure its efficient execution. Presently, the Department has no intention of mandating that contracting offices adopt presumptive measures that would reduce the number of small contracts subject to Level 2 certification assessment, nor does it plan to impose affirmative requirements on prime contracts to utilize enclaves.

Prior to conduct of an assessment, the OSC engages with the C3PAO assessor. It is during this time that classification of assets should be established, and the results of these discussions documented in pre-planning materials. This is an example of the pre-assessment and planning material submitted by the C3PAO as required in § 170.9(b)(8) and the CMMC Assessment Scope

submitted to eMASS as required in § 170.17(a)(1)(i)(D). The DoD considered the NIST definitions for System Information and Security Relevant Information in the development of the CMMC definition for SPD. This rule does not regulate an OSA's SPD, but instead implements existing regulatory requirements for the safeguarding of CUI, as defined in 32 CFR 2002.14(h)(2) and implemented by DFARS clause 252.204-7012. The DFARS clause 252.204-7012 requires protection of security protection assets and security protection data through its specification of NIST SP 800-171. Section 1.1 of NIST SP 800-171 R2 states: "The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components." There is therefore no increase in the scope as described in the rule, and no revisions to cost estimates are required.

The DoD received numerous comments about the requirements for CMMC when an ESP is used. In response to these comments, the DoD revised the rule to reduce the assessment burden on External Service Providers (ESPs) by updating the ESP assessment, certification, and authorization requirements in §§ 170.19(c)(2) and (d)(2).

The use of an ESP, its relationship to the OSA, and the services provided need to be documented in the OSA's System Security Plan and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSA and ESP with respect to the services provided.

An ESP is considered a Cloud Service Provider (CSP) when it provides its own cloud services based on a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction on the part of the OSA. ESPs that are CSPs, and process, store, or transmit CUI, must meet the FedRAMP requirements in DFARS clause 252.204-7012. ESPs that are CSPs and do *not* process, store, or transmit CUI, are not required to meet FedRAMP requirements in DFARS clause 252.204-7012.

An ESP that is not an CSP and processes, stores, or transmits CUI, is considered an extension of the OSA's environment and the ESP services used to meet OSA requirements are within the scope of the OSA's CMMC assessment. As part of that environment, the ESP will be assessed against all applicable requirements and accountable for all users who have access to CUI as part of the ESP's service, not just OSA employees. ESPs that are not CSPs and do NOT process, store, or transmit CUI, do not require CMMC assessment.

Nothing in the rule precludes an ESP, that is not a CSP, from voluntarily requesting a C3PAO assessment, and a C3PAO from performing such an assessment, if the ESP makes that business decision. Similarly, the ESP can request a Level 3 certification assessment from the DCMA DIBCAC if they have successfully met all the requirements during a Level 2 certification assessment.

ESPs can be part of the same corporate/organizational structure but still be external to the OSA such as a centralized SOC or NOC which supports multiple business units. An ESP that is used as staff augmentation and the OSA provides all processes, technology, and facilities does not need a CMMC assessment.

An ESP (not a CSP) that provides technical support services to its clients would be considered an MSP, since it does not host its own cloud platform offering. An ESP may utilize cloud offerings to deliver services to clients without being a CSP. An ESP that manages a thirdparty cloud service on behalf of an OSA would not be considered a CSP.

6. POA&M. Commenters expressed concern regarding the limited nature of POA&Ms in
CMMC as well as the timeline and lack of flexibility in remediating the POA&Ms.

DoD Response. The DoD did not accept the recommendation to change the criteria in § 170.21 for POA&M requirements or the timeline allowed to remediate open POA&M items. The 180-day timeline and the determination of which weighted practices can be placed on a POA&M were risk-based decisions. The determination factored into account for the relative risk DoD is willing to accept when a particular practice is not met and the amount of risk the DoD is willing to accept for those security practices that remain "NOT MET" for the extended period of time.

The phased implementation plan in § 170.3(e) is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements. DoD has updated the rule to add an additional six months to the Phase 1 timeline, now one year. Phase 2 will start one calendar year after the start of Phase 1.

7. Incorporation by Reference. Commenters expressed concern about the confusion between the NIST 800-171 R2 being included in the CMMC rule and not the recently published Rev 3.

DoD Response. The Office of the Federal Register regulations (1 CFR part 51) require the specification of a revision to a standard. Specifying a revision benefits the CMMC Ecosystem by ensuring it moves forward from one NIST standard to the next in an organized manner. The DoD cites NIST SP 800-171 R2 in this final rule for a variety of reasons, including the time needed for industry preparation to implement and time needed to prepare the CMMC Ecosystem to perform assessments against subsequent revisions. DoD is unable to incorporate suggestions that CMMC assessments be aligned to whichever NIST revision is current at the time of solicitation. Comments on the specifics on NIST SP 800-171 Revision 3 should be directed to NIST.

8. Affirmation. Commenters expressed confusion regarding the definition of the Affirming Official as well as how the affirmation process works i.e., is the affirmation for each company or the whole supply chain. One commenter also expressed confusion regarding whether an affirmation was required at each certification level annually.

DoD Response. The rule was modified to include a definition for *Affirming Official* in § 170.4.

The DoD considered the recommended text revisions and modified the text for added clarity about affirmations. DoD's use of the term OSA within the affirmations section is deliberate and conveys that each organization is responsible for affirmations pertaining to their own assessments. To help clarify the point in question, § 170.22(a)(1) addresses Affirming Official and has been revised to clarify that CMMC affirmations shall be submitted by the OSA and apply only to the information systems of that organization.

The DoD deems that the requirement to annually affirm continuing compliance with the CMMC requirements at the designated CMMC Level and following the procedures in § 170.22 is not a significant additional burden. The requirement for annual affirmations takes the place of an annual recertification and ensures the Affirming Official responsible for CMMC requirements is monitoring compliance.

9. Alternatives. Several commenters provided suggestions for alternative means to implement verification of compliance with cybersecurity standards. These suggestions included the following:

- Provide flexibility for the CMMC AB to allow a C3PAO partial assessment of perspective Managed Service Providers.
- Allow small businesses to continue performing self-assessments and self-certify along with increasing the support provided to small business from DC3 to expand paying for consultants to assist with compliance as well as paying for small businesses assessments,
- Integrate cybersecurity and traditional counterintelligence measures, establishing a secure software development environment in a cloud that DoD hosts, as well as providing a secure environment in which small businesses could operate.
- Require Prime contractors to assume the cost of CMMC for their supply chain.
- Only assess a sampling of the Defense Industrial Base.
- Increase the Certification validity time period from 3 to 10 years.
- Shift the requirement to post award.
- Re-evaluate the program to reduce requirements to make it easier.
- Stay with only the DCMA DIBCAC performing assessments on the DIB.

DoD Response: DoD considered many alternatives before deciding upon the current CMMC structure. To date, alternative methods of assessment have proven inadequate and necessitated the establishment of CMMC. The DoD determined the requirements for a CMMC Accreditation Body, and this accreditation body will administer the CMMC Ecosystem.

DoD must enforce CMMC requirements uniformly across the DIB for all contractors and subcontractors who process, store, or transmit CUI. The value of information and the impact of its loss does not diminish when the information moves to contractors and subcontractors.

The DoD notes with interest the commenter's reference to initiatives in a report to Congress describing the breadth of cybersecurity related initiatives within the Department. While the CMMC Program is an important initiative, it is by no means the Department's only effort to improve DIB cybersecurity. The CMMC Program addresses the adequate safeguarding of contractor owned information systems which process, store, or transmit FCI or CUI. Other DoD initiatives related to secure cloud or software development environments are beyond the scope of the CMMC Program.

The DoD declined to accept the recommended alternative of relying exclusively on selfassessment with the potential to require a DIBCAC assessment for only a sampling of DoD contractors, which is essentially the status quo. Both GAO reporting and other DoD analysis have shown that the DIB has not consistently implemented the NIST SP 800-171 requirements needed to comply with DFARS clause 252.204-7012, notwithstanding DoD's stated objective in this clause is for compliance "as soon as practical, but not later than December 31, 2017."

The DoD declined to accept the risk associated with implementing CMMC as a postaward requirement. When contracts require contractors to process, store, or transmit CUI, DoD requires that they be compliant with DFARS clause 252.204-7012 and competent to adequately safeguard CUI from the beginning of the period of performance.

DoD declined the recommendation to require primes to assume the cost of CMMC compliance for their subcontractors.

The aggregated SPRS reporting and scoring is CUI. The DoD does not plan to make this information public at this time, as it may aid adversaries in coordinating their attacks.

The Department declined to adopt the recommendation to allow DIB members to assist in designing the DoD's mechanism for assessing DIB compliance with DoD's contractual requirements. In developing the CMMC program, the DoD sought and considered DIB input.

DoD disagreed with the comment that there is a lack of scalability in the CMMC Program. The phased implementation plan described in § 170.3(e) is intended to address rampup issues within the CMMC Ecosystem, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements.

The rule was updated to add an additional six months to the Phase 1 timeline, now one year. Further extension of the implementation period or other solutions may be considered in the future to mitigate any C3PAO capacity issues, but the Department has no such plans at this time.

As with all DoD programs, the Department intends to effectively oversee the CMMC Program and take the actions needed to manage its effective implementation. Although the full extent of DoD's oversight process is beyond the scope of this rule, the rule text does address DoD's authority to waive the application of CMMC requirements when warranted.

The DoD disagrees with commenters' assertions about NIST SP 800-171 R2 and the available assessment methods. The NIST SP 800-171 R2 standard was chosen since it is enterprise focused and already required in DoD contracts when DFARS clause 252.204-7012 is applicable.

DCMA DIBCAC currently performs assessments against NIST SP 800-171 R2, which identifies the target audience to include individuals with security assessment responsibilities, such as auditors, assessors, and "independent verifiers."

The Department does not have the organic capacity to adequately assess the 220,000+ companies in the DIB. The DoD will not assume the workload of directly assessing every DIB contractor.

In this final rule, DoD established a scalable way to verify, through assessment, that contractors have implemented required security measures necessary to safeguard DoD's information.

It is important that contractors maintain security compliance for systems that process, store, or transmit DoD CUI. Given the evolving cybersecurity threat, DoD's best interests are served by ensuring that Level 2 self-assessment and certification assessments remain valid for no longer than a 3-year period, regardless of who performs the assessment.

10. Applicability. Commenters expressed frustration with exempting Commercial-OffThe-Shelf (COTS) products and procurements under the micro-purchase threshold from CMMC certification, and not providing exemptions for Native American, small, disadvantaged businesses, and Small Business Innovative Research contracts. They also expressed concerns about perceived threatened penalties and lack of recognition of recurring costs to Level 1 assessments. A commenter also recommended reversing the phased approach to require Level 3 requirements be implemented first.

DoD Response: Some comments pertain to the 48 CFR part 204 CMMC Acquisition rule, including applicability of the CMMC clause to COTS procurements and those below the micro-purchase threshold. Such comments are not within the scope of this 32 CFR part 170 CMMC Program rule, which outlines program requirements rather than contracting procedures.

This rule has no disproportionate impact on Native American owned businesses. Once identified as a requirement, the CMMC Program requirements will apply uniformly to all prospective contractors.

DoD must enforce safeguarding requirements uniformly across the DIB for all contractors and subcontractors who process, store, or transmit CUI. The value of information and impact of its loss does not diminish when the information moves to DoD contractors and DoD subcontractors, regardless of their status as Native American or small disadvantaged businesses.

The purpose of the CMMC Program is to ensure that DoD contracts that require contractors to safeguard FCI and CUI (i.e., contracts that include FAR clause 52.204-21 and DFARS clause 252.204-7012) will be awarded to contractors with the ability to protect that information appropriately. Accordingly, all contractor owned information systems that process, store, or transmit FCI or CUI in the performance of a contract are subject to the requirements of FAR clause 52.204-21 and NIST SP 800-171 as implemented by DFARS clause 252.204-7012.

The CMMC Program rule does not include "threatened penalties." If a requirement of a DoD contract is not met, then standard contractual remedies applicable to that contract may apply.

The phased implementation plan described in § 170.3(e) is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements.

The self-assessment requirements build on the existing DFARS clause 252.204-7020 requirement as part of basic safeguarding of CUI. CMMC Level 3 requires advanced implementation, and the phase-in period provides additional time for an OSC to achieve the higher standard.

11. Flow down. Commenters expressed concern that the CMMC rule language was not clear enough regarding when self-assessments are allowed. One commenter believed requiring prime contractors to validate the compliance of those they transmit CUI to was too onerous and that the rule language was not clear on how to determine what level of CUI is being passed.

DoD Response: DoD policies guide Program Managers to appropriately apply CMMC Status requirements in DoD solicitations and resulting contracts, to include when Level 2 selfassessment rather than Level 2 certification assessment is appropriate.

The commenter misinterprets the text of § 170.23, which states: *If* a subcontractor will process, store, or transmit CUI in performance of the subcontract *and* the associated prime contractor has a requirement for a CMMC Status of Level 2 (C3PAO), *then the* CMMC Status of Level 2 (C3PAO) is the minimum requirement for the subcontractor.

CMMC flow down requirements are designed to apply consistent assessment requirements to all contractors, whether prime or subcontractor and regardless of company size, who are required to adequately safeguard CUI. The DoD cannot dictate DIB business practices and encourages prime contractors to carefully consider the necessity of sharing CUI information and to work with its subcontractors to flow down CUI with the required security and the least burden.

Defense contractors may share information about their CMMC Status with other DIB members to facilitate effective teaming arrangements when competing for DoD contract opportunities.

In addition, CMMC requirements apply for prime contractors and their subcontractors as outlined in § 170.23. For additional information about flow down of contractual requirements, see the 48 CFR part 204 CMMC Acquisition rule, RIN 0750-AK81, Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041).

12. International. Commenters expressed concern about international partners' use of cloud services that do not have FedRAMP or GovCloud equivalency. Also concerns that the draft language [in the proposed rule] did not explain reciprocity of cybersecurity standards between the US and International Partners. One commenter recommended exempting foreign businesses from assessment requirements.

DoD Response: A domestic or international business seeking a contract that includes DFARS clause 252.204-7012, and using a cloud service provider to process, store, or transmit covered defense information in performance of that DoD contract, must meet FedRAMP authorization or equivalency requirements. As the FedRAMP program and FedRAMP equivalency are available to international organizations, foreign partners do not need to develop their own FedRAMP program.

The DoD leverages FedRAMP to provide the requirements for the adoption of secure cloud services across the Federal Government by providing a standardized approach to security and risk assessment for cloud technologies and Federal agencies.

The Implementation of CMMC Program requirements described in § 170.3(e) of the rule does not promote assessments of any contractors over any other contractors. All companies, regardless of size, location, or nationality, will have access to authorized C3PAOs for certification assessments. The rule does not preclude non-U.S. citizens or foreign-owned C3PAOs from operating in the U.S. Additionally, U.S.-owned C3PAOs may operate in a foreign nation.

Section 170.20 states that OSCs that have completed a DCMA DIBCAC High Assessment aligned with CMMC Level 2 Scoping will be given the CMMC Status of Final Level 2 (C3PAO). International standards acceptance is not addressed in this rule.

Any consideration of reciprocity between foreign partner protected information and CUI and FCI would require a formal government to government international arrangement or agreement and is outside the scope of this 32 CFR part 170 CMMC Program rule.

Any discussion of exemptions for foreign businesses are outside the scope of the 32 CFR part 170 CMMC Program rule and may be addressed through government-to-government international arrangements or agreements.

The *Discussion of Public Comments and Resulting Changes* section in the preamble of the final rule addresses all public comments received during the mandatory 60-day public comment period for the proposed rule and supporting documents.

Response to Comments from Chief Counsel for Advocacy of the SBA

On December 26, 2023, the Department of Defense (DoD) published a proposed rule entitled Cybersecurity Maturity Model Certification (CMMC) Program, 88 CFR 89058. This proposed rule intends to create a mechanism by which the DoD can certify that contractors and subcontractors are in compliance with the stated cybersecurity guidelines. The SBA Office of Advocacy (SBA or Advocacy) submitted the following comments and concerns on the proposed rule in a letter addressed to the DoD CIO within the public comment period for the proposed 32 CFR part 170 CMMC Program rule.

"Advocacy is principally concerned with the ability for small businesses to meet and comply with the standards and timelines set out in the CMMC Program without further clarification and guidance documents from the DoD. The current rule does not provide clear guidance on the process to create enclaves, which would allow more small business subcontractors to participate in DoD contracts without meeting the full requirements necessary for the prime contractor. Advocacy seeks clarification on the role of Third-Party Assessment Organizations (C3PAO) and the indemnification a C3PAO has if a contractor or subcontractor is out of compliance."

"Advocacy concerns also include the process of how and if more C3PAOs can be certified by the DoD to review the numerous contracts that will be subject to certifications. Advocacy urges the DoD to provide clarification about the enforcement mechanisms for breaches of cybersecurity."

"Lastly, Advocacy reminds the DoD that this rule will impose a high cost of compliance on small businesses and any means to reduce the burden on small businesses will increase the participation of these impacted businesses."

"The proposed rule would give contractual effect to NIST SP 800-171 and 172, requiring companies to meet the three levels of compliance if the contracts involve FCI or CUI. CMMC attempts to redesign previous iterations of cybersecurity models with a more streamlined process. This proposal would simplify previous systems to create a more streamlined certification system. This rule differs from previous iterations by allowing for businesses to create enclaves within their business models, allowing the business to implement the CMMC standards while not drastically changing every aspect of their business process."

"SBA Comment 1: Under the proposed rule, the CMMC Program will require all DoD contractors and subcontractors who handle Federal contract information (FCI) and Controlled Unclassified Information (CUI) to maintain cybersecurity protections of their systems. CMMC will create three levels of compliance, depending on the level of security necessary for which the contractor has access. Level 1 has 15 requirements focused on logging access to potential FCI. Level 2 includes minimum requirements for contractors handling CUI and adds 110 requirements. Level 3 addresses an additional 24 requirements. Each level will pose varying challenges for small businesses of every kind to comply with the progressing requirements. Advocacy has commented on previous proposals for CMMC concerning the significant impact this will have on small business contractors."

"Advocacy held outreach meetings with diverse small business stakeholders concerning this rule, both in-person and virtually. - Small businesses expressed concerns with how to compensate the increased costs due to implementing CMMC and asked for clarity on aspects of the proposed CMMC rule. Advocacy has four chief concerns with the proposed rule."

"Advocacy requests clear and concise guidance for small business contractors and subcontractors to create enclaves in order to lessen the burden of compliance on the businesses."

"The proposed rule states that different business segments or different enclaves of a business can be assessed or certified at different CMMC levels. Creating and implementing enclaves will be most effective when a large prime contractor creates these enclaves to ease the burden on small subcontractors. The rule mentions the use of enclaves but does not provide guidance on how to implement enclaves within a business."

DoD Response: The Department acknowledges the concerns articulated by the Small Business Administration (SBA) and commits to enhancing training provisions after the rule is final and effective. Moreover, the Department pledges to reinstate outreach endeavors targeting the broader industry and specifically small businesses to facilitate familiarity with CMMC requirements once the rule is final and effective. However, the Department does not intend to formulate specific directives pertaining to the configuration and segregation of corporate information systems into enclaves. Such determinations must be tailored to individual companies, considering a multitude of unique factors.

External service providers (ESPs) will be a driving force for small businesses' compliance with CMMC requirements. ESPs are vendors that handle security related data or CUI

on their own assets and software. The ability of ESPs to create effective and economically feasible services will allow businesses to enclave different operations more easily and avoid unduly costly compliance expenses.

"SBA Comment 2: Advocacy recommends that the DoD create a presumption to reduce the number of small contracts that are subject to CMMC Level 2. This can be achieved through varying means, including a positive requirement for prime contractors or the ability for a prime contractor to engage in using enclaves as a positive value marker for their contracts. Further, the agency contracting officer could be required to engage in mitigating efforts if such CMMC related issues arise between a subcontractor and prime contractor."

DoD Response: The Department is committed to robustly supervising the CMMC Program and will take appropriate measures to ensure its efficient execution. Presently, the Department has no intention to mandate contracting offices adopt presumptive measures that would diminish the number of small contracts subject to CMMC Level 2 assessment, nor does it plan to impose affirmative requirements on prime contracts to utilize enclaves.

"SBA Comment 3: Advocacy seeks clarity on the role of C3PAOs and the ability of C3PAOs to meet the demand for CMMC.

"For CMMC Level 2 compliance, a CMMC third-party assessor (C3PAO) will triennially inspect the businesses' compliance with the 110 requirements of CMMC Level 2. Stakeholders raised concerns regarding the role C3PAOs will play in Level 2 certification and sought clarity on the indemnification of issues arising from a certification. Stakeholders raised concerns that if there are an insufficient number of C3PAOs to timely inspect every contractor before the rule is effective, then small businesses will be the last ones to be certified. Advocacy recommends creating a streamlined process to provide organizations with C3PAO certifications. This process would meet the immediate need of contractors to initially certify with a C3PAO that the business meets CMMC Level 2 requirements. Particularly, there should be availability of C3PAOs for small businesses and ensure small business owners are not falling behind."

DoD Response: In alignment with its standard practice across all programs, the Department is committed to diligent oversight of the CMMC Program and will enact appropriate measures to ensure its successful execution. The phased implementation strategy outlined in § 170.3(e) in the rule is designed to tackle initial challenges, facilitate assessor training, and afford companies sufficient time to comprehend and integrate CMMC prerequisites.

While the Department remains open to considering future adjustments, including potential extensions to the implementation timeline or alternative solutions to address any capacity constraints faced by C3PAOs, no such initiatives are currently under active consideration.

"SBA Comment 4: Advocacy asks the DoD to clarify enforcement guidelines/mechanisms.

As proposed, Level 1 contractors would annually attest their compliance with the requirements. While at Level 2, there would be attestations with C3PAO certifications every three years. Stakeholders raised questions about the practical steps the DoD will take in enforcement actions for breaches. Further, stakeholders raised concerns regarding the availability of remediating steps in the instance of failure to meet a CMMC requirement. Advocacy recommends the agency create guidance documents for small business contractors to better understand the legal effects of the CMMC."

DoD Response: Regarding enforcement, as the CMMC is slated for implementation as a precondition for contract award consideration, non-compliance with CMMC requirements will result in disqualification from contract award; or post-award, could result in standard contractual and other remedies for failure to timely and satisfactorily address outstanding POA&Ms to fully implement CMMC requirements and meet contractual obligations.

"SBA Comment 5: Advocacy highlights the need for DoD to create rules that encourage and improve small business participation in contracting programs. Advocacy reiterates the importance of small businesses in Federal contracting. [Excerpt from footnote 21: "Small businesses make up 99.9 percent of all U.S. businesses as well as 73 percent of companies in the

defense industrial base, and last year small businesses were awarded over 25 percent of all DoD prime contracts. As the economic engine of our nation, small businesses create jobs, generate innovation, and are essential, daily contributors to national security and the defense mission.] Creating accessible, commercially viable, and secure cyber systems is critical for the future of national security. Small businesses wish to continue to be a powerful driver of national defense contracting. Advocacy heard small business stakeholders from across the country express their strong commitment to protecting our country from cyber-attacks and recognize the critical need for CMMC and other cybersecurity measures.

"Small businesses urge DoD to create flexibilities such as using Plan of Action and Milestones (POA&Ms) when this rule goes into effect initially, allowing small businesses to ramp up to full compliance with their respective CMMC level."

DoD Response: Department acknowledges the concerns voiced by the SBA regarding the participation of small businesses in contracting programs and the importance of fostering their involvement in Federal contracting, particularly within the defense industrial base. Recognizing the significant role small businesses play in national security and defense missions, the Department is committed to diligently addressing these concerns.

While the Department values the input provided by small business stakeholders and understands the desire for flexibilities, including the use of POA&Ms during the initial implementation phase, it must carefully balance multiple factors to ensure the effectiveness and integrity of the CMMC Program.

"SBA Comment 6: Advocacy's chief concerns surround a lack of clarity on key aspects of the proposed rule. Advocacy requests clarification from DoD as to how to create enclaves within businesses. Encouraging the use of ESPs and incentivizing large prime contractors to keep all subcontractors from being subject to high levels of cybersecurity will be key in keeping small businesses engaged in DoD contracting. Guidance documents for small businesses (especially aimed at the smallest of small businesses) and ESPs will create an easier ramp for small business compliance. Advocacy requests clarity from DoD regarding the role of C3PAOs and encourages the DoD to ensure small businesses can obtain certification from C3PAOs in a timely manner. Further, the DoD should clarify the enforcement and procedural repercussions for a failure to meet various CMMC levels. Lastly, the DoD should set achievable goals as CMMC is implemented, ensuring that current small businesses contracting with the agency can continue work with the government while ensuring our nation's defense."

DoD Response: The DoD acknowledges the SBA advocacy chief's concerns and will make additional training resources available following finalization of this rule. The DoD deems that the level of detail on the topics identified is appropriate for codification in the 32 CFR part 170 CMMC Program rule. The DoD will resume outreach efforts with the aim of promoting CMMC familiarization among small businesses once the rule is final and effective and any constraints on such engagements no longer apply. However, DoD caveats that providing any specific instructions for configuring corporate information systems into enclaves is beyond the guidance that DoD intends to provide, as such decisions are unique to each company.

The role of C3PAOs is thoroughly described in § 170.9 CMMC Third-Party Assessment Organizations (C3PAOs) and in the supplemental documents.

In terms of enforcement, since CMMC will be implemented as a pre-award requirement, the repercussions of failure to meet CMMC requirements will include failure to be selected for contract award, or standard contractual and other remedies for failure to timely and satisfactorily close-out a POA&M and meet or maintain the contractual CMMC requirements.

As with all of DoD programs, the Department intends to effectively oversee the CMMC Program and take the appropriate actions needed to manage its effective implementation. The phased implementation plan described in § 170.3(e) was extended by six months and is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements.

Small Business Entities Impacted

This rule will impact small businesses that do business with the Department of Defense, except those competing on contracts or orders that are exclusively for COTS items or when receiving contracts or orders valued at or below the micro-purchase threshold. According to the Federal Procurement Data System (FPDS) there is an average of 29,260 unique small business contractors: FY 2019 (31,189), FY 2020 (29,166) and FY 2021 (27,427).

Cost Assumptions and Analysis for CMMC

Complete details on CMMC requirements and associated costs, savings, and benefits of this rule are provided in the Regulatory Impact Analysis referenced in the preamble. Key Components of the model are described in §§ 170.14 through 170.24.

(a) Assumptions for the updated CMMC Program Cost Analysis

In estimating the public cost for a small DIB company to achieve CMMC compliance or certification at each CMMC level, DoD considered non-recurring engineering costs, recurring engineering costs, assessment costs, and affirmation costs for each CMMC Level[58]. These costs include labor and consulting.

Estimates include size and complexity assumptions to account for organizational differences and how it handles Information Technology (IT) and cybersecurity:

- small entities have a less complex, less expansive operating environment and Information Technology (IT) / Cybersecurity infrastructure compared to larger DIB companies.
- small entities outsource IT and cybersecurity to an External Service Provider (ESP) entities (large or small) pursuing CMMC Level 2 self-assessment will seek consulting or • implementation assistance from an ESP to either help them prepare for the assessment technically or participate in the assessment with the C3PAOs.

Estimates do not include implementation (Non-recurring Engineering Costs (NRE)) or maintenance costs (Recurring Engineering (RE)) for requirements prescribed in current regulations.

For **CMMC Levels 1 and 2**, cost estimates are based upon assessment, reporting and affirmation activities which a contractor will take to validate conformance with existing cybersecurity requirements from the FAR clause 52.204-21 (effective June 15, 2016) to protect FCI, and the DFARS clause 252.204-7012 which required contractor implementation of NIST SP 800-171 not later than December 31, 2017, to protect CUI. As such, costs estimates are not included for an entity to implement security requirements, maintain existing security requirements, or remediate a Plan of Action for unimplemented requirements.

For **CMMC Level 3**, the estimates factor in the assessment, reporting and affirmation activities in addition to estimates for NRE and RE to implement and maintain CMMC Level 3 requirements. CMMC Level 3 requirements are a subset of NIST SP 800-172 Feb2021 Enhanced Security Requirements as described in § 170.30 of the CMMC rule and are not currently required through other regulations. CMMC Level 3 is expected to apply only to a small subset of DIB contractors.

The **Cost Categories** used for each CMMC Level are described below:

1. ***Nonrecurring Engineering Costs:*** Estimates consist of hardware, software, and the associated labor to implement the same. Costs associated with implementing the requirements defined in FAR clause 52.204-21 and NIST SP 800-171 R2 are assumed to have been implemented and are therefore not accounted for in this cost estimate. As such, these costs only appear in CMMC Level 3. Where nonrecurring engineering costs are referenced, they are only accounted for as a one-time occurrence and are reflected in the year of the initial assessment.
2. ***Recurring Engineering Costs:*** Estimates consist of annually recurring fees and associated labor for technology refresh. Costs associated with implementing the

[58] DoD estimates of the hours, recurring and non-recurring costs, and labor rates are based upon subject matter expertise from the DOD Chief Information Office, CMMC Program Office, and DoD/DIBCAC.

requirements defined in FAR clause 52.204-21 and NIST SP 800-171 R2 are assumed to have been implemented and are therefore not accounted for in this cost estimate. As such, these costs only appear in CMMC Level 3.

***Assessment Costs**:* Estimates consist of activities for pre-assessment preparations (which includes gathering and/or developing evidence that the assessment objectives for each requirement have been satisfied), conducting and / or participating in the actual assessment, and completion of any post-assessment work. Assessment costs are represented by notional phases. Assessment costs assume the offeror / contractor passes the assessment on the first attempt (conditional – with an allowable POA&M or final). Each phase includes an estimate of hours to conduct the assessment activities including:

(a) Labor hour estimates for a company (and any ESP support) to prepare for and participate in the assessment.

(b) C3PAO cost estimates for companies pursuing a certification.

- Labor hour estimates for certified assessors to work with the small business to conduct the actual assessment.

(c) Assessment Costs broken down into phases.

- Phase 1: *Planning and preparing for the assessment.*
- Phase 2: *Conducting the assessment* (self or C3PAO).
- Phase 3: *Reporting of Assessment Results.*
- Phase 4: *POA&M Closeout* (for CMMC Level 3 only, where allowed, if applicable).
  - CMMC allows a limited open Plan of Action and Milestones (POA&M) for a period of 180 days to remediate the POA&M, see § 170.37.

3. Affirmations: Estimates consist of costs for a contractor to submit to SPRS an initial and affirmation of compliance that the covered contractor information system is compliant with and will maintain compliance with the requirements of the applicable CMMC Level. Where POA&Ms are allowed, an affirmation must be submitted with the POA&M closeout. Except for Small Entities for Level 1 and Level 2, it is assumed the task requires the same labor categories and estimated hours as the final reporting phase of the assessment.

(b) Comparison to the initial CMMC Program Cost Analysis

Public comments on the initial CMMC Program indicated that cost estimates were too low. Updated CMMC Program cost estimates account for that feedback with the following improvements:

- Allowance for outsourced IT services
- Increased total time for the contractor to prepare for the assessment, including limited time for learning the reporting and affirmation processes.
- Allowance for use of consulting firms to assist with the assessment process.
- Time for a senior level manager to review the assessment and affirmation before submitting the results into SPRS.
- Updated government and contractor labor rates that include applicable burden costs. As a result, some cost estimates for the updated CMMC Program may be higher than those included in the initial CMMC Program.

(c) Cost Analysis / Estimates by CMMC Level

CMMC Level 1 Self-Assessment and Affirmation Costs for Small Business Entities •

Nonrecurring and recurring engineering costs: There are no nonrecurring or recurring engineering costs associated with CMMC Level 1 since it is assumed the contractor has implemented basic safeguarding requirements.[59]

• ***Self-Assessment Costs and Initial Affirmation Costs**:* It is estimated that the cost to support a CMMC Level 1 assessment and affirmation is ***$5,977** (as summarized in table

[59] Again, it is assumed that that DIB contractors and subcontractors have already implemented the 15 basic safeguarding requirements in FAR clause 52.204-21.

1). A Level 1self-assessment is conducted annually, and is based on the assumptions detailed below:

- Phase 1: Planning and preparing for the assessment: **$1,803**

- A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
- An external service provider (ESP)[60] for 4 hours ($260.28 x 4hrs = $1,041)

- Phase 2: Conducting the self-assessment: **$2,705**

- A director (MGMT5) for 6 hours ($190.52/hr x 6hrs = $1,143)
- An external service provider (ESP) for 6 hours ($260.28 x 6hrs = $1,562)

- Phase 3: Reporting of Assessment Results into SPRS: **$909**

- A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
- An external service provider (ESP) for 2 hours ($260.28/hr * 2hrs = $521)
- A staff IT specialist (IT4) for 0.08 hours[61] ($86.24/hr x 0.08hrs = $7)

- Affirmation: initial affirmation post assessment: **$ 560**

- ***Reaffirmations****:* It is estimated that the costs to reaffirm a CMMC Level I annually for a small entity is **$560**

- A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
- A staff IT specialist (IT4) for 2.08 hours ($86.24/hr x 2.08hrs = $179)

- ***Summary****:* The following is the annual small entities total cost summary for CMMC

Level 1 self-assessments and affirmations over a ten-year period: (Example calculation, Year 1: ***$5,977** per entity (detailed above) x 699 entities (cumulative) = $4,177,845)

Table 30 – Total Cost Summary for Small Entities for CMMC Level 1 Self-Assessments and Affirmations

Year	Small Entities Per Year	Cumulative Small Entities	Annual Total Cost (self-assess, affirm)
1	699	699	$4,177,845
2	3,493	4,192	$25,055,116
3	11,654	15,846	$94,709,771
4	22,336	38,182	$228,209,547
5	22,333	60,515	$361,691,392
6	22,333	82,848	$495,173,237
7	20,162	103,010	$615,679,258
8		103,010	$615,679,258
9		103,010	$615,679,258
10		103,010	$615,679,258
Total	**103,010**		**$3,671,733,942**

CMMC Level 2 Self-Assessment and Affirmation Costs for Small Business Entities

The costs below account for a CMMC Level 2 self-assessment of the applicable contractor information system(s) with NIST SP 800-171 R2 requirements based on assumptions defined above.

- ***Nonrecurring and recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with CMMC Level 2 self-assessment since it is assumed the contractor has implemented NIST SP 800-171 R2 requirements.

[60] An external service provider is assumed to be an "Information Assurance Specialist Level 7" with an hourly rate of $260.

[61] A person needs to enter the information into SPRS, which should only take five minutes.

• ***Assessment Costs and Initial Affirmation Costs****:* It is estimated that the cost to support a CMMC Level 2 self-assessment and affirmation for a small entity is ***$34,277**. The threeyear cost is $37,196 (as summarized in 4.1.2 above, table 2), which includes the triennial assessment + affirmation, plus two additional annual affirmations ($34,277 + $1,459 +
$1,459).

- Phase 1: **Planning and preparing for the self-assessment**: **$14,426**

- A director (MGMT5) for 32 hours ($190.52/hr x* 32hrs = $6,097)
- An external service provider (ESP) for 32 hours ($260.28/hr x 32hrs = $8,329)

- Phase 2: Conducting the self-assessment: $15,542

- A director (MGMT5) for 16 hours ($190.52/hr x 16hrs = $3,048)
- An external service provider (ESP) for 48 hours ($260.28/hr x 48hrs = $12,493)

- Phase 3: **Reporting of assessment results**: **$2,851**

- A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
- An external service provider (ESP) for 8 hours ($260.28/hr x 8hrs = $2,082)
- A staff IT specialist (IT4) for 0.08 hours ($86.24/hr x 0.08hrs = $7)

- Affirmation – initial affirmation post assessment: **$1,459**

• ***Reaffirmations:*** It is estimated that the costs to reaffirm a CMMC Level 2 self-assessment annually is **$1,459** (three-year costs to reaffirm a CMMC Level 2 selfassessment annually is $4,377, or $1,459 x 3):

- A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
- A staff IT specialist (IT4) for 8.08 hours ($86.24/hr x 8.08hrs = $697)

• ***Summary****:* The following is the annual small entities total cost summary for CMMC Level 2 self-assessments and Affirmations over a ten-year period: (Example calculation, Year 2: **(*$34,277** self-assessment per entity x 101 entities) + (**$1,459** annual affirmation per entity x 20 entities) = $3,491,193)

Table 31- Total Cost Summary for Small Entities for CMMC Level 2 Self-assessments and Affirmations

CMMC Level 2: Self-Assessment for Small Entities			
Year	**Entities Performing Triennial Self-Assessments and Initial Affirmation**	**Entities Performing Annual Affirmation Actions Only**	**Total Cost**
1	20	0	$685,547
2	101	20	$3,491,193
3	335	121	$11,659,448
4	662	436	$23,327,706
5	743	997	$26,922,622
6	977	1,405	$35,538,762
7	1,241	1,720	$45,047,546
8	743	2,218	$28,703,951
9	977	1,984	$36,383,471
10	1,241	1,720	$45,047,546
Total	**7,040**	**10,621**	**$256,807,792**

CMMC Level 2 Certification and Affirmation Costs for Small Business Entities

The costs below account for a CMMC Level 2 Certification assessment and affirmation costs of the applicable contractor information system(s) with NIST SP 800-171 R2 requirements based on assumptions defined above. CMMC Level 2 certification assessments require hiring a C3PAO to perform the assessment.

- ***Nonrecurring or recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with CMMC Level 2 C3PAO Certification since it is assumed the contractor has implemented NIST SP 800-171 R2 requirements.
- ***Assessment Costs and Initial Affirmation Costs****:* It is estimated that the cost to support a CMMC Level 2 C3PAO Certification and affirmation for a small entity is ***$101,752.** The three-year cost is $104,670 (as summarized in section 3(b) above, table 1), and includes the triennial assessment + affirmation plus two additional annual affirmations ($101,752 + $1,459 + $1,459).

  - **Phase 1: Planning and preparing for the assessment**: **$20,699**
    - A director (MGMT5) for 54 hours ($190.52/hr x 54hrs = $10,288)
    - An external service provider (ESP) for 40 hours ($260.28/hr x 40hrs = $10,411)
  - **Phase 2: Conducting the C3PAO assessment**: **$45,509**
    - A director (MGMT5) for 64 hours ($190.52/hr x 64hrs = $12,193)
    - An external service provider (ESP) for 128 hours ($260.28/hr x 128hrs = $33,316)
  - **Phase 3: Reporting of C3PAO Assessment Results**: **$2,851**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - An external service provider (ESP) for 8 hours ($260.28/hr x 8hrs = $2,082)
    - A staff IT specialist (IT4) for 0.08 hours ($86.24/hr x 0.08hrs = $7)
  - **Affirmation** – initial affirmation post assessment: **$1,459**
  - **C3PAO Costs:** C3PAO engagement inclusive of Phases 1, 2, and 3 (3-person team) for 120 hours ($260.28/hr x 120hrs = **$31,234**)

- ***Reaffirmations****:* It is estimated that the costs to reaffirm a CMMC Level 2 C3PAO Assessment annually is **$1,459** (three-year cost is $4,377, or $1,459 x 3)
  - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
  - A staff IT specialist (IT4) for 8.08 hours ($86.24/hr x 8.08hrs = $697)
- ***Summary****:* The following is the annual small entities total cost summary for CMMC Level 2 Certifications and Affirmations over a ten-year period: (Example calculation, Year 2: (***$101,752** assessment per entity x 1,926 entities) + (**$1,459** annual affirmation per entity x 382 entities) = $196,531,451)

Table 32 – Total Cost Summary for Small Entities for CMMC Level 2 Certifications and Affirmations

CMMC Level 2: Certification for Small Entities			
Year	**Entities Performing Triennial Certifications and Initial Affirmation**	**Entities Performing Annual Affirmation Actions Only**	**Total Cost**
1	382	0	$38,869,223
2	1,926	382	$196,531,451
3	6,414	2,308	$656,003,811
4	12,675	8,340	$1,301,872,564
5	14,215	19,089	$1,474,252,306

6	18,703	26,890	$1,942,295,763
7	23,771	32,918	$2,466,768,671
8	14,215	42,474	$1,508,368,920
9	18,703	37,986	$1,958,483,830
10	23,771	32,918	$2,466,768,671
Total	**134,775**	**203,305**	**$14,010,215,209**

CMMC Level 3 Certification and Affirmation Costs for Small Business Entities

Contractors pursuing CMMC Level 3 certification assessment must have a current Final CMMC Level 2 certification assessment, and demonstrate compliance with CMMC Level 3, which is a subset of security requirements from NIST SP 800-172 Feb2021 that have DoD predefined selections and parameters. CMMC Level 3 requires compliance with security requirements not required in prior rules. Therefore, Nonrecurring Engineering and Recurring Engineering cost estimates have been included for the initial implementation and maintenance of the required subset of NIST 800-172 Feb2021 requirements. The cost estimates below accounts for time for a contractor to implement the security requirements and prepare for, support, and participate in a CMMC Level 3 assessment conducted by DCMA DIBCAC. The contractor should therefore keep in mind that the cost of a Level 3 certification will also incur the cost of a CMMC Level 2 certification assessment by a C3PAO in addition to the costs to assess the requirements specific to Level 3. Inclusion of CMMC Level 3 certification is expected to affect only a small subset of defense contractors or subcontractors in the DIB.

The estimated engineering costs per small entity is associated with the CMMC Level 3.

- ***Nonrecurring Engineering Costs**:* **$2,700,000**
- ***Recurring Engineering Costs**:* **$490,000**
  - ***Assessment Costs and Initial Affirmation Costs**:* It is estimated that the cost to support a CMMC Level 3 C3PAO Certification for a small entity is ***$9,050** The three-year cost is $12,802 (summarized in 4.1.2 above, table 2), and includes the triennial assessment + affirmation, plus two additional annual affirmations ($9,050 + $1,876 + $1,876):
  - **Phase 1: Planning and preparing for the Level 3 assessment**: **$1,905**
  - A director (MGMT5) for 10 hours ($190.52/hr x 10hrs = $1,905)
  - **Phase 2: Conducting the Level 3 assessment**: **$1,524**
    - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
  - **Phase 3: Reporting of Level 3 assessment results**: **$1,876**
    - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
    - A staff IT specialist (IT4) for 4.08 hours ($86.24/hr x 4.08hrs = $352)
  - **Phase 4: Remediation (for CMMC Level 3 if necessary** and allowed): **$1,869**
    - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
    - A staff IT specialist (IT4) for 48 hours ($86.24/hr x 48hrs = $345)
    - **Affirmation** – initial affirmation post assessment: **$1,876**
    - ***Reaffirmations**:* It is estimated that the costs to reaffirm a CMMC Level 3 Assessment annually is **$1,876** (three-year cost is $5,628, or $1,876 x 3)
  - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
  - A staff IT specialist (IT4) for 4.08 hours ($86.24/hr x 4.08hrs = $352)
- ***Summary:*** The following is the annual small entities total cost summary for CMMC Level 3 Certifications and Affirmations over a ten-year period. Example calculation, Year 2 (reference per entity amounts above):
  - *($9,050 Certification per entity x 45 entities) + ($1,876 Annual Affirmation per entity x 3 entities) = $412,897, and

- $121,500,000 Nonrecurring Engineering cost ($2,700,000 per entity x 45 entities being certified), and
- $23,520,000 Recurring Engineering cost ($490,000 per entity x 45 entities being certified) + ($490,000 per entity x 3 entities performing affirmations)
- $145,432,897 Total Cost = Certification and Affirmation Cost ($412,897) + Nonrecurring Engineering cost ($121,500,000) + Recurring Engineering cost ($23,520,000), or $145,432,897.

Table 33 – Total Cost Summary for Small Entities for CMMC Level 3 Certifications and Affirmations

Yr	Entities Performing Triennial Certification including Initial Affirmation	Entities Reaffirmation Actions Only	Triennial Certification and Affirmation Total Cost	Non-recurring Engineering Cost	Recurring Engineering Cost	Total Cost
1	3	0	$27,151	$8,100,000	$1,470,000	$9,597,151
2	45	3	$412,897	$121,500,000	$23,520,000	$145,432,897
3	151	48	$1,456,663	$407,700,000	$97,510,000	$506,666,663
4	292	196	$3,010,423	$780,300,000	$239,120,000	$1,022,430,423
5	334	443	$3,853,914	$780,300,000	$380,730,000	$1,164,883,914
6	440	626	$5,156,569	$780,300,000	$522,340,000	$1,307,796,569
7	553	774	$6,456,917	$704,700,000	$650,230,000	$1,361,386,917
8	334	993	$4,885,718		$650,230,000	$655,115,718
9	440	887	$5,646,207		$650,230,000	$655,876,207
10	553	774	$6,456,917		$650,230,000	$656,686,917
Tot	**3,145**	**4,744**	**$37,363,377**	**$3,582,900,000**	**$3,865,610,000**	**$7,485,873,377**

Projected Reporting, Recordkeeping, and Compliance Requirements

The CMMC Program provides for the assessment of contractor implementation of cybersecurity requirements to enhance confidence in contactor protection of unclassified information within the DoD supply chain. CMMC contractual requirements are implemented under the 48 CFR part 204 CMMC Acquisition rule, with associated rulemaking for the CMMC Program requirements (e.g., CMMC Scoring Methodology, certificate issuance, information accessibility) under the 32 CFR part 170 CMMC Program rule. The 32 CFR part 170 CMMC Program rule includes two separate information collection requests (ICR), one for the CMMC Program and one for CMMC eMASS.

This information collection is necessary to support the implementation of the CMMC assessment process for Levels 2 and 3 certification assessment, as defined in §§ 170.17 and 170.18 respectively.

The CMMC Level 2 certification assessment process is conducted by Certified Assessors, employed by CMMC Third-Party Assessment Organizations (C3PAOs). During the assessment process, Organizations Seeking Certification[62] (OSCs) hire C3PAOs to conduct the third-party assessment required for certification.

The CMMC Level 3 certification assessment process is conducted by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

[62] An Organization Seeking Certification (OSC) is an entity seeking to contract, obtain, or maintain CMMC certification for a given information system at a particular CMMC Level. An OSC is also an OSA.

Use of the Information

Level 1 and Level 2 CMMC Self-Assessments. Organizations Seeking Assessment[63] (OSAs) follow procedures as defined in §§ 170.15(a)(1) and 170.16(a)(1) to conduct CMMC Level 1 and Level 2 self-assessments on their information systems to determine conformance with the information safeguarding requirements associated with the CMMC level requirements. The Level 1 and Level 2 self-assessment information collection reporting and recordkeeping requirements will be included in a modification of an existing Defense Federal Acquisition Regulation Supplement (DFARS) collection approved under OMB Control Number 0750-0004, Assessing Contractor Implementation of Cybersecurity Requirements. Modifications to this DFARS collection will be addressed as part of the 48 CFR part 204 CMMC Acquisition final rule.

CMMC Level 2 Certification Assessment

The Level 2 certification assessment information collection burden for reporting and recordkeeping requirements are included in the 32 CFR part 170 CMMC Program rule. The information collection burden for the OSCs to upload affirmations in SPRS is included in the 48 CFR part 204 CMMC Acquisition final rule. Additionally, the information collection burden requirements for the CMMC instantiation of eMASS are addressed in a separate 32 CFR part 170 CMMC Program final rule information collection request (ICR).

OSCs follow procedures as defined in § 170.17 to prepare for CMMC Level 2 certification assessment.

Certified Assessors assigned by C3PAOs follow requirements and procedures as defined in § 170.17 to conduct CMMC assessments on defense contractor information systems to determine conformance with the information safeguarding requirements associated with CMMC Level 2. This is an assessment to validate implementation of the 110 security requirements from NIST SP 800-171 R2.

Prospective C3PAOs must complete and submit the Standard Form (SF) 328 Certificate Pertaining to Foreign Interests (OMB control number 0704-0579) upon request from Defense Counterintelligence and Security Agency (DCSA).

C3PAOs must generate and collect pre-assessment and planning material (contact information for the OSC, information about the C3PAO and assessors conducting the assessment, the level of assessment planned, the CMMC Model and Assessment Guide versions, and assessment approach), artifact information (list of artifacts, hash of artifacts, and hashing algorithm used), final assessment reports, appropriate CMMC certificates of assessment, and assessment appeal information. C3PAOs submit the data they generate and collect into the CMMC instantiation of eMASS, the information collection required for this submission is addressed in a separate CMMC eMASS ICR for the 32 CFR part 170 CMMC Program rule. OSCs may have a POA&M at CMMC Level 2 as addressed in § 170.21. C3PAOs perform a POA&M closeout assessment. The C3PAO process to conduct a POA&M Close-out Assessment, where applicable, is the same as the initial assessment with the same information collection requirements.

OSCs must retain artifacts used as evidence for the assessment for the duration of the validity period of the certificate of assessment, and at minimum, for six years from the date of certification assessment as addressed in § 170.17(c)(4). The OSC is responsible for compiling relevant artifacts as evidence and having knowledgeable personnel available during the assessment. The organizational artifacts are proprietary to the OSC and will not be retained by the assessment team unless expressly permitted by the OSC. To preserve the integrity of the artifacts reviewed, the OSC creates a hash of assessment evidence (to include a list of the artifact names, the return values of the hashing algorithm, and the hashing algorithm used) and retains the artifact information for six years. The information obtained from the artifacts is an

[63] An Organization Seeking Assessment (OSA) is an entity seeking to conduct, obtain, or maintain a CMMC assessment for a given information system at a particular CMMC Level. The term OSA includes all OSCs.

information collection and is provided to the C3PAO for uploading into the CMMC instantiation of eMASS (addressed in a separate CMMC eMASS ICR for the 32 CFR part 170 CMMC Program final rule); the artifacts themselves are not an information collection. The OSC process to support a POA&M Close-out Assessment, where applicable, is the same as the initial assessment with the same information collection requirements.

If an OSC does not agree with the assessment results, it may formally dispute the assessment and initiate an Assessment Appeal process with the C3PAO who conducted the assessment. C3PAOs submit assessment appeals using eMASS (addressed in a separate CMMC eMASS ICR for the 32 CFR part 170 CMMC Program final rule). Appeals are tracked in the CMMC instantiation of eMASS and any resulting changes to the assessment results are uploaded into the CMMC instantiation of eMASS.

C3PAOs maintain records for a period of six years of monitoring, education, training, technical knowledge, skills, experience, and authorization of each member of its personnel involved in inspection activities; contractual agreements with OSCs; any working papers generated from Level 2 certification assessments; and organizations for whom consulting services were provided as addressed in § 170.9(b)(9). The Accreditation Body provides the CMMC PMO with current data on C3PAOs, including authorization and accreditation records and status using the CMMC instantiation of eMASS (addressed in a separate CMMC eMASS ICR for the 32 CFR part 170 CMMC Program final rule).

The Accreditation Body provides all plans related to potential sources of revenue, to include but not limited to fees, licensing, processes, membership, and/or partnerships to the Government's CMMC PMO as addressed in § 170.8(b)(13).

CAICOs maintain records for a period of six years of all procedures, processes, and actions related to fulfillment of the requirements set forth in § 170.10(b)(9).

CMMC Level 3 Certification Assessment

The Level 3 certification assessment information collection burden for reporting and recordkeeping requirements are included in the 32 CFR part 170 CMMC Program final rule. The information collection burden for OSCs to upload affirmations in SPRS is included in the 48 CFR part 204 CMMC Acquisition final rule. Additionally, the information collection burden requirements for the CMMC instantiation of eMASS are addressed in a separate CMMC eMASS ICR for the 32 CFR part 170 CMMC Program final rule.

OSCs follow procedures as defined in § 170.18 to prepare for CMMC Level 3 certification assessment.

DCMA DIBCAC Assessors follow requirements and procedures as defined in § 170.18 to conduct CMMC assessments on defense contractor information systems to determine conformance with the information safeguarding requirements associated with CMMC Level 3. This is an assessment to validation the implementation of the 24 selected security requirements from NIST SP 800-172 Feb2021. Because DCMA DIBCAC is a government entity, there are no public information collection requirements.

DCMA DIBCAC must generate and collect pre-assessment and planning material (contact information for the OSC, information about the assessors conducting the assessment, the level of assessment planned, the CMMC Model and Assessment Guide versions, and assessment approach), artifact information (list of artifacts, hash of artifacts, and hashing algorithm used), final assessment reports, appropriate CMMC certificates of assessment, and assessment appeal information. DCMA DIBCAC submits the data it generates and collects into the CMMC instantiation of eMASS (addressed in a separate CMMC eMASS ICR for the 32 CFR part 170 CMMC Program final rule).

OSCs may have a POA&M at CMMC Level 3 as addressed in § 170.21.
DCMA DIBCAC performs a POA&M closeout assessment. The DCMA DIBCAC process to conduct a POA&M close-out assessment, where applicable, is the same as the initial assessment with the same information collection requirements.

OSCs must retain artifacts used as evidence for the assessment for the duration of the validity period of the certificate of assessment, and at minimum, for six years from the date of

certification assessment as addressed in § 170.18(c)(4). The OSC is responsible for compiling relevant artifacts as evidence and having knowledgeable personnel available during the assessment. Assessors will not permanently retain assessment artifacts. To preserve the integrity of the artifacts reviewed during the assessment, the OSC creates a hash of assessment evidence (to include a list of the artifact names, the return values of the hashing algorithm, and the hashing algorithm used) and retains the artifact information for six years. The information obtained from the artifacts is an information collection and DCMA DIBCAC uploads the information into the CMMC instantiation of eMASS; the artifacts themselves are not an information collection. The OSC process to support a POA&M close-out assessment, where applicable, is the same as the initial assessment with the same information collection requirements.

If an OSC does not agree with the assessment results, it may formally dispute the assessment and initiate an Assessment Appeal process with DCMA DIBCAC. DCMA DIBCAC submits assessment appeals using eMASS. Appeals are tracked in the CMMC instantiation of eMASS and any resulting changes to the assessment results are uploaded into CMMC eMASS.

DCMA DIBCAC maintains records for a period of six years of monitoring, education, training, technical knowledge, skills, experience, and authorization of each member of its personnel involved in inspection activities and working papers generated from Level 3 Certification Assessments.

Use of Information Technology

CMMC assessment data and results are collected using information technology. C3PAOs and DCMA DIBCAC electronically upload assessment data and results into the CMMC instantiation of eMASS (addressed in a separate CMMC eMASS ICR for the 32 CFR part 170 CMMC Program final rule). The CMMC instantiation of eMASS electronically transfers certification results to SPRS. For Level 1 and 2 self-assessments, OSAs upload their assessment data directly into SPRS.

Use of the CMMC instantiation of eMASS provides DoD visibility into the cybersecurity posture of the defense contractor supply chain and is the mechanism to generate reports on the health of the CMMC Ecosystem. SPRS is DoD's authoritative source for supplier and product performance information. Use of this electronic system to collect CMMC information eliminates the need for contractors to respond directly to multiple DoD requiring activities. SPRS serves as a single repository for Government access to CMMC assessment results. Modifications to information collections in SPRS will be addressed in the 48 CFR part 204 CMMC Acquisition final rule.

Non-duplication

The information obtained through this collection is unique and is not already available for use or adaptation from another cleared source.

Burden on Small Businesses

For Level 1 and 2 self-assessments, OSAs must report annually and triennially, respectively. Level 2 and Level 3 certification assessments must be conducted every three years by a C3PAO or DCMA DIBCAC, respectively. At all levels, an annual affirmation is required. In all cases, the burden applied to small business is the minimum consistent with applicable laws, Executive orders, regulations, and prudent business practices.

A C3PAO, although not a defense contractor, may also be a small business. Efforts to minimize the burden on C3PAOs include the electronic collection of data using the CMMC instantiation of eMASS and providing Microsoft Excel spreadsheet templates.

Less Frequent Collection

CMMC certifications last up to three years. The assessment frequency for each level was determined by the DoD based on the sensitivity of information processed, stored, or transmitted by the OSA at each level.

DoD Program Managers use the CMMC information in SPRS to confirm the validity status of an OSA's CMMC self-assessment or certification assessment prior to contract award. Rather than taking a contract-by-contract approach to securing Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), the OSA may obtain multiple contracts

with a single CMMC self-assessment or certification assessment, thereby reducing the cost to both DoD and industry.

Consultation and Public Comments

The Department consulted with members of the DIB Sector Coordinating Council (SCC), and government organizations including the DCMA DIBCAC and the Missile Defense Agency in determining what data to collect in the CMMC instantiation of eMASS.

The 60-Day *Federal Register* notice information is included in the preamble of the 32 CFR part 170 CMMC Program final rule for public comment.

The CMMC PMO is also working with a records management point-of-contact to ensure records produced from this information collection are retained and disposed of according to a NARA-approved records retention and disposition schedule. Records will be treated as permanent until the appropriate schedule is identified or approved.

PART A & B: Respondent Burden and its Labor Costs

The Level 1 and Level 2 self-assessment information collection reporting and recordkeeping requirements for the CMMC Program will be included in a modification of an existing DFARS collection approved under OMB Control Number 0750-0004, Assessing Contractor Implementation of Cybersecurity Requirements. Modifications to this DFARS collection will be addressed as part of the 48 part 204 CMMC Acquisition final rule.

The public burden costs associated with Level 2 and Level 3 certification assessment information collection reporting and recordkeeping requirements for the CMMC Program are addressed here, except for the eMASS reporting requirements which will be addressed as part of a separate CMMC eMASS ICR for the 32 CFR part 170 CMMC Program final rule. Respondent burden and cost for these information collection reporting and recordkeeping requirements are as follows:

Table 34 – Public Respondent Burden and Labor Costs for CMMC Level 2 and Level 3 Certification Assessment

Collection Instrument and Rule Citation	Entity Type	Number of Responses [68]	Hours per Response [69]	Burden Hours	Hourly Rate [70]	Burden Per Response	Total Burden
Level 2 Certification Assessment § 170.17(a)	OSC (& hired C3PAO [71]) - Small	8,098	417.83	3,383,587.34	$239.89	$100,233	$811,688,767
	OSC (& hired C3PAO [71]) - Other Than Small	2,844	833.83	2,371,412.52	$131.44	$109,599	$311,698,462
Level 3 Certification Assessment § 170.18(a)	OSC - Small	190	42.08	7,995.20	$170.48	$ 7,174	$1,363,022
	OSC - Other Than Small	23	384.08	8,833.84	$ 94.53	$36,307	$ 835,063

Respondent Costs Other Than Burden Hour Costs

Non-Recurring and Recurring Engineering estimated costs are included for Level 3 certification assessments. Non-Recurring Engineering reflects a one-time cost consisting of hardware, software, and the associated labor to implement the same. Recurring Engineering reflects annually recurring fees and associated labor for technology refresh. The estimated amounts below are average annual amounts for all entities as indicated.

[68] Respondent is equivalent to an entity; an entity provides one response annually.

[69] Hours per Response represents the estimated burden hours to complete the indicated assessment.

[70] Hourly Rate represents a composite hourly rate derived from the detailed type of labor and associated rates estimated in the CMMC cost estimate model.

[71] The entity type refers to the size of the OSC as either Small or Other Than Small; the entity type does not refer to the size of the C3PAO.

Table 35 – Respondent Costs Other Than Burden

Rule Citation	Collection Requirement	Entity Type	Non-Recurring Cost	Recurring Cost	Total Costs
§ 170.18(a)					$ 606,100,000
	Level 3 Certification	OSC - Small OSC - Other Than Small	$ 513,000,000 $ 485,300,000	$ 93,100,000 $ 94,760,000	$ 580,060,000
	TOTAL				**$ 1,186,160,000**

Travel costs for C3PAO assessors may represent an additional cost for respondents.

Cost to the Federal Government

The government burden costs associated with Level 3 certification assessment information collection reporting and recordkeeping requirements for the CMMC Program are addressed here, except for the eMASS reporting requirements which will be addressed as part of a separate CMMC eMASS ICR for the 32 CFR part 170 CMMC Program rule. Respondent burden and cost for these information collection reporting and recordkeeping requirements are as follows:

Table 36 – Government Respondent Burden and Labor Costs for Level 3 Certification Assessment

Collection [64] Instrument and Rule Citation	Entity Type	Number of Responses [72]	Hours per Response[65]	Burden Hours	Hourly Rate[74]	Burden Per Response	Total Burden
Level 3 Certification Assessment § 170.18(a)	OSC (& DCMA DIBCAC[66]) - Small	190	117.75	22,372.50	$108.47	$ 12,772	$2,426,745
	OSC (& DCMA DIBCAC[75]) - Other Than Small	23	435.75	10,022.25	$ 81.01	$35,300	$ 811,902

Steps Taken to Minimize Economic Impact

DoD took aggressive steps to minimize the economic impact of this program by streamlining requirements to reduce the number of steps in the process and the number of requirements that needed to be met, and reduced the requirement of 100% compliance, and the number of thirdparty assessments required.

To further elaborate the DoD established a review body that evaluated the CMMC Program to ensure it was meeting the programmatic requirements to secure Controlled Unclassified Information within the non-Federal networks of the Defense Industrial Base. A special independent team was established to review and provide recommendations on improving the program.

The DoD determined that the CMMC program should only employ the Cybersecurity Standards prescribed by the NIST SP 800-171 that had been required for defense contractors since 2017 as implemented by the DFARS clause 252.204-7012, which resulted in the removal of 20 requirements aligned with cybersecurity maturity. The ESG also recommended simplifying the program structure to require only 3 levels of certification vice the original 5. The program further determined that certifications should not be required at CMMC Level 1 and that self-assessment with an annual affirmation was sufficient for this level. Level 2 CMMC was

[64] Respondent is equivalent to an entity; an entity provides one response annually.

[65] Hours per Response represents the estimated Government burden hours to complete the indicated assessment.

[74] The Hourly Rate represents a composite hourly rate derived from the detailed type of Government labor and associated rates estimated in the CMMC cost estimate model.

[66] The entity type refers to the size of the OSC as either Small or Other Than Small; the entity type does not refer to the size of DCMA DIBCAC.

further evaluated and determined that bifurcation of this level was appropriate, and some CUI would only require a Level 2 self-assessment with annual affirmation, which further reduced the costs for the program. Further the ESG recommended that Plans of Actions and Milestones (POA&Ms) for lower-level requirements that were not met be allowed for a limited period of time. This rule was updated to allow POA&Ms for no more than 180 days to give contractors the ability to achieve contract award without being fully compliant with all requirements of NIST SP 800-171 R2.

And, in another effort to minimize the economic impact the program developed a Phase-in approach to incrementally implement CMMC in four phases over 4 years, with the first year being focused on Self-assessment and compliance with NIST SP 800-171 R2 giving contractors more time to implement the requirements already required in their contracts since 2017. A CMMC waiver process was also included in the program which allows DoD the discretion to waive CMMC Program requirements to a procurement or class of procurements in advance of the solicitation in accordance with all applicable policies, procedures, and approval requirements. This waiver would allow contract award and the contractor would be expected to achieve compliance and certification at a defined time post-award.

The DoD is employing a phased approach to the CMMC rollout to reduce implementation risk. DoD expects that the public has utilized the lead-time prior to the publication of this rule to prepare for CMMC implementation. CMMC Program requirements make no changes to existing policies for information security requirements implemented by the DoD.

The phased CMMC implementation plan described in § 170.3(e) is intended to address CMMC ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements. DoD has updated the rule to add an additional six months to the Phase 1 timeline. Phase 2 will start one calendar year after the start of Phase 1, and Phase 3 will start one calendar year after the start of Phase 2. As with all DoD programs, the Department intends to effectively oversee CMMC, and take appropriate actions needed to manage its effective implementation.

Alternatives.

DoD considered and adopted several alternatives during the development of this rule that reduce the burden on defense contractors and still meet the objectives of the rule. These alternatives include:

Maintaining status quo and leveraging only the current requirements implemented in DFARS provision 252.204-7019 and DFARS clause 252.204-7020 requiring defense contractors and offerors to self-assess compliance and utilizing the DoD Assessment Methodology and entering a Basic Summary Score in SPRS.

Revising CMMC to reduce the burden for small businesses and contractors who do not process, store, or transmit CUI by eliminating the requirement to hire a C3PAO and instead allow selfassessment with affirmation to maintain compliance at CMMC Level 1, and allowing triennial self-assessment with an annual affirmation to maintain compliance for some CMMC Level 2 programs.

Exempting contracts and orders exclusively for the acquisition of commercially available offthe-shelf items; and,

Implementing a phased implementation for CMMC.

In addition, the Department took into consideration the timing of the requirement to achieve a specified CMMC level: (1) at time of proposal or offer submission, (2) after contract award, (3) at the time of contract award, or (4) permitting government Program Managers to seek approval to waive inclusion of CMMC requirements in solicitations and resulting contracts that involve disclosure or creation of FCI or CUI as part of the contract effort. Such waivers will be requested and approved by DoD in accordance with internal policies, procedures, and approval requirements.

The Department ultimately adopted alternatives (3) and (4). The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC level after the release of the solicitation and

before contract award. The drawback of alternative 2 (after contract award) is the increased risk to the Department with respect to the costs, program schedule, and uncertainty in the event the contractor is unable to achieve the required CMMC level in a reasonable amount of time given its current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI.

CMMC does not require implementation of any additional security protection requirements beyond those identified in current FAR clause 52.204-21 and in NIST SP 800-171 R2 for CMMC Levels 1 and Level 2, respectively. CMMC Level 3 requirements are new and based upon NIST SP 800-172 Feb2021.

Steps Taken to Minimize Additional Cost of Credit

The DoD is not a "covered agency" under 5 U.S.C. 604.

E. Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

Sections of this rule contain information collection requirements. As required by the Paperwork Reduction Act (44 U.S.C. Chapter 35), DoD has submitted information collection packages to the Office of Management and Budget for review and approval. The titles and proposed OMB control numbers are as follows.

- Cybersecurity Maturity Model Certification (CMMC) Enterprise Mission Assurance Support-Service (eMASS) Instantiation Information Collection (OMB control number 0704-
0676).
- Cybersecurity Maturity Model Certification (CMMC) Program Reporting and Recordkeeping Requirements Information Collection (OMB Control Number 0704-0677).

In the proposed rule, DoD invited comments on these information collection requirements and the paperwork burden associated with this rule. Five comments were received on the information clearance packages that were not applicable to the information collection requirements; however, the comments were applicable to other aspects of the rule, and they are addressed in the comments section of this preamble. There were no changes to paperwork burden included in the proposed rule that published December 26, 2023 (88 FR 89058) based on public comments received. To review these collections —including all background materials— please visit at https://www.reginfo.gov/public/do/PRAMain and use the search function to enter either the title of the collection or the OMB Control Number.

F. Executive Order 13132, "Federalism"

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a final rule that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. This final rule will not have a substantial effect on State and local governments.

G. Executive Order 13175, "Consultation and Coordination with Indian Tribal Governments"

Executive Order 13175 establishes certain requirements that an agency must meet when it promulgates a final rule that imposes substantial direct compliance costs on one or more Indian Tribes, preempts Tribal law, or effects the distribution of power and responsibilities between the Federal Government and Indian Tribes. This final rule will not have a substantial effect on Indian Tribal governments.

List of Subjects in 32 CFR Part 170

Certification, CMMC, CMMC Levels, CMMC Program, contracts, Controlled Unclassified Information, cybersecurity, Federal Contract Information, Government procurement, Incorporation by reference.

Accordingly, the Department of Defense adds 32 CFR part 170 to read as follows:

PART 170 - CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Subpart A—General Information

Sec.

170.1 Purpose.

Authority: 5 U.S.C. 301; Sec. 1648, Pub. L. 116-92, 133 Stat. 1198.
Subpart A—General Information.
§ 170.1 Purpose.

(a) This part describes the Cybersecurity Maturity Model Certification (CMMC) Program of the Department of Defense (DoD) and establishes requirements for defense contractors and subcontractors to implement prescribed cybersecurity standards for safeguarding Federal
Contract Information (FCI) and Controlled Unclassified Information (CUI). This part (the CMMC Program) also establishes requirements for conducting an assessment of compliance with the applicable prescribed cybersecurity standard for contractor information systems that: process, store, or transmit FCI or CUI; provide security protections for systems which process, store, or transmit CUI; or are not logically or physically isolated from systems which process, store, or transmit CUI.

(b) The CMMC Program provides DoD with a viable means of conducting the volume of assessments necessary to verify contractor and subcontractor implementation of required cybersecurity requirements.

(c) The CMMC Program is designed to ensure defense contractors are properly safeguarding FCI and CUI that is processed, stored, or transmitted on defense contractor information systems. FCI and CUI must be protected to meet evolving threats and safeguard nonpublic, unclassified information that supports and enables the warfighter. The CMMC Program provides a consistent methodology to assess a defense contractor's implementation of required cybersecurity requirements. The CMMC Program utilizes the security standards set forth in the 48 CFR 52.204-21; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Basic Safeguarding of Covered Contractor Information Systems,* Revision 2, February 2020 (includes updates as of January 28, 2021) (NIST SP 800-171 R2); and selected requirements from the NIST SP 800-172, *Enhanced Security Requirements for*

Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800171, February 2021 (NIST SP 800-172 Feb2021), as applicable (see table 1 to § 170.14(c)(4) for requirements, see § 170.2 for availability of NIST publications).

(d) The CMMC Program balances the need to safeguard FCI and CUI and the requirement to share information appropriately with defense contractors in order to develop capabilities for the DoD. The CMMC Program is designed to ensure implementation of cybersecurity practices for defense contractors and to provide DoD with increased assurance that FCI and CUI information will be adequately safeguarded when residing on or transiting contractor information systems.

(e) The CMMC Program creates no right or benefit, substantive or procedural, enforceable by law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

§ 170.2 Incorporation by reference.

Certain material is incorporated by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. Material approved for incorporation by reference (IBR) is available for inspection at the Department of Defense (DoD) and at the National Archives and Records Administration (NARA). Contact DoD online: https://DoDcio.defense.gov/CMMC/; email: osd.mc-alex.DoD-cio.mbx.cmmc-rule@mail.mil; or phone: (202) 770-9100. For information on the availability of this material at NARA, visit: www.archives.gov/federal-register/cfr/ibr-locations or email: fr.inspection@nara.gov. The material may be obtained from the following sources:

(a) National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899; phone: (301) 975-8443; website: https://csrc.nist.gov/publications/.

(1) FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006 (FIPS PUB 200 Mar2006); IBR approved for § 170.4(b).

(2) FIPS PUB 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, January 2022 (FIPS PUB 201-3 Jan2022); IBR approved for § 170.4(b).

(3) SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018 (NIST SP 800-37 R2); IBR approved for § 170.4(b).

(4) SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011 (NIST SP 800-39 Mar2011); IBR approved for § 170.4(b).

(5) SP 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5, September 2020 (includes updates as of December 10, 2020) (NIST SP 800-53 R5);
IBR approved for § 170.4(b).

(6) SP 800-82r3, Guide to Operational Technology (OT) Security, September 2023 (NIST SP 800-82r3); IBR approved for § 170.4(b).

(7) SP 800-115, Technical Guide to Information Security Testing and Assessment, September 2008 (NIST SP 800-115 Sept2008); IBR approved for § 170.4(b).

(8) SP 800-160, Volume 2, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, Revision 1, December 2021 (NIST SP 800-160 V2R1); IBR approved for § 170.4(b).

(9) SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Revision 2, February 2020 (includes updates as of January 28, 2021), (NIST
SP 800-171 R2); IBR approved for §§ 170.4(b) and 170.14(a) through (c).

(10) SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, June 2018 (NIST SP 800-171A Jun2018); IBR approved for §§ 170.11(a), 170.14(d), 170.15(c), 170.16(c), 170.17(c), and 170.18(c).

(11) SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171, February 2021 (NIST SP 800-172 Feb2021); IBR approved for §§ 170.4(b), 170.5(a), and 170.14(a) and (c).

(12) SP 800-172A, Assessing Enhanced Security Requirements for Controlled Unclassified Information, March 2022 (NIST SP 800-172A Mar2022); IBR approved for §§ 170.4(b), 170.14(d), and 170.18(c).

(b) International Organization for Standardization (ISO) Chemin de Blandonnet 8, CP 401 - 1214 Vernier, Geneva, Switzerland; phone: +41 22 749 01 11; website: www.iso.org/popular-standards.html.

(1) ISO/IEC 17011:2017(E), Conformity assessment – Requirements for accreditation bodies accrediting conformity assessment bodies, Second edition, November 2017 (ISO/IEC 17011:2017(E)); IBR approved for §§ 170.8(b)(3), 170.9(b)(13), and 170.10(b)(4).

(2) ISO/IEC 17020:2012(E), Conformity assessment – Requirement for the operation of various types of bodies performing inspection, Second edition, March 1, 2012 (ISO/IEC 17020:2012(E)); IBR approved for §§ 170.8(a), (b)(1), (b)(3) and 170.9(b)(2) and (b)(13).

(3) ISO/IEC 17024:2012(E), Conformity assessment – General requirements for bodies operating certification of persons, second edition, July 1, 2012 (ISO/IEC 17024:2012(E)); IBR approved for §§ 170.8(b)(2) and 170.10(a) and (b)(4), (7), and (8).

Note 1 to paragraph (b): The ISO/IEC standards incorporated by reference in this part may be viewed at no cost in "read only" format at https://ibr.ansi.org.

§ 170.3 Applicability.

(a) The requirements of this part apply to:

(1) All DoD contract and subcontract awardees that will process, store, or transmit information, in performance of the DoD contract, that meets the standards for FCI or CUI on contractor information systems; and,

(2) Private-sector businesses or other entities comprising the CMMC Assessment and Certification Ecosystem, as specified in subpart C of this part.

(b) The requirements of this part do not apply to Federal information systems operated by contractors or subcontractors on behalf of the Government.

(c) CMMC Program requirements apply to all DoD solicitations and contracts pursuant to which a defense contractor or subcontractor will process, store, or transmit FCI or CUI on unclassified contractor information systems, including those for the acquisition of commercial items (except those exclusively for COTS items) valued at greater than the micro-purchase threshold except under the following circumstances:

(1) The procurement occurs during Implementation Phase 1, 2, or 3 as described in paragraph (e) of this section, in which case CMMC Program requirements apply in accordance with the requirements for the relevant phase-in period; or

(2) Application of CMMC Program requirements to a procurement or class of procurements may be waived in advance of the solicitation at the discretion of DoD in accordance with all applicable policies, procedures, and approval requirements.

(d) DoD Program Managers or requiring activities are responsible for selecting the CMMC Status that will apply for a particular procurement or contract based upon the type of information, FCI or CUI, that will be processed on, stored on, or transmitted through a contractor information system. Application of the CMMC Status for subcontractors will be determined in accordance with § 170.23.

(e) DoD is utilizing a phased approach for the inclusion of CMMC Program requirements in solicitations and contracts. Implementation of CMMC Program requirements will occur over four (4) phases:

(1) *Phase 1*. Begins on the effective date of the complementary 48 CFR part 204 CMMC Acquisition final rule. DoD intends to include the requirement for CMMC Statuses of Level 1 (Self) or Level 2 (Self) for all applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, include the requirement for CMMC Status of

Level 1 (Self) or Level 2 (Self) for applicable DoD solicitations and contracts as a condition to exercise an option period on a contract awarded prior to the effective date. DoD may also, at its discretion, include the requirement for CMMC Status of Level 2 (C3PAO) in place of the Level 2 (Self) CMMC Status for applicable DoD solicitations and contracts.

(2) *Phase 2*. Begins one calendar year following the start date of Phase 1. In addition to Phase 1 requirements, DoD intends to include the requirement for CMMC Status of Level 2 (C3PAO) for applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, delay the inclusion of requirement for CMMC Status of Level 2 (C3PAO) to an option period instead of as a condition of contract award. DoD may also, at its discretion, include the requirement for CMMC Status of Level 3 (DIBCAC) for applicable DoD solicitations and contracts.

(3) *Phase 3*. Begins one calendar year following the start date of Phase 2. In addition to Phase 1 and 2 requirements, DoD intends to include the requirement for CMMC Status of Level 2 (C3PAO) for all applicable DoD solicitations and contracts as a condition of contract award and as a condition to exercise an option period on a contract awarded after the effective date. DoD intends to include the requirement for CMMC Status of Level 3 (DIBCAC) for all applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, delay the inclusion of requirement for CMMC Status of Level 3 (DIBCAC) to an option period instead of as a condition of contract award.

(4) *Phase 4, full implementation*. Begins one calendar year following the start date of Phase 3. DoD will include CMMC Program requirements in all applicable DoD solicitations and contracts including option periods on contracts awarded prior to the beginning of Phase 4.

§ 170.4 Acronyms and definitions.

(a) *Acronyms*. Unless otherwise noted, the following acronyms and their terms are for the purposes of this part.

AC	Access Control
APT	Advanced Persistent Threat
AT	Awareness and Training
C3PAO	CMMC Third-Party Assessment Organization
CA	Security Assessment
CAICO	CMMC Assessors and Instructors Certification Organization
CAGE	Commercial and Government Entity
CCA	CMMC-Certified Assessor
CCI	CMMC-Certified Instructor
CCP	CMMC-Certified Professional
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CM	Configuration Management

CMMC	Cybersecurity Maturity Model Certification
CMMC PMO	CMMC Program Management Office
CNC	Computerized Numerical Control
CoPC	Code of Professional Conduct
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
DCMA	Defense Contract Management Agency
DD	Represents any two-character CMMC Domain acronym
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIBCAC	DCMA's Defense Industrial Base Cybersecurity Assessment Center
DoD	Department of Defense
DoDI	Department of Defense Instruction
eMASS	Enterprise Mission Assurance Support Service
ESP	External Service Provider
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
FedRAMP	Federal Risk and Authorization Management Program
GFE	Government Furnished Equipment
IA	Identification and Authentication
ICS	Industrial Control System
IIoT	Industrial Internet of Things
IoT	Internet of Things
IR	Incident Response
IS	Information System

IEC	International Electrotechnical Commission
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
IT	Information Technology
L#	CMMC Level Number
MA	Maintenance
MP	Media Protection
MSSP	Managed Security Service Provider
NARA	National Archives and Records Administration
NAICS	North American Industry Classification System
NIST	National Institute of Standards and Technology
N/A	Not Applicable
ODP	Organization-Defined Parameter
OSA	Organization Seeking Assessment
OSC	Organization Seeking Certification
OT	Operational Technology
PI	Provisional Instructor
PIEE	Procurement Integrated Enterprise Environment
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
POA&M	Plan of Action and Milestones
PRA	Paperwork Reduction Act
RM	Risk Management
SAM	System of Award Management
SC	System and Communications Protection
SCADA	Supervisory Control and Data Acquisition

SI	System and Information Integrity
SIEM	Security Information and Event Management
SP	Special Publication
SPD	Security Protection Data
SPRS	Supplier Performance Risk System
SSP	System Security Plan

(b) *Definitions*. Unless otherwise noted, these terms and their definitions are for the purposes of this part.

Access Control (AC) means the process of granting or denying specific requests to obtain and use information and related information processing services; and/or entry to specific physical facilities (e.g., Federal buildings, military establishments, or border crossing entrances), as defined in FIPS PUB 201-3 Jan2002 (incorporated by reference, see § 170.2).

Accreditation means a status pursuant to which a CMMC Assessment and Certification Ecosystem member (person or organization), having met all criteria for the specific role they perform including required ISO/IEC accreditations, may act in that role as set forth in § 170.8 for the Accreditation Body and § 170.9 for C3PAOs. (CMMC-custom term)

Accreditation Body is defined in § 170.8 and means the one organization DoD contracts with to be responsible for authorizing and accrediting members of the CMMC Assessment and Certification Ecosystem, as required. The Accreditation Body must be approved by DoD. At any given point in time, there will be only one Accreditation Body for the DoD CMMC Program. (CMMC-custom term)

Advanced Persistent Threat (APT) means an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period-of-time, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives, as is defined in NIST SP 800-39 Mar2011 (incorporated by reference, see § 170.2).

Affirming Official means the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations. (CMMC-custom term)

Assessment means the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization, as defined in §§ 170.15 through 170.18. (CMMC-custom term)

(i) *Level 1 self-assessment* is the term for the activity performed by an OSA to evaluate its own information system when seeking a CMMC Status of Level 1 (Self).

(ii) *Level 2 self-assessment* is the term for the activity performed by an OSA to evaluate its own information system when seeking a CMMC Status of Level 2 (Self).

(iii) *Level 2 certification assessment* is the term for the activity performed by a C3PAO to evaluate the information system of an OSC when seeking a CMMC Status of Level 2 (C3PAO).

(iv) *Level 3 certification assessment* is the term for the activity performed by the DCMA DIBCAC to evaluate the information system of an OSC when seeking a CMMC Status of Level 3 (DIBCAC).

(v) *POA&M closeout self-assessment* is the term for the activity performed by an OSA to evaluate only the NOT MET requirements that were identified with POA&M during the initial assessment, when seeking a CMMC Status of Final Level 2 (Self).

(vi) *POA&M closeout certification assessment* is the term for the activity performed by a C3PAO or DCMA DIBCAC to evaluate only the NOT MET requirements that were identified with POA&M during the initial assessment, when seeking a CMMC Status of Final Level 2 (C3PAO) or Final Level 3 (DIBCAC) respectively.

Assessment Findings Report means the final written assessment results by the third-party or government assessment team. The Assessment Findings Report is submitted to the OSC and to the DoD via CMMC eMASS. (CMMC-custom term)

Assessment objective means a set of determination statements that, taken together, expresses the desired outcome for the assessment of a security requirement. Successful implementation of the corresponding CMMC security requirement requires meeting all applicable assessment objectives defined in NIST SP 800–171A Jun2018 (incorporated by reference, see § 170.2) or NIST SP 800-172A Mar2022 (incorporated by reference, see § 170.2). (CMMC-custom term)

Assessment Team means participants in the Level 2 certification assessment (CMMC Certified Assessors and CMMC Certified Professionals) or the Level 3 certification assessment (DCMA DIBCAC assessors). This does not include the OSC participants preparing for or participating in the assessment. (CMMC-custom term)

Asset means an item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns, as defined in NIST SP 800-160 V2R1 (incorporated by reference, see § 170.2).

Asset Categories means a grouping of assets that process, store or transmit information of similar designation, or provide security protection to those assets. (CMMC-custom term)

Authentication is defined in FIPS PUB 200 Mar2006 (incorporated by reference, see § 170.2).

Authorized means an interim status during which a CMMC Ecosystem member (person or organization), having met all criteria for the specific role they perform other than the required ISO/IEC accreditations, may act in that role for a specified time as set forth in § 170.8 for the Accreditation Body and § 170.9 for C3PAOs. (CMMC-custom term)

Capability means a combination of mutually reinforcing controls implemented by technical means, physical means, and procedural means. Such controls are typically selected to achieve a common information security or privacy purpose, as defined in NIST SP 800-37 R2 (incorporated by reference, see § 170.2).

Cloud Service Provider (CSP) means an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, ondemand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This definition is based on the definition for cloud computing in NIST SP 800-145 Sept2011. (CMMC-custom term)

CMMC Assessment and Certification Ecosystem means the people and organizations described in subpart C of this part. This term is sometimes shortened to CMMC Ecosystem. (CMMC-custom term)

CMMC Assessment Scope means the set of all assets in the OSA's environment that will be assessed against CMMC security requirements. (CMMC-custom term)

CMMC Assessor and Instructor Certification Organization (CAICO) is defined in § 170.10 and means the organization responsible for training, testing, authorizing, certifying, and recertifying CMMC certified assessors, certified instructors, and certified professionals. (CMMC-custom term)

CMMC Instantiation of eMASS means a CMMC instance of the Enterprise Mission Assurance Support Service (eMASS), a government owned and operated system. (CMMCcustom term)

CMMC Security Requirements means the 15 Level 1 requirements listed in the 48 CFR 52.204-21(b)(1), the 110 Level 2 requirements from NIST SP 800-171 R2 (incorporated by reference, see § 170.2), and the 24 Level 3 requirements selected from NIST SP 800-172 Feb2021 (incorporated by reference, see § 170.2).

CMMC Status is the result of meeting or exceeding the minimum required score for the corresponding assessment. The CMMC Status of an OSA information system is officially stored in SPRS and additionally presented on a Certificate of CMMC Status, if the assessment was conducted by a C3PAO or DCMA DIBCAC. The potential CMMC Statuses are outlined in the paragraphs that follow. (CMMC-custom term)

(i) *Final Level 1 (Self)* is defined in § 170.15(a)(1) and (c)(1). (CMMC-custom term)

(ii) *Conditional Level 2 (Self)* is defined in § 170.16(a)(1)(ii). (CMMC-custom term)

(iii) *Final Level 2 (Self)* is defined in § 170.16(a)(1)(iii). (CMMC-custom term)

(iv) *Conditional Level 2 (C3PAO)* is defined in § 170.17(a)(1)(ii). (CMMC-custom term)

(v) *Final Level 2 (C3PAO)* is defined in § 170.17(a)(1)(iii). (CMMC-custom term) (vi) *Conditional Level 3 (DIBCAC)* is defined in § 170.18(a)(1)(ii). (CMMC-custom term)

(vii) *Final Level 3 (DIBCAC)* is defined in § 170.18(a)(1)(iii). (CMMC-custom term)

CMMC Status Date means the date that the CMMC Status results are submitted to SPRS or the CMMC instantiation of eMASS, as appropriate. The date of the Conditional CMMC Status will remain as the CMMC Status Date after a successful POA&M closeout. A new date is not set for a Final that follows a Conditional. (CMMC-custom term)

CMMC Third-Party Assessment Organization (C3PAO) means an organization that has been authorized or accredited by the Accreditation Body to conduct Level 2 certification assessments and has the roles and responsibilities identified in § 170.9. (CMMC-custom term)

Contractor is defined in 48 CFR 3.502-1.

Contractor Risk Managed Assets are defined in table 3 to § 170.19(c)(1). (CMMCcustom term)

Controlled Unclassified Information (CUI) is defined in 32 CFR 2002.4(h).

Controlled Unclassified Information (CUI) Assets means assets that can process, store, or transmit CUI. (CMMC-custom term)

DCMA DIBCAC High Assessment means an assessment that is conducted by Government personnel in accordance with NIST SP 800-171A Jun2018 and leveraging specific guidance in the DoD Assessment Methodology that:

(i) Consists of:

(A) A review of a contractor's Basic Assessment;

(B) A thorough document review;

(C) Verification, examination, and demonstration of a contractor's system security plan to validate that NIST SP 800-171 R2 security requirements have been implemented as described in the contractor's system security plan; and

(D) Discussions with the contractor to obtain additional information or clarification, as needed; and

(ii) Results in a confidence level of "High" in the resulting score. (Source: 48 CFR 252.204-7020).

Defense Industrial Base (DIB) is defined in 32 CFR 236.2.

DoD Assessment Methodology (DoDAM) documents a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800-171 R2, a requirement for compliance with 48 CFR 252.204-7012. (Source: DoDAM Version 1.2.1)

Enduring Exception means a special circumstance or system where remediation and full compliance with CMMC *s*ecurity *r*equirements is not feasible. Examples include systems required to replicate the configuration of 'fielded' systems, medical devices, test equipment, OT, and IoT. No operational plan of action is required but the circumstance must be documented within a system security plan. Specialized Assets and GFE may be enduring exceptions. (CMMC-custom term)

Enterprise means an organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).

External Service Provider (ESP) means external people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. (CMMC-custom term)

Federal Contract Information (FCI) is defined in 48 CFR 4.1901.

Government Furnished Equipment (GFE) has the same meaning as "governmentfurnished property" as defined in 48 CFR 45.101.

Industrial Control Systems (ICS) means a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations that are often found in the industrial sectors and critical infrastructures, such as Programmable Logic Controllers (PLC). An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy), as defined in NIST SP 800-82r3 (incorporated by reference, see § 170.2).

Information System (IS) is defined in NIST SP 800-171 R2 (incorporated by reference, see § 170.2).

Internet of Things (IoT) means the network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information, as defined in NIST SP 800-172A Mar2022 (incorporated by reference, see § 170.2).

Operational plan of action as used in security requirement CA.L2-3.12.2, means the formal artifact which identifies temporary vulnerabilities and temporary deficiencies (e.g., necessary information system updates, patches, or reconfiguration as threats evolve) in implementation of requirements and documents how they will be mitigated, corrected, or eliminated. The OSA defines the format (e.g., document, spreadsheet, database) and specific content of its operational plan of action. An operational plan of action does not identify a timeline for remediation and is not the same as a POA&M, which is associated with an assessment for remediation of deficiencies that must be completed within 180 days. (CMMCcustom term)

Operational Technology (OT) means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms, as defined in NIST SP 800-160 V2R1 (incorporated by reference, see § 170.2).

Organization-defined means as determined by the OSA except as defined in the case of

Organization-Defined Parameter (ODP). (CMMC-custom term)

Organization-Defined Parameters (ODPs) means selected enhanced security requirements contain selection and assignment operations to give organizations flexibility in defining variable parts of those requirements, as defined in NIST SP 800-172A Mar2022 (incorporated by reference, see § 170.2).

Note 1 to *ODPs*: The organization defining the parameters is the DoD.

Organization Seeking Assessment (OSA) means the entity seeking to undergo a selfassessment or certification assessment for a given information system for the purposes of achieving and maintaining any CMMC Status. The term OSA includes all Organizations Seeking Certification (OSCs). (CMMC-custom term)

Organization Seeking Certification (OSC) means the entity seeking to undergo a certification assessment for a given information system for the purposes of achieving and maintaining the CMMC Status of Level 2 (C3PAO) or Level 3 (DIBCAC). An OSC is also an OSA. (CMMC-custom term)

Out-of-Scope Assets means assets that cannot process, store, or transmit CUI because they are physically or logically separated from information systems that do process, store, or transmit CUI, or are inherently unable to do so; except for assets that provide security protection for a CUI asset (see the definition for *Security Protection Assets*). (CMMC-custom term)

Periodically means occurring at a regular interval as determined by the OSA that may not exceed one year. (CMMC-custom term)

Personally Identifiable Information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).

Plan of Action and Milestones (POA&M) means a document that identifies tasks needing 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 NIST SP 800-115 Sept2008 (incorporated by reference, see § 170.2).

Prime Contractor is defined in 48 CFR 3.502-1.

Process, store, or transmit means data can be used by an asset (e.g., accessed, entered, edited, generated, manipulated, or printed); data is inactive or at rest on an asset (e.g., located on electronic media, in system component memory, or in physical format such as paper documents); or data is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods). (CMMC-custom term)

Restricted Information Systems means systems (and associated IT components comprising the system) that are configured based on government requirements (e.g., connected to something that was required to support a functional requirement) and are used to support a contract (e.g., fielded systems, obsolete systems, and product deliverable replicas). (CMMCcustom term)

Risk means a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of:

(i) The adverse impacts that would arise if the circumstance or event occurs; and

(ii) The likelihood of occurrence, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).

Risk Assessment means the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Risk Assessment is part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis, as defined in NIST SP 800-39 Mar2011 (incorporated by reference, see § 170.2).

Security Protection Assets (SPA) means assets providing security functions or capabilities for the OSA's CMMC Assessment Scope. (CMMC-custom term)

Security Protection Data (SPD) means data stored or processed by Security Protection Assets (SPA) that are used to protect an OSC's assessed environment. SPD is security relevant information and includes but is not limited to: configuration data required to operate an SPA, log files generated by or ingested by an SPA, data related to the configuration or vulnerability status of in-scope assets, and passwords that grant access to the in-scope environment. (CMMCcustom term)

Specialized Assets means types of assets considered specialized assets for CMMC: Government Furnished Equipment, Internet of Things (IoT) or Industrial Internet of Things (IIoT), Operational Technology (OT), Restricted Information Systems, and Test Equipment. (CMMC-custom term)

Subcontractor is defined in 48 CFR 3.502-1.

Supervisory Control and Data Acquisition (SCADA) means a generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated, as defined in NIST SP 800-82r3 (incorporated by reference, see § 170.2).

System Security Plan (SSP) means the formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The system security plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).

Temporary deficiency means a condition where remediation of a discovered deficiency is feasible, and a known fix is available or is in process. The deficiency must be documented in an operational plan of action. A temporary deficiency is not based on an 'in progress' initial implementation of a CMMC security requirement but arises after implementation. A temporary deficiency may apply during the initial implementation of a security requirement if, during rollout, specific issues with a very limited subset of equipment is discovered that must be separately addressed. There is no standard duration for which a temporary deficiency may be active. For example, FIPS-validated cryptography that requires a patch and the patched version is no longer the validated version may be a temporary deficiency. (CMMC-custom term)

Test Equipment means hardware and/or associated IT components used in the testing of products, system components, and contract deliverables. (CMMC-custom term)

User means an individual, or (system) process acting on behalf of an individual, authorized to access a system, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).

§ 170.5 Policy.

(a) Protection of FCI and CUI on contractor information systems is of paramount importance to the DoD and can directly impact its ability to successfully conduct essential missions and functions. It is DoD policy that defense contractors and subcontractors shall be required to safeguard FCI and CUI that is processed, stored, or transmitted on contractor information systems by applying specified security requirements. In addition, defense contractors and subcontractors may be required to implement additional safeguards defined in NIST SP 800-172 Feb2021 (incorporated by reference, see § 170.2), implementing DoD specified parameters to meet CMMC Level 3 security requirements (see table 1 to § 170.14(c)(4)). These additional requirements are necessary to protect CUI being processed, stored, or transmitted in contractor information systems, when designated by a requirement for CMMC Status of Level 3 (DIBCAC) as defined by a DoD program manager or requiring activity. In general, the Department will identify a requirement for a CMMC Status of Level 3

(DIBCAC) for solicitations and resulting contracts supporting its most critical programs and technologies.

(b) Program managers and requiring activities are responsible for identifying the CMMC Status that will apply to a procurement. Selection of the applicable CMMC Status will be based on factors including but not limited to:

(1) Criticality of the associated mission capability;

(2) Type of acquisition program or technology;

(3) Threat of loss of the FCI or CUI to be shared or generated in relation to the effort;

(4) Impacts from exploitation of information security deficiencies; and

(5) Other relevant policies and factors, including Milestone Decision Authority guidance.

(c) In accordance with the implementation plan described in § 170.3, CMMC Program requirements will apply to new DoD solicitations and contracts, and shall flow down to subcontractors who will process, store, or transmit FCI or CUI in performance of the subcontract, as described in § 170.23.

(d) In very limited circumstances, and in accordance with all applicable policies, procedures, and requirements, a Service Acquisition Executive or Component Acquisition Executive in the DoD, or as delegated, may elect to waive inclusion of CMMC Program requirements in a solicitation or contract. In such cases, contractors and subcontractors will remain obligated to comply with all applicable cybersecurity and information security requirements.

(e) The CMMC Program does not alter any separately applicable requirements to protect
FCI or CUI, including those requirements in accordance with 48 CFR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*, or covered defense information in accordance with 48 CFR 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, or any other applicable information protection requirements. The CMMC Program provides a means of verifying implementation of the security requirements set forth in 48 CFR 52.204-21, NIST SP 800-171 R2, and NIST SP 800-172 Feb2021, as applicable.

Subpart B—Government Roles and Responsibilities.

§ 170.6 CMMC PMO.

(a) The Office of the Department of Defense Chief Information Officer (DoD CIO) Office of the Deputy CIO for Cybersecurity (DoD CIO(CS)) provides oversight of the CMMC Program and is responsible for establishing CMMC assessment, accreditation, and training requirements as well as developing and updating CMMC Program policies and implementing guidance.

(b) The CMMC PMO is responsible for monitoring the CMMC AB's performance of roles assigned in this rule and acting as necessary to address problems pertaining to effective performance.

(c) The CMMC PMO retains, on behalf of the DoD CIO(CS), the prerogative to review decisions of the CMMC Accreditation Body as part of its oversight of the CMMC program and evaluate any alleged conflicts of interest purported to influence the CMMC Accreditation Body's objectivity.

(d) The CMMC PMO is responsible for sponsoring necessary DCSA activities including FOCI risk assessment and Tier 3 security background investigations for the CMMC Ecosystem members as specified in §§ 170.8(b)(4) and (5), 170.9(b)(3) through (5), 170.11(b)(3) and (4), and 170.13(b)(3) and (4).

(e) The CMMC PMO is responsible for investigating and acting upon indications that an active CMMC Status has been called into question. Indications that may trigger investigative evaluations include, but are not limited to, reports from the CMMC Accreditation Body, a C3PAO, or anyone knowledgeable of the security processes and activities of the OSA. Investigative evaluations include, but are not limited to, reviewing pertinent assessment information, and exercising the right to conduct a DCMA DIBCAC assessment of the OSA, as provided for under the 48 CFR 252.204-7020.

(f) If a subsequent DCMA DIBCAC assessment shows that adherence to the provisions of this rule and the required CMMC Status have not been achieved or maintained, the DIBCAC results will take precedence over any pre-existing CMMC Status recorded in SPRS, or its successor capability. The DoD will update SPRS to reflect that the OSA is out of compliance and does not meet DoD CMMC requirements. If the OSA is working on an active contract requiring CMMC compliance, then standard contractual remedies will apply.

§ 170.7 DCMA DIBCAC.

(a) DCMA DIBCAC assessors in support of the CMMC Program will:

(1) Complete CMMC Level 2 and Level 3 training.

(2) Conduct Level 3 certification assessments and upload assessment results into the CMMC instantiation of eMASS, or its successor capability.

(3) Issue Certificates of CMMC Status resulting from Level 3 certification assessments.

(4) Conduct Level 2 certification assessments of the Accreditation Body and prospective C3PAOs' information systems that process, store, and/or transmit CUI.

(5) Create and maintain a process for assessors to collect the list of assessment artifacts to include artifact names, their return value of the hashing algorithm, the hashing algorithm used, and upload that data into the CMMC instantiation of eMASS.

(6) As authorized and in accordance with all legal requirements, enter and track, OSC appeals and updated results arising from Level 3 certification assessment activities into the CMMC instantiation of eMASS.

(7) Retain all records in accordance with DCMA-MAN 4501-04.

(8) Conduct an assessment of the OSA, when requested by the CMMC PMO per §§ 170.6(e) and (f), as provided for under the 48 CFR 252.204-7019 and 48 CFR 252.204-7020.

(9) Identify assessments that meet the criteria in § 170.20 and verify that SPRS accurately reflects the CMMC Status.

(b) An OSC, the CMMC AB, or a C3PAO may appeal the outcome of its DCMA DIBCAC conducted assessment within 21 days by submitting a written basis for appeal with the requirements in question for DCMA DIBCAC consideration. Appeals may be submitted for review by visiting www.dcma.mil/DIBCAC for contact information, and a DCMA DIBCAC Quality Assurance Review Team will provide a written response or request additional supporting documentation.

Subpart C—CMMC Assessment and Certification Ecosystem.

§ 170.8 Accreditation Body.

(a) *Roles and responsibilities*. The Accreditation Body is responsible for authorizing and ensuring the accreditation of CMMC Third-Party Assessment Organizations (C3PAOs) in accordance with ISO/IEC 17020:2012(E) (incorporated by reference, see § 170.2) and all applicable authorization and accreditation requirements set forth. The Accreditation Body is responsible for establishing the C3PAO authorization requirements and the C3PAO Accreditation Scheme and submitting both for approval by the CMMC PMO. At any given point in time, there will be only one Accreditation Body for the DoD CMMC Program.

(b) *Requirements*. The CMMC Accreditation Body shall:

(1) Be US-based and be and remain a member in good standing of the Inter-American Accreditation Cooperation (IAAC) and become an International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA) signatory, with a signatory status scope of ISO/IEC 17020:2012(E) (incorporated by reference, see § 170.2).

(2) Be and remain a member in good standing of the International Accreditation Forum (IAF) with mutual recognition arrangement signatory status scope of ISO/IEC 17024:2012(E) (incorporated by reference, see § 170.2).

(3) Achieve and maintain full compliance with ISO/IEC 17011:2017(E) (incorporated by reference, see § 170.2) and complete a peer assessment by other ILAC signatories for competence in accrediting conformity assessment bodies to ISO/IEC 17020:2012(E) (incorporated by reference, see § 170.2), both within 24 months of DoD approval.

(i) Prior to achieving full compliance as set forth in this paragraph (b)(3), the Accreditation Body shall:

(A) Authorize C3PAOs who meet all requirements set forth in § 170.9 as well as administrative requirements as determined by the Accreditation Body to conduct Level 2 certification assessments and issue Certificates of CMMC Status to OSCs based on the assessment results.

(B) Require all C3PAOs to achieve and maintain the ISO/IEC 17020:2012(E) (incorporated by reference, see § 170.2) requirements within 27 months of authorization.

(ii) The Accreditation Body shall accredit C3PAOs, in accordance with ISO/IEC 17020:2012(E) (incorporated by reference, see § 170.2), who meet all requirements set forth in § 170.9 to conduct Level 2 certification assessments and issue Certificates of CMMC Status to OSCs based on the results.

(4) Ensure that the Accreditation Body's Board of Directors, professional staff, Information Technology (IT) staff, accreditation staff, and independent CMMC Certified Assessor staff complete a Tier 3 background investigation resulting in a determination of national security eligibility. This Tier 3 background investigation will not result in a security clearance and is not being executed for the purpose of government employment. The Tier 3 background investigation is initiated using the Standard Form (SF) 86 (www.gsa.gov/reference/forms/questionnaire-for-national-security-positions) and submitted by DoD CIO Security to Washington Headquarters Services (WHS) for coordination for processing by the Defense Counterintelligence and Security Agency (DCSA). These positions are designated as non-critical sensitive with a risk designation of "Moderate Risk" in accordance with 5 CFR 1400.201(b) and (d) and the investigative requirements of 5 CFR 731.106(c)(2).

(5) Comply with Foreign Ownership, Control or Influence (FOCI) by:

(i) Completing the Standard Form (SF) 328 (www.gsa.gov/reference/forms/certificatepertaining-to-foreign-interests), *Certificate Pertaining to Foreign Interests*, and submit it directly to Defense Counterintelligence and Security Agency (DCSA) and undergo a National Security Review with regards to the protection of controlled unclassified information based on the factors identified in 32 CFR 117.11(b) using the procedures outlined in 32 CFR 117.11(c). The Accreditation Body must receive a non-disqualifying eligibility determination by the CMMC PMO to be recognized by the Department of Defense.

(ii) Reporting any change to the information provided on its SF 328 by resubmitting the SF 328 to DCSA within 15 business days of the change being effective. A disqualifying eligibility determination, based on the results of the change, will result in the Accreditation Body losing its authorization or accreditation under the CMMC Program.

(iii) Identifying all prospective C3PAOs to the CMMC PMO. The CMMC PMO will sponsor the prospective C3PAO for a FOCI risk assessment conducted by the DCSA using the SF 328 as part of the authorization and accreditation processes.

(iv) Notifying prospective C3PAOs of the CMMC PMO's eligibility determination resulting from the FOCI risk assessment.

(6) Obtain a Level 2 certification assessment in accordance with the procedures specified in § 170.17(a)(1) and (c). This assessment, conducted by DCMA DIBCAC, shall meet all requirements for a Final Level 2 (C3PAO) but will not result in a CMMC Status of Level 2 (C3PAO). The Level 2 certification assessment process must be performed every three years.

(7) Provide all documentation and records in English.

(8) Establish, maintain, and manage an up-to-date list of authorized and accredited C3PAOs on a single publicly accessible website and provide the list of these entities and their status to the DoD through submission in the CMMC instantiation of eMASS.

(9) Provide the CMMC PMO with current data on C3PAOs, including authorization and accreditation records and status in the CMMC instantiation of eMASS. This data shall include the dates associated with the authorization and accreditation of each C3PAO.

(10) Provide the DoD with information about aggregate statistics pertaining to operations of the CMMC Ecosystem to include the authorization and accreditation status of C3PAOs or other information as requested.

(11) Provide inputs for assessor supplemental guidance to the CMMC PMO. Participate and support coordination of these and other inputs through DoD-led Working Groups.

(12) Ensure that all information about individuals is encrypted and protected in all Accreditation Body information systems and databases.

(13) Provide all plans that are related to potential sources of revenue, to include but not limited to: fees, licensing, processes, membership, and/or partnerships to the Department's CMMC PMO.

(14) Ensure that the CMMC Assessors and Instructors Certification Organization (CAICO) is compliant with ISO/IEC 17024:2012(E)

(15) Ensure all training products, instruction, and testing materials are of high quality and subject to CAICO quality control policies and procedures, to include technical accuracy and alignment with all applicable legal, regulatory, and policy requirements.

(16) Develop and maintain an internal appeals process, as required by ISO/IEC 17020:2017(E), and render a final decision on all elevated appeals.

(17) Develop and maintain a comprehensive plan and schedule to comply with all ISO/IEC 17011:2017(E), and DoD requirements for Conflict of Interest, Code of Professional Conduct, and Ethics policies as set forth in the DoD contract. All policies shall apply to the Accreditation Body, and other individuals, entities, and groups within the CMMC Ecosystem who provide Level 2 certification assessments, CMMC instruction, CMMC training materials, or Certificates of CMMC Status on behalf of the Accreditation Body. All policies in this section must be approved by the CMMC PMO prior to effectivity in accordance with the following requirements.

(i) *Conflict of Interest (CoI) policy*. The CoI policy shall:

(A) Include a detailed risk mitigation plan for all potential conflicts of interest that may pose a risk to compliance with ISO/IEC 17011:2017(E).

(B) Require employees, Board directors, and members of any accreditation committees or appeals adjudication committees to disclose to the CMMC PMO, in writing, as soon as it is known or reasonably should be known, any actual, potential, or perceived conflict of interest with sufficient detail to allow for assessment.

(C) Require employees, Board directors, and members of any accreditation committees or appeals adjudication committees who leave the board or organization to enter a "cooling off period" of one (1) year whereby they are prohibited from working with the Accreditation Body or participating in any and all CMMC activities described in Subpart C.

(D) Require CMMC Ecosystem members to actively avoid participating in any activity, practice, or transaction that could result in an actual or perceived conflict of interest.

(E) Require CMMC Ecosystem members to disclose to Accreditation Body leadership, in writing, any actual or potential conflict of interest as soon as it is known, or reasonably should be
known.

(ii) *Code of Professional Conduct (CoPC) policy*. The CoPC policy shall:

(A) Describe the performance standards by which the members of the CMMC Ecosystem will be held accountable and the procedures for addressing violations of those performance standards.

(B) Require the Accreditation Body to investigate and resolve any potential violations that are reported or are identified by the DoD.

(C) Require the Accreditation Body to inform the DoD in writing of new investigations within 72 hours.

(D) Require the Accreditation Body to report to the DoD in writing the outcome of completed investigations within 15 business days.

(E) Require CMMC Ecosystem members to represent themselves and their companies accurately; to include not misrepresenting any professional credentials or status, including CMMC authorization or CMMC Status, nor exaggerating the services that they or their company are capable or authorized to deliver.

(F) Require CMMC Ecosystem members to be honest and factual in all CMMC-related activities with colleagues, clients, trainees, and others with whom they interact.

(G) Prohibit CMMC Ecosystem members from participating in the Level 2 certification assessment process for an assessment in which they previously served as a consultant to prepare the organization for any CMMC assessment within 3 years.

(H) Require CMMC Ecosystem members to maintain the confidentiality of customer and government data to preclude unauthorized disclosure.

(I) Require CMMC Ecosystem members to report results and data from Level 2 certification assessments and training objectively, completely, clearly, and accurately.

(J) Prohibit CMMC Ecosystem members from cheating, assisting another in cheating, or allowing cheating on CMMC examinations.

(K) Require CMMC Ecosystem members to utilize official training content developed by a CMMC training organization approved by the CAICO in all CMMC certification courses.

(iii) *Ethics policy*. The Ethics policy shall:

(A) Require CMMC Ecosystem members to report to the Accreditation Body within 30 days of convictions, guilty pleas, or no contest pleas to crimes of fraud, larceny, embezzlement, misappropriation of funds, misrepresentation, perjury, false swearing, conspiracy to conceal, or a similar offense in any legal proceeding, civil or criminal, whether or not in connection with activities that relate to carrying out their role in the CMMC Ecosystem.

(B) Prohibit harassment or discrimination by CMMC Ecosystem members in all interactions with individuals whom they encounter in connection with their roles in the CMMC Ecosystem.

(C) Require CMMC Ecosystem members to have and maintain a satisfactory record of integrity and business ethics.

§ 170.9 CMMC Third-Party Assessment Organizations (C3PAOs).

(a) *Roles and responsibilities*. C3PAOs are organizations that are responsible for conducting Level 2 certification assessments and issuing Certificates of CMMC Status to OSCs based on the results. C3PAOs must be accredited or authorized by the Accreditation Body in accordance with the requirements set forth.

(b) *Requirements*. C3PAOs shall:

(1) Obtain authorization or accreditation from the Accreditation Body in accordance with § 170.8(b)(3)(i) and (ii).

(2) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in § 170.8(b)(17); and achieve and maintain compliance with ISO/IEC 17020:2012(E) (incorporated by reference, see § 170.2) within 27 months of authorization.

(3) Require all C3PAO company personnel participating in the Level 2 certification assessment process to complete a Tier 3 background investigation resulting in a determination of national security eligibility. This includes the CMMC Assessment Team and the quality assurance individual. This Tier 3 background investigation will not result in a security clearance and is not being executed for the purpose of government employment. The Tier 3 background investigation is initiated using the Standard Form (SF) 86

(www.gsa.gov/reference/forms/questionnaire-for-national-security-positions). These positions are designated as non-critical sensitive with a risk designation of "Moderate Risk" in accordance with 5 CFR 1400.201(b) and (d) and the investigative requirements of 5 CFR 731.106(c)(2).

(4) Require all C3PAO company personnel participating in the Level 2 certification assessment process 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.

(5) Comply with Foreign Ownership, Control or Influence (FOCI) by:

(i) Completing and submitting Standard Form (SF) 328 (www.gsa.gov/reference/forms/certificate-pertaining-to-foreign-interests), *Certificate Pertaining to Foreign Interests*, upon request from DCSA and undergo a National Security Review with regards to the protection of controlled unclassified information based on the factors identified in 32 CFR 117.11(b) using the procedures outlined in 32 CFR 117.11(c).

(ii) Receiving a non-disqualifying eligibility determination from the CMMC PMO resulting from the FOCI risk assessment in order to proceed to a DCMA DIBCAC CMMC Level 2 assessment, as part of the authorization and accreditation process set forth in paragraph (b)(6) of this section.

(iii) Reporting any change to the information provided on its SF 328 by resubmitting the SF 328 to DCSA within 15 business days of the change being effective. A disqualifying eligibility determination, based on the results of the change, will result in the C3PAO losing its authorization or accreditation.

(6) Undergo a Level 2 certification assessment meeting all requirements for a Final Level 2 (C3PAO) in accordance with the procedures specified in § 170.17(a)(1) and (c), with the following exceptions:

(i) The assessment will be conducted by DCMA DIBCAC.

(ii) The assessment will not result in a CMMC Status of Level 2 (C3PAO) nor receive a Certificate of CMMC Status.

(7) Provide all documentation and records in English.

(8) Submit pre-assessment and planning material, final assessment reports, and CMMC certificates of assessment into the CMMC instantiation of eMASS.

(9) Unless disposition is otherwise authorized by the CMMC PMO, maintain all assessment related records for a period of six (6) years. Such records include any materials generated by the C3PAO in the course of an assessment, any working papers generated from Level 2 certification assessments; and materials relating to monitoring, education, training, technical knowledge, skills, experience, and authorization of all personnel involved in assessment activities; contractual agreements with OSCs; and organizations for whom consulting services were provided.

(10) Provide any requested audit information, including any out-of-cycle from ISO/IEC 17020:2012(E) requirements, to the Accreditation Body.

(11) Ensure that all personally identifiable information (PII) is encrypted and protected in all C3PAO information systems and databases.

(12) Meet the requirements for Assessment Team composition. An Assessment Team must include at least two people: a Lead CCA, as defined in § 170.11(b)(10), and at least one other CCA. Additional CCAs and CCPs may also participate on an Assessment Team.

(13) Implement a quality assurance function that ensures the accuracy and completeness of assessment data prior to upload into the CMMC instantiation of eMASS. Any individual fulfilling the quality assurance function must be a CCA and cannot be a member of an Assessment Team for which they are performing a quality assurance role. A quality assurance individual shall manage the C3PAO's quality assurance reviews as defined in paragraph (b)(14) of this section and the appeals process as required by paragraphs (b)(19) and (20) of this section and in accordance with ISO/IEC 17020:2012(E) (incorporated by reference, see § 170.2) and ISO/IEC 17011:2017(E) (incorporated by reference, see § 170.2).

(14) Conduct quality assurance reviews for each assessment, including observations of the Assessment Team's conduct and management of CMMC assessment processes.

(15) Ensure that all Level 2 certification assessment activities are performed on the information system within the CMMC Assessment Scope.

(16) Maintain all facilities, personnel, and equipment involved in CMMC activities that are in scope of their Level 2 certification assessment and comply with all security requirements and procedures as prescribed by the Accreditation Body.

(17) Ensure that all assessment data and information uploaded into the CMMC instantiation of eMASS assessment data is compliant with the CMMC assessment data standard as set forth in eMASS CMMC Assessment Import Templates on the CMMC eMASS website: https://cmmc.emass.apps.mil. This system is accessible only to authorized users.

(18) Issue Certificates of CMMC Status to OSCs in accordance with the Level 2 certification assessment requirements set forth in § 170.17, that include, at a minimum, all industry CAGE codes associated with the information systems addressed by the CMMC Assessment Scope, the C3PAO name, assessment unique identifier, the OSC name, and the CMMC Status date and level.

(19) Address all OSC appeals arising from Level 2 certification assessment activities. If the OSC or C3PAO is not satisfied with the result of the appeal either the OSC or the C3PAO can elevate the matter to the Accreditation Body for final determination.

(20) Submit assessment appeals, review records, and decision results of assessment appeals to DoD using the CMMC instantiation of eMASS.

§ 170.10 CMMC Assessor and Instructor Certification Organization (CAICO).

(a) *Roles and responsibilities*. The CAICO is responsible for training, testing, authorizing, certifying, and recertifying CMMC assessors, instructors, and related professionals. Only the CAICO may make decisions relating to examination certifications, including the granting, maintaining, recertifying, expanding, and reducing the scope of certification, and suspending or withdrawing certification in accordance with current ISO/IEC 17024:2012(E)
(incorporated by reference, see § 170.2). At any given point in time, there will be only one CAICO for the DoD CMMC Program.

(b) *Requirements*. The CAICO shall:

(1) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in § 170.8(b)(17); and achieve and maintain ISO/IEC 17024(E) accreditation within 12 months of [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

(2) Provide all documentation and records in English.

(3) Train, test, and designate PIs in accordance with the requirements of this section. Train, test, certify, and recertify CCPs, CCAs, and CCIs in accordance with the requirements of this section.

(4) Ensure the instructor and assessor certification examinations are certified under ISO/IEC 17024:2012(E) (incorporated by reference, see § 170.2), by a recognized US-based accreditor who is not a member of the CMMC Accreditation Body. The US-based accreditor must be a signatory to International Laboratory Accreditation Cooperation (ILAC) or relevant International Accreditation Forum (IAF) Mutual Recognition Arrangement (MRA) and must operate in accordance with ISO/IEC 17011:2017(E) (incorporated by reference, see § 170.2).

(5) Establish quality control policies and procedures for the generation of training products, instruction, and testing materials.

(6) Oversee development, administration, and management pertaining to the quality of training and examination materials for CMMC assessor and instructor certification and recertification.

(7) Establish and publish an authorization and certification appeals process to receive, evaluate, and make decisions on complaints and appeals in accordance with ISO/IEC 17024:2012(E) (incorporated by reference, see § 170.2).

(8) Address all appeals arising from the CCA, CCI, and CCP authorizations and certifications process through use of internal processes in accordance with ISO/IEC 17024:2012(E) (incorporated by reference, see § 170.2).

(9) Maintain records for a period of six (6) years of all procedures, processes, and actions related to fulfillment of the requirements set forth in this section and provide the Accreditation
Body access to those records.

(10) Provide the Accreditation Body information about the authorization and accreditation status of assessors, instructors, training community, and publishing partners.

(11) Ensure separation of duties between individuals involved in testing activities, training activities, and certification activities.

(12) Safeguard and require any CAICO training support service providers, as applicable, to safeguard the confidentiality of applicant, candidate, and certificate-holder information and ensure the overall security of the certification process.

(13) Ensure that all PII is encrypted and protected in all CAICO information systems and databases and those of any CAICO training support service providers.

(14) Ensure the security of assessor and instructor examinations and the fair and credible administration of examinations.

(15) Neither disclose nor allow any CAICO training support service providers, as applicable, to disclose CMMC data or metrics related to authorization or certification activities to any entity other than the Accreditation Body and DoD, except as required by law.

(16) Require retraining and redesignation of PIs upon significant change to DoD's CMMC Program requirements. Require retraining and recertification of CCPs, CCAs, and CCIs upon significant change to DoD's CMMC Program requirements, as determined by the DoD or the CAICO.

(17) Require CMMC Ecosystem members to report to the CAICO within 30 days of convictions, guilty pleas, or no contest pleas to crimes of fraud, larceny, embezzlement, misappropriation of funds, misrepresentation, perjury, false swearing, conspiracy to conceal, or a similar offense in any legal proceeding, civil or criminal, whether or not in connection with activities that relate to carrying out their role in the CMMC Ecosystem.

§ 170.11 CMMC Certified Assessor (CCA).

(a) *Roles and responsibilities*. CCAs, in support of a C3PAO, conduct Level 2 certification assessments of OSCs in accordance with NIST SP 800-171A Jun2018 (incorporated by reference, see § 170.2), the assessment processes defined in § 170.17, and the scoping requirements defined in § 170.19(c). CCAs must meet all of the requirements set forth in paragraph (b) of this section. A CCA may conduct Level 2 certification assessments and participate on a C3PAO Assessment Team.

(b) *Requirements*. CCAs shall:

(1) Obtain and maintain certification from the CAICO in accordance with the requirements set forth in § 170.10. Certification is valid for 3 years from the date of issuance.

(2) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in § 170.8(b)(17).

(3) Complete a Tier 3 background investigation resulting in a determination of national security eligibility. This Tier 3 background investigation will not result in a security clearance and is not being executed for the purpose of government employment. The Tier 3 background investigation is initiated using the Standard Form (SF) 86 (www.gsa.gov/reference/forms/questionnaire-for-national-security-positions). These positions are designated as non-critical sensitive with a risk designation of "Moderate Risk" in accordance with 5 CFR 1400.201(b) and (d) and the investigative requirements of 5 CFR 731.106(c)(2).

(4) Meet the equivalent of a favorably adjudicated Tier 3 background investigation when not eligible for a Tier 3 background investigation. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only.

(5) Provide all documentation and records in English.

(6) Be a CCP who has at least 3 years of cybersecurity experience, at least 1 year of assessment or audit experience, and at least one foundational qualification, aligned to at least the Intermediate Proficiency Level of the DoD Cyberspace Workforce Framework's Security Control Assessor (612) Work Role, from DoD Manual 8140.03, *Cyberspace Workforce Qualification and Management Program* (https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf). Information on the Work Role 612 can be found at https://public.cyber.mil/dcwf-work-role/security-controlassessor/.

(7) Only use IT, cloud, cybersecurity services, and end-point devices provided by the authorized/accredited C3PAO that has been engaged to perform that OSA's Level 2 certification assessment and which has undergone a Level 2 certification assessment by DCMA DIBCAC (or higher) for all assessment activities. Individual assessors are prohibited from using any other IT, including IT that is personally owned, to include internal and external cloud services and end-point devices, to process, store, or transmit CMMC assessment reports or any other CMMC assessment-related information. The evaluation of assessment evidence within the OSC environment, using OSC tools, is permitted.

(8) Immediately notify the responsible C3PAO of any breach or potential breach of security to any CMMC-related assessment materials under the assessors' purview.

(9) Not share any information about an OSC obtained during CMMC pre-assessment and assessment activities with any person not involved with that specific assessment, except as otherwise required by law.

(10) Qualify as a Lead CCA by having at least 5 years of cybersecurity experience, 5 years of management experience, 3 years of assessment or audit experience, and at least one foundational qualification aligned to Advanced Proficiency Level of the DoD Cyberspace Workforce Framework's Security Control Assessor (612) Work Role, from DoD Manual 8140.03, *Cyberspace Workforce Qualification and Management Program* (https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf). Information on the Work Role 612 can be found at https://public.cyber.mil/dcwf-work-role/security-controlassessor/.

§ 170.12 CMMC Instructor.

(a) *CMMC Provisional Instructor (PI) roles and responsibilities.* A CMMC Provisional Instructor (PI) teaches CCA and CCP candidates during the transitional period that ends 18 months after [INSERT DATE 60 DAYS AFTER THE DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. A PI is trained, tested, and designated to perform CMMC instructional duties by the CAICO to teach CCP and CCA candidates. PIs are designated by the CAICO after successful completion of the PI training and testing requirements set forth by the CAICO. A PI with a valid CCP certification may instruct CCP candidates, while a PI with a valid CCA certification may instruct CCP and CCA candidates. PIs are required to meet requirements in (c) of this section.

(b) *CMMC Certified Instructor (CCI) roles and responsibilities*. A CMMC Certified Instructor (CCI) teaches CCP, CCA, and CCI candidates and performs CMMC instructional duties. Candidate CCIs are certified by the CAICO after successful completion of the CCI training and testing requirements. A CCI is required to obtain and maintain assessor and instructor certifications from the CAICO in accordance with the requirements set forth in § 170.10 and in paragraph (c) of this section. A CCI with a valid CCP certification may instruct CCP candidates, while a CCI with a valid CCA certification may instruct CCP, CCA, and CCI candidates. Certifications are valid for 3 years from the date of issuance. CCIs are required to meet requirements in paragraph (c) of this section.

(c) *Requirements*. CMMC Instructors shall:

(1) Obtain and maintain instructor designation or certification, as appropriate, from the CAICO in accordance with the requirements set forth in § 170.10.

(2) Obtain and maintain CCP or CCA certification to deliver CCP training.

(3) Obtain and maintain a CCA certification to deliver CCA training.

(4) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in § 170.8(b)(17).

(5) Provide all documentation and records in English.

(6) Provide the Accreditation Body and the CAICO annually with accurate information detailing their qualifications, training experience, professional affiliations, and certifications, and, upon reasonable request, submit documentation verifying this information.

(7) Not provide CMMC consulting services while serving as a CMMC instructor; however, subject to the Code of Professional Conduct and Conflict of Interest policies, can serve on an assessment team.

(8) Not participate in the development of exam objectives and/or exam content or act as an exam proctor while at the same time serving as a CCI.

(9) Keep confidential all information obtained or created during the performance of CMMC training activities, including trainee records, except as required by law.

(10) Not disclose any CMMC-related data or metrics that is PII, FCI, or CUI to anyone without prior coordination with and approval from DoD.

(11) Notify the Accreditation Body or the CAICO if required by law or authorized by contractual commitments to release confidential information.

(12) Not share with anyone any CMMC training-related information not previously publicly disclosed.

§ 170.13 CMMC Certified Professional (CCP).

(a) *Roles and responsibilities*. A CMMC Certified Professional (CCP) completes rigorous training on CMMC and the assessment process to provide advice, consulting, and recommendations to their OSA clients. Candidate CCPs are certified by the CAICO after successful completion of the CCP training and testing requirements set forth in paragraph (b) of this section. CCPs are eligible to become CMMC Certified Assessors and can participate as a CCP on Level 2 certification assessments with CCA oversight where the CCA makes all final determinations.

(b) *Requirements*. CCPs shall:

(1) Obtain and maintain certification from the CAICO in accordance with the requirements set forth in § 170.10. Certification is valid for 3 years from the date of issuance.

(2) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics as set forth in § 170.8(b)(17).

(3) Complete a Tier 3 background investigation resulting in a determination of national security eligibility. This Tier 3 background investigation will not result in a security clearance and is not being executed for the purpose of government employment. The Tier 3 background investigation is initiated using the Standard Form (SF) 86 (www.gsa.gov/reference/forms/questionnaire-for-national-security-positions). These positions are designated as non-critical sensitive with a risk designation of "Moderate Risk" in accordance with 5 CFR 1400.201(b) and (d) and the investigative requirements of 5 CFR 731.106(c)(2).

(4) Meet the equivalent of a favorably adjudicated Tier 3 background investigation when not eligible to obtain a Tier 3 background investigation. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only.

(5) Provide all documentation and records in English.

(6) Not share any information about an OSC obtained during CMMC pre-assessment and assessment activities with any person not involved with that specific assessment, except as otherwise required by law.

Subpart D—Key Elements of the CMMC Program.

§ 170.14 CMMC Model.

(a) *Overview*. The CMMC Model incorporates the security requirements from:

(1) 48 CFR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*;

(2) NIST SP 800-171 R2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (incorporated by reference, see § 170.2); and

(3) Selected security requirements from NIST SP 800-172 Feb2021, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171* (incorporated by reference, see § 170.2).

(b) *CMMC domains*. The CMMC Model consists of domains that map to the Security Requirement Families defined in NIST SP 800-171 R2 (incorporated by reference, see § 170.2).

(c) *CMMC level requirements*. CMMC Levels 1-3 utilize the safeguarding requirements and security requirements specified in 48 CFR 52.204-21 (for Level 1), NIST SP 800-171 R2 (incorporated by reference, see § 170.2) (for Level 2), and selected security requirements from NIST SP 800-172 Feb2021 (incorporated by reference, see § 170.2) (for Level 3). This paragraph discusses the numbering scheme and the security requirements for each level.

(1) *Numbering*. Each security requirement has an identification number in the format – DD.L#-REQ – where:

(i) DD is the two-letter domain abbreviation;

(ii) L# is the CMMC level number; and

(iii) REQ is the 48 CFR 52.204-21 paragraph number, NIST SP 800-171 R2 requirement number, or NIST SP 800-172 Feb2021 requirement number.

(2) *CMMC Level 1 security requirements*. The security requirements in CMMC Level 1 are those set forth in 48 CFR 52.204-21(b)(1)(i) through (xv).

(3) *CMMC Level 2 security requirements*. The security requirements in CMMC Level 2 are identical to the requirements in NIST SP 800-171 R2.

(4) *CMMC Level 3 security requirements*. The security requirements in CMMC Level 3 are selected from NIST SP 800-172 Feb2021, and where applicable, Organization-Defined Parameters (ODPs) are assigned. Table 1 to this paragraph identifies the selected requirements and applicable ODPs that represent the CMMC Level 3 security requirements. ODPs for the NIST SP 800-172 Feb2021 requirements are italicized, where applicable:

Table 1 to § 170.14(c)(4)

Security Requirement Number*	**CMMC Level 3 Security Requirements (Selected NIST SP 800-172 Feb2021 security requirement with DoD ODPs italicized)**
(i) AC.L3-3.1.2e	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.
(ii) AC.L3-3.1.3e	Employ *secure information transfer solutions* to control information flows between security domains on connected systems.

(iii) AT.L3-3.2.1e	Provide awareness training *upon initial hire, following a significant cyber event, and at least annually*, focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training *at least annually* or when there are significant changes to the threat.
(iv) AT.L3-3.2.2e	Include practical exercises in awareness training for *all users, tailored by roles, to include general users, users with specialized roles, and privileged users*, that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.
(v) CM.L3-3.4.1e	Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.
(vi) CM.L3-3.4.2e	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, *remove the components or place the components in a quarantine or remediation network* to facilitate patching, re-configuration, or other mitigations.
(vii) CM.L3-3.4.3e	Employ automated discovery and management tools to maintain an upto-date, complete, accurate, and readily available inventory of system components.
(viii) IA.L3-3.5.1e	Identify and authenticate *systems and system components, where possible,* before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.

(ix) IA.L3-3.5.3e	Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.
(x) IR.L3-3.6.1e	Establish and maintain a security operations center capability that operates *24/7, with allowance for remote/on-call staff*.
(xi) IR.L3-3.6.2e	Establish and maintain a cyber-incident response team that can be deployed by the organization within *24 hours*.
(xii) PS.L3-3.9.2e	Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.
(xiii) RA.L3-3.11.1e	Employ *threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources*, as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.
(xiv) RA.L3-3.11.2e	Conduct cyber threat hunting activities *on an on-going aperiodic basis or when indications warrant*, to search for indicators of compromise in *organizational systems* and detect, track, and disrupt threats that evade existing controls.

(xv) RA.L3-3.11.3e	Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.
(xvi) RA.L3-3.11.4e	Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.

(xvii) RA.L3-3.11.5e	Assess the effectiveness of security solutions *at least annually or upon receipt of relevant cyber threat information, or in response to a relevant cyber incident*, to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.
(xviii) RA.L3-3.11.6e	Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.
(xix) RA.L3-3.11.7e	Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan *at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident*.
(xx) CA.L3-3.12.1e	Conduct penetration testing *at least annually or when significant security changes are made to the system*, leveraging automated scanning tools and ad hoc tests using subject matter experts.
(xxi) SC.L3-3.13.4e	Employ *physical isolation techniques or logical isolation techniques or both* in organizational systems and system components.
(xxii) SI.L3-3.14.1e	Verify the integrity of *security critical and essential software* using root of trust mechanisms or cryptographic signatures.
(xxiii) SI.L3-3.14.3e	Ensure that *specialized assets including IoT, IIoT, OT, GFE, Restricted Information Systems, and test equipment* are included in the scope of the
	specified enhanced security requirements or are segregated in purposespecific networks.
(xxiv) SI.L3-3.14.6e	Use threat indicator information and effective mitigations obtained from, *at a minimum, open or commercial sources, and any DoDprovided sources*, to guide and inform intrusion detection and threat hunting.

* Roman numerals in parentheses before the Security Requirement are for numbering purposes only. The numerals are not part of the naming convention for the requirement.

(d) *Implementation*. Assessment of security requirements is prescribed by NIST SP 800-171A Jun2018 (incorporated by reference, see § 170.2) and NIST SP 800-172A Mar2022 (incorporated by reference, see § 170.2). Descriptive text in these documents support OSA implementation of the security requirements and use the terms organization-defined and periodically. Except where referring to Organization-Defined Parameters (ODPs), organizationdefined means as determined by the OSA. Periodically means occurring at regular intervals. As used in many requirements within CMMC, the interval length is organization-defined to provided contractor flexibility, with an interval length of no more than one year.

§ 170.15 CMMC Level 1 self-assessment and affirmation requirements.

(a) *Level 1 self-assessment*. To comply with CMMC Level 1 self-assessment requirements, the OSA must meet the requirements detailed in paragraphs (a)(1) and (2) of this section. An OSA conducts a Level 1 self-assessment as detailed in paragraph (c) of this section to achieve a CMMC Status of Final Level 1 (Self).

(1) *Level 1 self-assessment requirements*. The OSA must complete and achieve a MET result for all security requirements specified in § 170.14(c)(2) to achieve the CMMC Status of Final Level 1 (Self). No POA&Ms are permitted for CMMC Level 1. The OSA must conduct a self-assessment in accordance with the procedures set forth in § 170.15(c)(1) and submit assessment results in SPRS. To maintain compliance with the requirements for the CMMC Status of Final Level 1 (Self), the OSA must conduct a Level 1 self-assessment on an annual basis and submit the results in SPRS, or its successor capability.

(i) *Inputs to SPRS*. The Level 1 self-assessment results in the Supplier Performance Risk System (SPRS) shall include, at minimum, the following items:

(A) CMMC Level.

(B) CMMC Status Date.

(C) CMMC Assessment Scope.

(D) All industry CAGE code(s) associated with the information system(s) addressed by the CMMC Assessment Scope

(E) Compliance result.

(ii) [Reserved]

(2) *Affirmation*. Affirmation of the Level 1 (Self) CMMC Status is required for all Level 1 self-assessments. Affirmation procedures are set forth in § 170.22.

(b) *Contract eligibility*. Prior to award of any contract or subcontract with a requirement for the CMMC Status of Level 1 (Self), OSAs must both achieve a CMMC Status of Level 1 (Self) and have submitted an affirmation of compliance into SPRS for all information systems within the CMMC Assessment Scope.

(c) *Procedures*–(1) *Level 1 self-assessment*. The OSA must conduct a Level 1 selfassessment scored in accordance with the CMMC Scoring Methodology described in § 170.24. The Level 1 self-assessment must be performed in accordance with the CMMC Level 1 scope requirements set forth in § 170.19(a) and (b) and the following:

(i) The Level 1 self-assessment must be performed using the objectives defined in NIST SP 800-171A Jun2018 (incorporated by reference, see § 170.2) for the security requirement that maps to the CMMC Level 1 security requirement as specified in table 1 to paragraph (c)(1)(ii) of this section. In any case where an objective addresses CUI, FCI should be substituted for CUI in the objective.

(ii) Mapping table for CMMC Level 1 security requirements to the NIST SP 800-171A Jun2018 objectives.

Table 2 to § 170.15(c)(1)(ii)—CMMC Level 1 Security Requirements Mapped to NIST SP 800-171A Jun2018

CMMC Level 1 Security Requirements as set forth in § 170.14(c)(2)	NIST SP 800-171A Jun2018
AC.L1-b.1.i	3.1.1
AC.L1-b.1.ii	3.1.2
AC.L1-b.1.iii	3.1.20
AC.L1-b.1.iv	3.1.22
IA.L1-b.1.v	3.5.1
IA.L1-b.1.vi	3.5.2
MP.L1-b.1.vii	3.8.3
PE.L1-b.1.viii	3.10.1
First phrase of PE.L1-b.1.ix (FAR b.1.ix*)	3.10.3
Second phrase of PE.L1-b.1.ix (FAR b.1.ix*)	3.10.4
Third phrase of PE.L1-b.1.ix (FAR b.1.ix*)	3.10.5
SC.L1-b.1.x	3.13.1
SC.L1-b.1.xi	3.13.5
SI.L1-b.1.xii	3.14.1
SI.L1-b.1.xiii	3.14.2
SI.L1-b.1.xiv	3.14.4
SI.L1-b.1.xv	3.14.5
* Three of the 48 CFR 52.204-21 requirements were broken apart by "phrase" when NIST SP 800-171 R2 was developed.	

(iii) Additional guidance can be found in the guidance document listed in paragraph (b) of appendix A to this part.

(2) *Artifact retention*. The artifacts used as evidence for the assessment must be retained by the OSA for six (6) years from the CMMC Status Date.

§ 170.16 CMMC Level 2 self-assessment and affirmation requirements.

(a) *Level 2 self-assessment*. To comply with Level 2 self-assessment requirements, the OSA must meet the requirements detailed in paragraphs (a)(1) and (2) of this section. An OSA conducts a Level 2 self-assessment as detailed in paragraph (c) of this section to achieve a CMMC Status of either Conditional or Final Level 2 (Self). Achieving a CMMC Status of Level 2 (Self) also satisfies the requirements for a CMMC Status of Level 1 (Self) detailed in § 170.15 for the same CMMC Assessment Scope.

(1) *Level 2 self-assessment requirements*. The OSA must complete and achieve a MET result for all security requirements specified in § 170.14(c)(3) to achieve the CMMC Status of Level 2 (Self). The OSA must conduct a self-assessment in accordance with the procedures set forth in paragraph (c)(1) of this section and submit assessment results in Supplier Performance Risk System (SPRS). To maintain compliance with the requirements for a CMMC Status of Level 2 (Self), the OSA must conduct a Level 2 self-assessment every three years and submit the results in SPRS, within three years of the CMMC Status Date associated with the Conditional Level 2 (Self).

(i) *Inputs to SPRS*. The Level 2 self-assessment results in the SPRS shall include, at minimum, the following information:

(A) CMMC Level.

(B) CMMC Status Date.

(C) CMMC Assessment Scope.

(D) All industry CAGE code(s) associated with the information system(s) addressed by the CMMC Assessment Scope.

(E) Overall Level 2 self-assessment score (e.g., 105 out of 110).

(F) POA&M usage and compliance status, if applicable.

(ii) *Conditional Level 2 (Self)*. The OSA has achieved the CMMC Status of Conditional Level 2 (Self) if the Level 2 self-assessment results in a POA&M and the POA&M meets all the CMMC Level 2 POA&M requirements listed in § 170.21(a)(2).

(A) *Plan of Action and Milestones*. A Level 2 POA&M is allowed only in accordance with the CMMC POA&M requirements listed in § 170.21.

(B) *POA&M closeout*. The OSA must remediate any NOT MET requirements, must perform a POA&M closeout self-assessment, and must post compliance results to SPRS within 180 days of the CMMC Status Date associated with the Conditional Level 2 (Self). If the POA&M is not successfully closed out within the 180-day timeframe, the Conditional Level 2 (Self) CMMC Status for the information system will expire. If Conditional Level 2 (Self) CMMC Status expires within the period of performance of a contract, standard contractual remedies will apply, and the OSA will be ineligible for additional awards with a requirement for the CMMC Status of Level 2 (Self), or higher requirement, for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(iii) *Final Level 2 (Self)*. The OSA has achieved the CMMC Status of Final Level 2 (Self) if the Level 2 self-assessment results in a passing score as defined in § 170.24. This score may be achieved upon initial self-assessment or as the result of a POA&M closeout selfassessment, as applicable.

(iv) *CMMC Status investigation*. The DoD reserves the right to conduct a DCMA DIBCAC assessment of the OSA, as provided for under the 48 CFR 252.204-7020. If the investigative results of a subsequent DCMA DIBCAC assessment show that adherence to the provisions of this part have not been achieved or maintained, these DCMA DIBCAC results will take precedence over any pre-existing CMMC Status. At that time, standard contractual remedies will be available and the OSA will be ineligible for additional awards with CMMC Status requirement of Level 2 (Self), or higher requirement, for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(2) *Affirmation*. Affirmation of the Level 2 (Self) CMMC Status is required for all Level 2 self-assessments at the time of each assessment, and annually thereafter. Affirmation procedures are set forth in § 170.22.

(b) *Contract eligibility*. Prior to award of any contract or subcontract with requirement for CMMC Status of Level 2 (Self), the following two requirements must be met:

(1) The OSA must achieve, as specified in paragraph (a)(1) of this section, a CMMC Status of either Conditional Level 2 (Self) or Final Level 2 (Self).

(2) The OSA must submit an affirmation of compliance into SPRS, as specified in paragraph (a)(2) of this section.

(c) *Procedures*—(1) *Level 2 self-assessment of the OSA*. The OSA must conduct a Level 2 self-assessment in accordance with NIST SP 800-171A Jun2018 (incorporated by reference, see § 170.2) and the CMMC Level 2 scoping requirements set forth in §§ 170.19(a) and (c) for the information systems within the CMMC Assessment Scope. The Level 2 self-assessment must be scored in accordance with the CMMC Scoring Methodology described in § 170.24 and the OSA must upload the results into SPRS. If a POA&M exists, a POA&M closeout selfassessment must be performed by the OSA when all NOT MET requirements have been remediated. The POA&M closeout self-assessment must be performed within 180-days of the Conditional CMMC Status Date. Additional guidance can be found in the guidance document listed in paragraph (c) of appendix A to this part.

(2) *Level 2 self-assessment with the use of Cloud Service Provider (CSP)*. An OSA may use a cloud environment to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 2 (Self) under the following circumstances:

(i) The CSP product or service offering is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or

(ii) The CSP product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline. FedRAMP Moderate or FedRAMP Moderate equivalent is in accordance with DoD Policy.

(iii) In accordance with § 170.19(c)(2), the OSA's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the Customer Responsibility Matrix (CRM) must be documented or referred to in the OSA's System Security Plan (SSP).

(3) *Level 2 self-assessment with the use of an External Service Provider (ESP), not a CSP*. An OSA may use an ESP that is not a CSP to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 2 (Self) under the following circumstances:

(i) The use of the ESP, its relationship to the OSA, and the services provided are documented in the OSA's SSP and described in the ESP's service description and CRM.

(ii) The ESP services used to meet OSA requirements are assessed within the scope of the OSA's assessment against all Level 2 security requirements.

(iii) In accordance with § 170.19(c)(2), the OSA's on-premises infrastructure connecting to the ESP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSA's SSP.

(4) *Artifact retention*. The artifacts used as evidence for the assessment must be retained by the OSA for six (6) years from the CMMC Status Date.

§ 170.17 CMMC Level 2 certification assessment and affirmation requirements.

(a) *Level 2 certification assessment*. To comply with Level 2 certification assessment requirements, the OSC must meet the requirements set forth in paragraphs (a)(1) and (2) of this section. An OSC undergoes a Level 2 certification assessment as detailed in paragraph (c) of this section to achieve a CMMC Status of either Conditional or Final Level 2 (C3PAO).

Achieving a CMMC Status of Level 2 (C3PAO) also satisfies the requirements for a CMMC Statuses of Level 1 (Self) and Level 2 (Self) set forth in §§ 170.15 and 170.16 respectively for the same CMMC Assessment Scope.

(1) *Level 2 certification assessment requirements*. The OSC must complete and achieve a MET result for all security requirements specified in § 170.14(c)(3) to achieve the CMMC Status of Level 2 (C3PAO). The OSC must obtain a Level 2 certification assessment from an authorized or accredited C3PAO following the procedures outlined in paragraph (c) of this section. The C3PAO must submit the Level 2 certification assessment results into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS. To maintain compliance with the requirements for a CMMC Status of Level 2 (C3PAO), the Level 2 certification assessment must be completed within three years of the CMMC Status Date associated with the Conditional Level 2 (C3PAO)

(i) *Inputs into the CMMC instantiation of eMASS*. The Level 2 certification assessment results input into the CMMC instantiation of eMASS shall include, at minimum, the following information:

(A) Date and level of the assessment.

(B) C3PAO name.

(C) Assessment unique identifier.

(D) For each Assessor conducting the assessment, name and business contact information.

(E) All industry CAGE codes associated with the information systems addressed by the
CMMC Assessment Scope.

(F) The name, date, and version of the SSP.

(G) CMMC Status Date.

(H) Assessment result for each requirement objective.

(I) POA&M usage and compliance, as applicable.

(J) List of the artifact names, the return value of the hashing algorithm, and the hashing algorithm used.

(ii) *Conditional Level 2 (C3PAO)*. The OSC has achieved the CMMC Status of Conditional Level 2 (C3PAO) if the Level 2 certification assessment results in a POA&M and the POA&M meets all CMMC Level 2 POA&M requirements listed in § 170.21(a)(2).

(A) *Plan of Action and Milestones*. A Level 2 POA&M is allowed only in accordance with the CMMC POA&M requirements listed in § 170.21.

(B) *POA&M closeout*. The OSC must remediate any NOT MET requirements, must undergo a POA&M closeout certification assessment from a C3PAO, and the C3PAO must post compliance results into the CMMC instantiation of eMASS within 180 days of the CMMC Status Date associated with the Conditional Level 2 (C3PAO). If the POA&M is not successfully closed out within the 180-day timeframe, the Conditional Level 2 (C3PAO) CMMC Status for the information system will expire. If Conditional Level 2 (C3PAO) CMMC Status expires within the period of performance of a contract, standard contractual remedies will apply, and the OSC will be ineligible for additional awards with a requirement for the CMMC Status of Level 2 (C3PAO), or higher requirement, for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(iii) *Final Level 2 (C3PAO)*. The OSC has achieved the CMMC Status of Final Level 2
(C3PAO) if the Level 2 certification assessment results in a passing score as defined in § 170.24. This score may be achieved upon initial certification assessment or as the result of a POA&M closeout certification assessment, as applicable.

(iv) *CMMC Status investigation*. The DoD reserves the right to conduct a DCMA DIBCAC assessment of the OSC, as provided for under the 48 CFR 252.204-7020. If the investigative results of a subsequent DCMA DIBCAC assessment show that adherence to the provisions of this part have not been achieved or maintained, these DCMA DIBCAC

results will take precedence over any pre-existing CMMC Status. At that time, standard contractual remedies will be available and the OSC will be ineligible for additional awards with CMMC Status requirement of Level 2 (C3PAO), or higher requirement, for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(2) *Affirmation*. Affirmation of the Level 2 (C3PAO) CMMC Status is required for all Level 2 certification assessments at the time of each assessment, and annually thereafter. Affirmation procedures are provided in § 170.22.

(b) *Contract eligibility*. Prior to award of any contract or subcontract with a requirement for the CMMC Status of Level 2 (C3PAO), the following two requirements must be met:

(1) The OSC must achieve, as specified in paragraph (a)(1) of this section, a CMMC Status of either Conditional Level 2 (C3PAO) or Final Level 2 (C3PAO).

(2) The OSC must submit an affirmation of compliance into SPRS, as specified in paragraph (a)(2) of this section.

(c) *Procedures*–(1) *Level 2 certification assessment of the OSC*. An authorized or accredited C3PAO must perform a Level 2 certification assessment in accordance with NIST SP 800-171A Jun2018 (incorporated by reference, see § 170.2) and the CMMC Level 2 scoping requirements set forth in § 170.19(a) and (c) for the information systems within the CMMC Assessment Scope. The Level 2 certification assessment must be scored in accordance with the CMMC Scoring Methodology described in § 170.24 and the C3PAO must upload the results into the CMMC instantiation of eMASS. Final results are communicated to the OSC through a CMMC Assessment Findings Report.

(2) *Security requirement re-evaluation*. A security requirement that is NOT MET (as defined in § 170.24) may be re-evaluated during the course of the Level 2 certification assessment and for 10 business days following the active assessment period if all of the following conditions exist:

(i) Additional evidence is available to demonstrate the security requirement has been MET;

(ii) Cannot change or limit the effectiveness of other requirements that have been scored MET; and

(iii) The CMMC Assessment Findings Report has not been delivered.

(3) *POA&M.* If a POA&M exists, a POA&M closeout certification assessment must be performed by a C3PAO within 180-days of the Conditional CMMC Status Date. Additional guidance can be found in § 170.21 and in the guidance document listed in paragraph (c) of appendix A to this part.

(4) *Artifact retention and integrity*. The hashed artifacts used as evidence for the assessment must be retained by the OSC for six (6) years from the CMMC Status Date. To ensure that the artifacts have not been altered, the OSC must hash the artifact files using a NISTapproved hashing algorithm. The OSC must provide the C3PAO with a list of the artifact names, the return value of the hashing algorithm, and the hashing algorithm for upload into the CMMC instantiation of eMASS. Additional guidance for hashing artifacts can be found in the guidance document listed in paragraph (h) of appendix A to this part.

(5) *Level 2 certification assessment with the use of Cloud Service Provider (CSP)*. An OSC may use a cloud environment to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 2 (C3PAO) under the following circumstances:

(i) The CSP product or service offering is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or

(ii) The CSP product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by

the FedRAMP Moderate (or higher) baseline. FedRAMP Moderate or FedRAMP Moderate equivalent is in accordance with DoD Policy.

(iii) In accordance with § 170.19(c)(2), the OSC's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope. As such, the security requirements from the CRM must be documented or referred to in the OSC's SSP.

(6) *Level 2 certification assessment with the use of an External Service Provider (ESP), not a CSP*. An OSA may use an ESP that is not a CSP to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 2 (C3PAO) under the following circumstances:

(i) The use of the ESP, its relationship to the OSA, and the services provided are documented in the OSA's SSP and described in the ESP's service description and customer responsibility matrix.

(ii) The ESP services used to meet OSA requirements are assessed within the scope of the OSA's assessment against all Level 2 security requirements.

(iii) In accordance with § 170.19(c)(2), the OSA's on-premises infrastructure connecting to the ESP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSA's SSP.

§ 170.18 CMMC Level 3 certification assessment and affirmation requirements.

(a) *Level 3 certification assessment*. To comply with Level 3 certification assessment requirements, the OSC must meet the requirements set forth in paragraphs (a)(1) and (2) of this section. An OSC undergoes a Level 3 certification assessment as detailed in paragraph (c) of this section to achieve a CMMC Status of either Conditional or Final Level 3 (DIBCAC). A CMMC Status of Final Level 2 (C3PAO) for information systems within the Level 3 CMMC Assessment Scope is a prerequisite to undergo a Level 3 certification assessment. CMMC Level 3 recertification also has a prerequisite for a new CMMC Level 2 assessment. Achieving a CMMC Status of Level 3 (DIBCAC) also satisfies the requirements for CMMC Statuses of Level 1 (Self), Level 2 (Self), and Level 2 (C3PAO) set forth in §§ 170.15 through 170.17 respectively for the same CMMC Assessment Scope.

(1) *Level 3 certification assessment requirements*. The OSC must achieve a CMMC Status of Final Level 2 (C3PAO) on the Level 3 CMMC Assessment Scope, as defined in § 170.19(d), prior to initiating a Level 3 certification assessment, which will be performed by DCMA DIBCAC (www.dcma.mil/DIBCAC) on behalf of the DoD. The OSC must complete and achieve a MET result for all security requirements specified in table 1 to § 170.14(c)(4) to achieve the CMMC Status of Level 3 (DIBCAC). DCMA DIBCAC will submit the Level 3 certification assessment results into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS. To maintain compliance with the requirements for a CMMC Status of Level 3 (DIBCAC), the Level 3 certification assessment must be performed every three years for all information systems within the Level 3 CMMC Assessment Scope. In addition, given that compliance with Level 2 requirements is a prerequisite for applying for CMMC Level 3, a Level 2 (C3PAO) certification assessment must also be conducted every three years to maintain CMMC Level 3 (DIBCAC) status. Level 3 certification assessment must be completed within three years of the CMMC Status Date associated with the Final Level 3 (DIBCAC) or, if there was a POA&M, then within three years of the CMMC Status Date associated with the Conditional Level 3 (DIBCAC).

(i) *Inputs into the CMMC instantiation of eMASS*. The Level 3 certification assessment results input into the CMMC instantiation of eMASS shall include, at minimum, the following items:

(A) Date and level of the assessment.

(B) For each Assessor(s) conducting the assessment, name and government organization information.

(C) All industry CAGE code(s) associated with the information system(s) addressed by the CMMC Assessment Scope.

(D) The name, date, and version of the system security plan(s) (SSP).

(E) CMMC Status Date.

(F) Result for each security requirement objective.

(G) POA&M usage and compliance, as applicable.

(H) List of the artifact names, the return value of the hashing algorithm, and the hashing algorithm used.

(ii) *Conditional Level 3 (DIBCAC)*. The OSC has achieved the CMMC Status of Conditional Level 3 (DIBCAC) if the Level 3 certification assessment results in a POA&M and the POA&M meets all CMMC Level 3 POA&M requirements listed in § 170.21(a)(3).

(A) *Plan of Action and Milestones*. A Level 3 POA&M is allowed only in accordance with the CMMC POA&M requirements listed in § 170.21.

(B) *POA&M closeout*. The OSC must remediate any NOT MET requirements, must undergo a POA&M closeout certification assessment from DCMA DIBCAC, and DCMA DIBCAC must post compliance results into the CMMC instantiation of eMASS within 180 days of the CMMC Status Date associated with the Conditional Level 3 (DIBCAC). If the POA&M is not successfully closed out within the 180-day timeframe, the Conditional Level 3 (DIBAC) CMMC Status for the information system will expire. If Conditional Level 3 (DIBCAC) CMMC Status expires within the period of performance of a contract, standard contractual remedies will apply, and the OSC will be ineligible for additional awards with a requirement for the CMMC Status of Level 3 (DIBCAC) for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(iii) *Final Level 3 (DIBCAC)*. The OSC has achieved the CMMC Status of Final Level 3
(DIBCAC) if the Level 3 certification assessment results in a passing score as defined in § 170.24. This score may be achieved upon initial certification assessment or as the result of a POA&M closeout certification assessment, as applicable.

(iv) *CMMC Status investigation*. The DoD reserves the right to conduct a DCMA DIBCAC assessment of the OSC, as provided for under the 48 CFR 252.204-7020. If the investigative results of a subsequent DCMA DIBCAC assessment show that adherence to the provisions of this part have not been achieved or maintained, these DCMA DIBCAC results will take precedence over any pre-existing CMMC Status. At that time, standard contractual remedies will be available and the OSC will be ineligible for additional awards with CMMC Status requirement of Level 3 (DIBCAC) for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(2) *Affirmation*. Affirmation of the Level 3 (DIBCAC) CMMC Status is required for all Level 3 certification assessments at the time of each assessment, and annually thereafter. Affirmation procedures are provided in § 170.22.

(b) *Contract eligibility*. Prior to award of any contract or subcontract with requirement for CMMC Status of Level 3 (DIBCAC), the following two requirements must be met:

(1) The OSC must achieve, as specified in paragraph (a)(1) of this section, a CMMC
Status of either Conditional Level 3 (DIBCAC) or Final Level 3 (DIBCAC).

(2) The OSC must submit an affirmation of compliance into SPRS, as specified in paragraph (a)(2) of this section.

(c) *Procedures* – (1) *Level 3 certification assessment of the OSC*. The CMMC Level 3 certification assessment process includes:

(i) *Final Level 2 (C3PAO)*. The OSC must achieve a CMMC Status of Final Level 2 (C3PAO) for information systems within the Level 3 CMMC Assessment Scope prior to the CMMC Level 3 certification assessment. The CMMC Assessment Scope for the Level 3

certification assessment must be equal to, or a subset of, the CMMC Assessment Scope associated with the OSC's Final Level 2 (C3PAO). Asset requirements differ for each CMMC Level. Scoping differences are set forth in § 170.19.

(ii) *Initiating the Final Level 3 (DIBCAC)*. The OSC (including ESPs that voluntarily elect to undergo a Level 3 certification assessment) initiates a Level 3 certification assessment by emailing a request to DCMA DIBCAC point of contact found at www.dcma.mil/DIBCAC. The request must include the Level 2 certification assessment unique identifier. DCMA DIBCAC will validate the OSC has achieved a CMMC Status of Level 2 (C3PAO) and will contact the OSC to schedule their Level 3 certification assessment.

(iii) *Conducting the Final Level 3 (DIBCAC)*. DCMA DIBCAC will perform a Level 3 certification assessment in accordance with NIST SP 800-171A Jun2018 (incorporated by reference, see § 170.2) and NIST SP 800-172A Mar2022 (incorporated by reference, see § 170.2) and the CMMC Level 3 scoping requirements set forth in § 170.19(d) for the information systems within the CMMC Assessment Scope. The Level 3 certification assessment will be scored in accordance with the CMMC Scoring Methodology set forth in § 170.24 and DCMA DIBCAC will upload the results into the CMMC instantiation of eMASS. Final results are communicated to the OSC through a CMMC Assessment Findings Report. For assets that changed asset category (i.e., CRMA to CUI Asset) or assessment requirements (i.e., Specialized Assets) between the Level 2 and Level 3 certification assessments, DCMA DIBCAC will perform limited checks of Level 2 security requirements. If the OSC had these upgraded asset categories included in their Level 2 certification assessment, then DCMA DIBCAC may still perform limited checks for compliance. If DCMA DIBCAC identifies that a Level 2 security requirement is NOT MET, the Level 3 assessment process may be paused to allow for remediation, placed on hold, or immediately terminated.

(2) *Security requirement re-evaluation*. A security requirement that is NOT MET (as defined in § 170.24) may be re-evaluated during the course of the Level 3 certification assessment and for 10 business days following the active assessment period if all of the following conditions exist:

(i) Additional evidence is available to demonstrate the security requirement has been MET;

(ii) The additional evidence does not materially impact previously assessed security requirements; and

(iii) The CMMC Assessment Findings Report has not been delivered.

(3) *POA&M.* If a POA&M exists, a POA&M closeout certification assessment will be performed by DCMA DIBCAC within 180-days of the Conditional CMMC Status Date. Additional guidance is located in § 170.21 and in the guidance document listed in paragraph (d) of appendix A to this part.

(4) *Artifact retention and integrity*. The hashed artifacts used as evidence for the assessment must be retained by the OSC for six (6) years from the CMMC Status Date. The hashed artifacts used as evidence for the assessment must be retained by the OSC for six (6) years from the CMMC Status Date. To ensure that the artifacts have not been altered, the OSC must hash the artifact files using a NIST-approved hashing algorithm. Assessors will collect the list of the artifact names, the return value of the hashing algorithm, and the hashing algorithm used and upload that data into the CMMC instantiation of eMASS. Additional guidance for hashing artifacts can be found in the guidance document listed in paragraph (h) of appendix A to this part.

(5) *Level 3 certification assessment with the use of Cloud Service Provider (CSP)*. An OSC may use a cloud environment to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 3 (DIBCAC) under the following circumstances:

(i) The OSC may utilize a CSP product or service offering that meets the FedRAMP

Moderate (or higher) baseline. If the CSP's product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline, the product or service offering must meet security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline in accordance with DoD Policy.

(ii) Use of a CSP does not relieve an OSC of its obligation to implement the 24 Level 3 security requirements. These 24 requirements apply to every environment where the CUI data is processed, stored, or transmitted, when Level 3 (DIBCAC) is the designated CMMC Status. If any of these 24 requirements are inherited from a CSP, the OSC must demonstrate that protection during a Level 3 certification assessment via a Customer Implementation Summary/Customer Responsibility Matrix (CIS/CRM) and associated Body of Evidence (BOE). The BOE must clearly indicate whether the OSC or the CSP is responsible for meeting each requirement and which requirements are implemented by the OSC versus inherited from the CSP.

(iii) In accordance with § 170.19(d)(2), the OSC's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope. As such, the security requirements from the CRM must be documented or referred to in the OSC's SSP.

(6) *Level 3 certification assessment with the use of an ESP, not a CSP*. An OSC may use an ESP that is not a CSP to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 3 (DIBCAC) under the following circumstances:

(i) The use of the ESP, its relationship to the OSC, and the services provided are documented in the OSC's SSP and described in the ESP's service description and customer responsibility matrix.

(ii) The ESP services used to meet OSC requirements are assessed within the scope of the OSC's assessment against all Level 2 and Level 3 security requirements.

(iii) In accordance with § 170.19(d)(2), the OSC's on-premises infrastructure connecting to the ESP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSC's SSP.

§ 170.19 CMMC scoping.

(a) *Scoping requirement*. (1) The CMMC Assessment Scope must be specified prior to assessment in accordance with the requirements of this section. The CMMC Assessment Scope is the set of all assets in the OSA's environment that will be assessed against CMMC security requirements.

(2) The requirements for defining the CMMC Assessment Scope for CMMC Levels 1, 2, and 3 are set forth in this section. Additional guidance regarding scoping can be found in the guidance documents listed in paragraphs (e) through (g) of appendix A to this part.

(b) *CMMC Level 1 scoping.* Prior to performing a Level 1 self-assessment, the OSA must specify the CMMC Assessment Scope.

(1) *Assets in scope for Level 1 self-assessment*. OSA information systems which process, store, or transmit FCI are in scope for CMMC Level 1 and must be self-assessed against applicable CMMC security requirements.

(2) *Assets not in scope for Level 1 self-assessment*—(i) *Out-of-Scope Assets*. OSA information systems which do not process, store, or transmit FCI are outside the scope for CMMC Level 1. An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of FCI beyond the Keyboard/Video/Mouse sent to the VDI client is considered out-of-scope. There are no documentation requirements for out-of-scope assets.

(ii) *Specialized Assets*. Specialized Assets are those assets that can process, store, or transmit FCI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment. Specialized Assets are not part of the Level 1 CMMC Assessment Scope and are not assessed against

CMMC security requirements.

(3) *Level 1 self-assessment scoping considerations.* To scope a Level 1 self-assessment, OSAs should consider the people, technology, facilities, and External Service Providers (ESP) within its environment that process, store, or transmit FCI.

(c) *CMMC Level 2 Scoping*. Prior to performing a Level 2 self-assessment or Level 2 certification assessment, the OSA must specify the CMMC Assessment Scope.

(1) The CMMC Assessment Scope for CMMC Level 2 is based on the specification of asset categories and their respective requirements as defined in table 3 to this paragraph (c)(1). Additional information is available in the guidance document listed in paragraph (f) of appendix A to this part.

Table 3 to § 170.19(c)(1)—CMMC Level 2 Asset Categories and Associated Requirements

Asset Category	Asset Description	OSA Requirements	CMMC Assessment Requirements
Assets that are in the Level 2 CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	• Assets that process, store, or transmit CUI	• Document in the asset inventory • Document asset treatment in the System Security Plan (SSP) • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC Level 2 security requirements	• Assess against all Level 2 security requirements

Security Protection Assets	• Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope	• Document in the asset inventory • Document asset treatment in SSP • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC Level 2 security requirements	• Assess against Level 2 security requirements that are relevant to the capabilities provided
Contractor Risk Managed Assets	• Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place • Assets are not required to be physically or logically separated from CUI assets	• Document in the asset inventory • Document asset treatment in the SSP • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC Level 2 security requirements	• Review the SSP: • If sufficiently documented, do not assess against other CMMC security requirements, except as noted • If OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies

			• The limited check(s) shall not materially increase the assessment duration nor the assessment cost • The limited check(s) will be assessed against CMMC security requirements
Specialized Assets	• Assets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment	• Document in the asset inventory • Document asset treatment in the SSP • Show these assets are managed using the contractor's risk-based security policies, procedures, and practices • Document in the network diagram of the CMMC Assessment Scope	• Review the SSP • Do not assess against other CMMC security requirements
Assets that are not in the Level 2 CMMC Assessment Scope			

Out-of-Scope Assets	• Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets • Assets that are physically or logically separated from CUI assets • Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset • An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset	• Prepare to justify the inability of an Out-ofScope Asset to process, store, or transmit CUI	• None

(2)(i) Table 4 to this paragraph (c)(2)(i) defines the requirements to be met when utilizing an External Service Provider (ESP). The OSA must consider whether the ESP is a Cloud Service Provider (CSP) and whether the ESP processes, stores, or transmits CUI and/or Security Protection Data (SPD).

Table 4 to § 170.19(c)(2)(i)—ESP Scoping Requirements

	When utilizing an ESP that is:

When the ESP processes, stores, or transmits:	A CSP	Not a CSP
CUI (with or without SPD)	The CSP shall meet the FedRAMP requirements in 48 CFR 252.204-7012.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as part of the OSA's assessment.
SPD (without CUI)	The services provided by the CSP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.
Neither CUI nor SPD	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.

(ii) The use of an ESP, its relationship to the OSA, and the services provided need to be documented in the OSA's SSP and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSA and ESP with respect to the services provided. Note that the ESP may voluntarily undergo a CMMC certification assessment to reduce the ESP's effort required during the OSA's assessment. The minimum assessment type for the ESP is dictated by the OSA's DoD contract requirement.

(d) *CMMC Level 3 scoping*. Prior to performing a Level 3 certification assessment, the CMMC Assessment Scope must be specified.

(1) The CMMC Assessment Scope for Level 3 is based on the specification of asset categories and their respective requirements as set forth in table 5 to this paragraph (d)(1). Additional information is available in the guidance document listed in paragraph (g) of appendix A to this part.

Table 5 to § 170.19(d)(1)—CMMC Level 3 Asset Categories and Associated Requirements

Asset Category	Asset Description	OSC Requirements	CMMC Assessment Requirements

Assets that are in the Level 3 CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	• Assets that process, store, or transmit CUI • Assets that can, but are not intended to, process, store, or transmit CUI (defined as Contractor Risk Managed Assets in table 1 to paragraph (c)(1) of this section CMMC Scoping)	• Document in the asset inventory • Document asset treatment in the System Security Plan (SSP) • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC Level 2 and Level 3 security requirements	• Limited check against Level 2 and assess against all Level 3 CMMC security requirements

Asset Category	Asset Description	OSC Requirements	CMMC Assessment Requirements
Security			

Protecti Assets	• Assets that provide security functions or capabilities to the OSC's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI	• Document in the asset inventory • Document asset treatment in the SSP • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC Level 2 and Level 3 security requirements	• Limited check against Level 2 and assess against all Level 3 CMMC security requirements that are relevant to the capabilities provided

Asset Category	Asset Description	OSC Requirements	CMMC Assessment Requirements
Specialized			

Assets	• Assets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment	• Document in the asset inventory • Document asset treatment in the SSP • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC Level 2 and Level 3 security requirements	• Limited check against Level 2 and assess against all Level 3 CMMC security requirements • Intermediary devices are permitted to provide the capability for the specialized asset to meet one or more CMMC security requirements
Assets that are not in the Level 3 CMMC Assessment Scope			
Asset Category	**Asset Description**	**OSC Requirements**	**CMMC Assessment Requirements**
Out-of-			

Scope Assets	• Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets • Assets that are physically or logically separated from CUI assets • Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset • An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset	• Prepare to justify the inability of an Out-of-Scope Asset to process, store, or transmit CUI	• None

(2)(i) Table 6 to this paragraph (d)(2)(i) defines the requirements to be met when utilizing an External Service Provider (ESP). The OSA must consider whether the ESP is a Cloud Service Provider (CSP) and whether the ESP processes, stores, or transmits CUI and/or Security Protection Data (SPD).

Table 6 to § 170.19(d)(2)(i)—ESP Scoping Requirements

	When utilizing an ESP that is:	
When the ESP processes, stores, or transmits:	**A CSP**	**Not a CSP**

CUI (with or without SPD)	The CSP shall meet the FedRAMP requirements in 48 CFR 252.204-7012.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as part of the OSA's assessment.
SPD (without CUI)	The services provided by the CSP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.
Neither CUI nor SPD	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.

(ii) The use of an ESP, its relationship to the OSC, and the services provided need to be documented in the OSC's SSP and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSC and ESP with respect to the services provided. Note that the ESP may voluntarily undergo a CMMC certification assessment to reduce the ESP's effort required during the OSA's assessment. The minimum. The minimum assessment type for the ESP is dictated by the OSC's DoD contract requirement.

(e) *Relationship between Level 2 and Level 3 CMMC Assessment Scope*. The Level 3 CMMC Assessment Scope must be equal to or a subset of the Level 2 CMMC Assessment Scope in accordance with § 170.18(a) (e.g., a Level 3 data enclave with greater restrictions and protections within a Level 2 data enclave). Any Level 2 POA&M items must be closed prior to the initiation of the Level 3 certification assessment. DCMA DIBCAC may check any Level 2 security requirement of any in-scope asset. If DCMA DIBCAC identifies that a Level 2 security requirement is NOT MET, the Level 3 assessment process may be paused to allow for remediation, placed on hold, or immediately terminated. For further information regarding scoping of CMMC Level 3 assessments please contact DCMA DIBCAC at www.dcma.mil/DIBCAC/.

§ 170.20 Standards acceptance.

(a) *NIST SP 800-171 R2 DoD assessments*. In order to avoid duplication of efforts, thereby reducing the aggregate cost to industry and the Department, OSCs that have completed a

DCMA DIBCAC High Assessment aligned with CMMC Level 2 Scoping will be given the CMMC Status of Final Level 2 (C3PAO) under the following conditions:

(1) *DCMA DIBCAC High Assessment*. An OSC that achieved a perfect score with no open POA&M from a DCMA DIBCAC High Assessment conducted prior to the effective date of this rule, will be given a CMMC Status of Level 2 Final (C3PAO) with a validity period of three (3) years from the date of the original DCMA DIBCAC High Assessment. DCMA DIBCAC will identify assessments that meet these criteria and verify that SPRS accurately reflects the CMMC Status. Eligible DCMA DIBCAC High Assessments include ones conducted with Joint Surveillance in accordance with the DCMA Manual 2302-01 Surveillance. The scope of the Level 2 certification assessment is identical to the scope of the DCMA DIBCAC High Assessment. In accordance with § 170.17(a)(2), the OSC must also submit an affirmation in SPRS and annually thereafter to achieve contractual eligibility.

(2) [Reserved].

(b) [Reserved].

§ 170.21 Plan of Action and Milestones requirements.

(a) *POA&M*. For purposes of achieving a Conditional CMMC Status, an OSA is only permitted to have a POA&M for select requirements scored as NOT MET during the CMMC assessment and only under the following conditions:

(1) *Level 1 self-assessment*. A POA&M is not permitted at any time for Level 1 selfassessments.

(2) *Level 2 self-assessment and Level 2 certification assessment*. An OSA is only permitted to achieve the CMMC Status of Conditional Level 2 (Self) or Conditional Level 2 (C3PAO), as appropriate, if all the following conditions are met:

(i) The assessment score divided by the total number of CMMC Level 2 security requirements is greater than or equal to 0.8;

(ii) None of the security requirements included in the POA&M have a point value of greater than 1 as specified in the CMMC Scoring Methodology set forth in § 170.24, except SC.L2-3.13.11 CUI Encryption may be included on a POA&M if encryption is employed but it is not FIPS-validated, which would result in a point value of 3; and

(iii) None of the following security requirements are included in the POA&M:

(A) AC.L2-3.1.20 External Connections (CUI Data).

(B) AC.L2-3.1.22 Control Public Information (CUI Data).

(C) CA.L2-3.12.4 System Security Plan

(D) PE.L2-3.10.3 Escort Visitors (CUI Data).

(E) PE.L2-3.10.4 Physical Access Logs (CUI Data).

(F) PE.L2-3.10.5 Manage Physical Access (CUI Data).

(3) *Level 3 certification assessment*. An OSC is only permitted to achieve the CMMC Status of Conditional Level 3 (DIBCAC) if all the following conditions are met:

(i) The assessment score divided by the total number of CMMC Level 3 security requirements is greater than or equal to 0.8; and

(ii) The POA&M does not include any of following security requirements:

(A) IR.L3-3.6.1e Security Operations Center.

(B) IR.L3-3.6.2e Cyber Incident Response Team.

(C) RA.L3-3.11.1e Threat-Informed Risk Assessment.

(D) RA.L3-3.11.6e Supply Chain Risk Response.

(E) RA.L3-3.11.7e Supply Chain Risk Plan.

(F) RA.L3-3.11.4e Security Solution Rationale.

(G) SI.L3-3.14.3e Specialized Asset Security.

(b) *POA&M closeout assessment*. A POA&M closeout assessment is a CMMC assessment that assesses only the NOT MET requirements that were identified with POA&M in the initial assessment. The closing of a POA&M must be confirmed by a POA&M closeout assessment within 180-days of the Conditional CMMC Status Date. If the POA&M is not successfully closed out within the 180-day timeframe, the Conditional CMMC Status for the information system will expire.

(1) *Level 2 self-assessment*. For a Level 2 self-assessment, the POA&M closeout selfassessment shall be performed by the OSA in the same manner as the initial self-assessment.

(2) *Level 2 certification assessment*. For Level 2 certification assessment, the POA&M closeout certification assessment must be performed by an authorized or accredited C3PAO.

(3) *Level 3 certification assessment*. For Level 3 certification assessment, DCMA DIBCAC will perform the POA&M closeout certification assessment.

§ 170.22 Affirmation.

(a) *General*. The OSA must affirm continuing compliance with the appropriate level selfassessment or certification assessment. An Affirming Official from each OSA, whether a prime or subcontractor, must affirm the continuing compliance of their respective organizations with the specified security requirement after every assessment, including POA&M closeout, and annually thereafter. Affirmations are entered electronically in SPRS. The affirmation shall be submitted in accordance with the following requirements:

(1) *Affirming Official*. The Affirming Official is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations.

(2) *Affirmation content*. Each CMMC affirmation shall include the following information:

(i) Name, title, and contact information for the Affirming Official; and

(ii) Affirmation statement attesting that the OSA has implemented and will maintain implementation of all applicable CMMC security requirements to their CMMC Status for all information systems within the relevant CMMC Assessment Scope.

(3) *Affirmation submission*. The Affirming Official shall submit a CMMC affirmation in the following instances:

(i) Upon achievement of a Conditional CMMC Status, as applicable;

(ii) Upon achievement of a Final CMMC Status;(iii) Annually following a Final CMMC Status Date; and

(iv) Following a POA&M closeout assessment, as applicable.

(b) *Submission procedures*. All affirmations shall be completed in SPRS. The Department will verify submission of the affirmation in SPRS to ensure compliance with CMMC solicitation or contract requirements.

(1) *Level 1 self-assessment*. At the completion of a Level 1 self-assessment and annually thereafter, the Affirming Official shall submit a CMMC affirmation attesting to continuing compliance with all requirements of the CMMC Status Level 1 (Self).

(2) *Level 2 self-assessment*. At the completion of a Level 2 self-assessment and annually following a Final CMMC Status Date, the Affirming Official shall submit a CMMC affirmation attesting to continuing compliance with all requirements of the CMMC Status Level 2 (Self). An affirmation shall also be submitted at the completion of a POA&M closeout self-assessment.

(3) *Level 2 certification assessment*. At the completion of a Level 2 certification assessment and annually following a Final CMMC Status Date, the Affirming Official shall submit a CMMC affirmation attesting to continuing compliance with all requirements of the CMMC Status Level 2 (C3PAO). An affirmation shall also be submitted at the completion of a POA&M closeout certification assessment.

(4) *Level 3 certification assessment*. At the completion of a Level 3 certification assessment and annually following a Final CMMC Status Date, the Affirming Official shall submit a CMMC affirmation attesting to continuing compliance with all requirements of the CMMC Status Level 3 (DIBCAC). Because C3PAOs and DCMA DIBCAC check for compliance with different requirements in their respective assessments, OSCs must annually affirm their CMMC Status of Level 2 (C3PAO) in addition to their CMMC Status of Level 3

(DIBCAC) to maintain eligibility for contracts requiring compliance with Level 3. An affirmation shall also be submitted at the completion of a POA&M closeout certification assessment.

§ 170.23 Application to subcontractors.

(a) CMMC requirements apply to prime contractors and subcontractors throughout the supply chain at all tiers that will process, store, or transmit any FCI or CUI on contractor information systems in the performance of the DoD contract or subcontract. Prime contractors shall comply and shall require subcontractors to comply with and to flow down CMMC requirements, such that compliance will be required throughout the supply chain at all tiers with the applicable CMMC level and assessment type for each subcontract as follows:

(1) If a subcontractor will only process, store, or transmit FCI (and not CUI) in performance of the subcontract, then a CMMC Status of Level 1 (Self) is required for the subcontractor.

(2) If a subcontractor will process, store, or transmit CUI in performance of the subcontract, then a CMMC Status of Level 2 (Self) is the minimum requirement for the subcontractor.

(3) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contract has a requirement for a CMMC Status of Level 2 (C3PAO), then the CMMC Status of Level 2 (C3PAO) is the minimum requirement for the subcontractor.

(4) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contract has a requirement for the CMMC Status of Level 3

(DIBCAC), then the CMMC Status of Level 2 (C3PAO) is the minimum requirement for the subcontractor.

(b) As with any solicitation or contract, the DoD may provide specific guidance pertaining to flow-down.

§ 170.24 CMMC Scoring Methodology.

(a) *General*. This scoring methodology is designed to provide a measurement of an OSA's implementation status of the NIST SP 800-171 R2 security requirements (incorporated by reference elsewhere in this part, see § 170.2) and the selected NIST SP 800-172 Feb2021 security requirements (incorporated by reference elsewhere in this part, see § 170.2). The CMMC Scoring Methodology is designed to credit partial implementation only in limited cases (e.g., multi-factor authentication IA.L2-3.5.3).

(b) *Assessment findings*. Each security requirement assessed under the CMMC Scoring Methodology must result in one of three possible assessment findings, as follows:

(1) *Met.* All applicable objectives for the security requirement are satisfied based on evidence. All evidence must be in final form and not draft. Unacceptable forms of evidence include but are not limited to working papers, drafts, and unofficial or unapproved policies.

(i) Enduring exceptions when described, along with any mitigations, in the system security plan shall be assessed as MET.

(ii) Temporary deficiencies that are appropriately addressed in operational plans of action (i.e., include deficiency reviews and show progress towards the implementation of corrections to reduce or eliminate identified vulnerabilities) shall be assessed as MET.

(2) *Not Met.* One or more applicable objectives for the security requirement is not satisfied. During an assessment, for each security requirement objective marked NOT MET, the assessor will document why the evidence does not conform.

(3) *Not Applicable (N/A).* A security requirement and/or objective does not apply at the time of the CMMC assessment. For example, Public-Access System Separation (SC.L2-3.13.5) might be N/A if there are no publicly accessible systems within the CMMC Assessment Scope. During an assessment, an assessment objective assessed as N/A is equivalent to the same assessment objective being assessed as MET.

(c) *Scoring*. At each CMMC Level, security requirements are scored as follows:

(1) *CMMC Level 1*. All CMMC Level 1 security requirements must be fully implemented to be considered MET. No POA&M is permitted for CMMC Level 1, and selfassessment results are scored as MET or NOT MET in their entirety.

(2) *CMMC Level 2 Scoring Methodology*. The maximum score achievable for a Level 2 self-assessment or Level 2 certification assessment is equal to the total number of CMMC Level 2 security requirements. If all CMMC Level 2 security requirements are MET, OSAs are awarded the maximum score. For each requirement NOT MET, the associated value of the security requirement is subtracted from the maximum score, which may result in a negative score.

(i) *Procedures.* (A) Scoring methodology for Level 2 self-assessment and Level 2 certification assessment is based on all CMMC Level 2 security requirement objectives, including those NOT MET.

(B) In the CMMC Level 2 Scoring Methodology, each security requirement has a value (e.g., 1, 3 or 5), which is related to the designation by NIST as basic or derived security requirements. Per NIST SP 800-171 R2, the basic security requirements are obtained from FIPS PUB 200 Mar2006, which provides the high-level and fundamental security requirements for Federal information and systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST SP 800-53 R5.

(*1*) For NIST SP 800-171 R2 basic and derived security requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration of CUI, five (5) points are subtracted from the maximum score. The basic and derived security requirements with a value of five (5) points include:

(*i*) *Basic security requirements*. AC.L2-3.1.1, AC.L2-3.1.2, AT.L2-3.2.1, AT.L2-3.2.2, AU.L2-3.3.1, CM.L2-3.4.1, CM.L2-3.4.2, IA-L2-3.5.1, IA-L2-3.5.2, IR.L2-3.6.1, IR.L2-3.6.2, MA.L2-3.7.2, MP.L2-3.8.3, PS.L2-3.9.2, PE.L2-3.10.1, PE.L2-3.10.2, CA.L2-3.12.1, CA.L2-3.12.3, SC.L2-3.13.1, SC.L2-3.13.2, SI.L2-3.14.1, SI.L2-3.14.2, and SI.L2-3.14.3.

(*ii*) *Derived security requirements*. AC.L2-3.1.12, AC.L2-3.1.13, AC.L2-3.1.16, AC.L23.1.17, AC.L2-3.1.18, AU.L2-3.3.5, CM.L2-3.4.5, CM.L2-3.4.6, CM.L2-3.4.7, CM.L2-3.4.8, IA.L2-3.5.10, MA.L2-3.7.5, MP.L2-3.8.7, RA.L2-3.11.2, SC.L2-3.13.5, SC.L2-3.13.6, SC.L2-
3.13.15, SI.L2-3.14.4, and SI.L2-3.14.6.

(*2*) For basic and derived security requirements that, if not implemented, have a specific and confined effect on the security of the network and its data, three (3) points are subtracted from the maximum score. The basic and derived security requirements with a value of three (3) points include:

(i) *Basic security requirements*. AU.L2-3.3.2, MA.L2-3.7.1, MP.L2-3.8.1, MP.L2-3.8.2, PS.L2-3.9.1, RA.L2-3.11.1, and CA.L2-3.12.2.

(ii) *Derived security requirements*. AC.L2-3.1.5, AC.L2- 3.1.19, MA.L2-3.7.4, MP.L2-3.8.8, SC.L2-3.13.8, SI.L2- 3.14.5, and SI.L2-3.14.7.

(3) All remaining derived security requirements, other than the exceptions noted, if not implemented, have a limited or indirect effect on the security of the network and its data. For these, 1 point is subtracted from the maximum score.

(4) Two derived security requirements, IA.L2-3.5.3 and SC.L2-3.13.11, can be partially effective even if not completely or properly implemented, and the points deducted may be adjusted depending on how the security requirement is implemented.

(i) Multi-factor authentication (MFA) (CMMC Level 2 security requirement IA.L2-3.5.3) is typically implemented first for remote and privileged users (since these users are both limited in number and more critical) and then for the general user, so three (3) points are subtracted from the maximum score if MFA is implemented only for remote and privileged users. Five (5) points are subtracted from the maximum score if MFA is not implemented for any users.

(ii) FIPS-validated encryption (CMMC Level 2 security requirement SC.L2-3.13.11) is required to protect the confidentiality of CUI. If encryption is employed, but is not

FIPSvalidated, three (3) points are subtracted from the maximum score; if encryption is not employed; five (5) points are subtracted from the maximum score.

(5) OSAs must have a System Security Plan (SSP) (CMMC security requirement CA.L23.12.4) in place at the time of assessment to describe each information system within the CMMC Assessment Scope. The absence of an up to date SSP at the time of the assessment would result in a finding that '*an assessment could not be completed due to incomplete information and noncompliance with 48 CFR 252.204-7012*.'

(6) For each NOT MET security requirement the OSA must have a POA&M in place. A POA&M addressing NOT MET security requirements is not a substitute for a completed requirement. Security requirements not implemented, whether described in a POA&M or not, is assessed as 'NOT MET.'

(7) Specialized Assets must be evaluated for their asset category per the CMMC scoping guidance for the level in question and handled accordingly as set forth in § 170.19.

(8) If an OSC previously received a favorable adjudication from the DoD CIO indicating that a security requirement is not applicable or that an alternative security measure is equally effective (in accordance with 48 CFR 252.204-7008 or 48 CFR 252.204-7012), the DoD CIO adjudication must be included in the system security plan to receive consideration during an assessment. A security requirement for which implemented security measures have been adjudicated by the DoD CIO as equally effective is assessed as MET if there have been no changes in the environment.

(ii) *CMMC Level 2 Scoring Table*. CMMC Level 2 scoring has been assigned based on the methodology set forth in table 1 to this paragraph (c)(2)(ii).

Table 7 to § 170.24(c)(2)(ii)—CMMC Level 2 Scoring Table

CMMC Level 2 Requirement Categories	Point Value Subtracted from Maximum Score
Basic Security Requirements	
If not implemented, could lead to significant exploitation of the network, or exfiltration of CUI	5
If not implemented, has specific and confined effect on the security of the network and its data	3
Derived Security Requirements	
If not implemented, could lead to significant exploitation of the network, or exfiltration of CUI	5

If not completely or properly implemented, could be partially effective and points adjusted depending on how the security requirement is implemented - Partially effective implementation - 3 points - Non-effective (not implemented at all) - 5 points	3 or 5
If not implemented, has specific and confined effect on the security of the network and its data	3
If not implemented, has a limited or indirect effect on the security of the network and its data	1

(3) *CMMC Level 3 assessment scoring methodology*. CMMC Level 3 scoring does not utilize varying values like the scoring for CMMC Level 2. All CMMC Level 3 security requirements use a value of one (1) point for each security requirement. As a result, the maximum score achievable for a Level 3 certification assessment is equivalent to the total number of the selected subset of NIST SP 800-172 Feb2021 security requirements for CMMC Level 3, see § 170.14(c)(4). The maximum score is reduced by one (1) point for each security requirement NOT MET. The CMMC Level 3 scoring methodology reflects the fact that all CMMC Level 2 security requirements must already be MET (for the Level 3 CMMC Assessment Scope). A maximum score on the Level 2 certification assessment is required to be eligible to initiate a Level 3 certification assessment. The Level 3 certification assessment score is equal to the number of CMMC Level 3 security requirements that are assessed as MET.

Appendix A to Part 170—Guidance

Guidance documents include:

(a) "CMMC Model Overview" available at https://DoDcio.defense.gov/CMMC/.

(b) "CMMC Assessment Guide - Level 1" available at https://DoDcio.defense.gov/CMMC/.

(c) "CMMC Assessment Guide - Level 2" available at https://DoDcio.defense.gov/CMMC/.

(d) "CMMC Assessment Guide - Level 3" available at https://DoDcio.defense.gov/CMMC/.

(e) "CMMC Scoping Guide - Level 1" available at https://DoDcio.defense.gov/CMMC/.

(f) "CMMC Scoping Guide - Level 2" available at https://DoDcio.defense.gov/CMMC/.

(g) "CMMC Scoping Guide - Level 3" available at https://DoDcio.defense.gov/CMMC/.

(h) "CMMC Hashing Guide" available at https://DoDcio.defense.gov/CMMC/.

Dated: September 30, 2024.

Patricia L. Toppings,

OSD Federal Register Liaison Officer,

Department of Defense.

[FR Doc. 2024-22905 Filed: 10/11/2024 8:45 am; Publication Date: 10/15/2024]