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: Proposed rule.

SUMMARY: DoD is proposing to establish requirements for a comprehensive and scalable assessment mechanism to ensure defense contractors and subcontractors have, as part of the Cybersecurity Maturity Model Certification (CMMC) Program, implemented required security measures to expand application of existing security requirements for Federal Contract Information (FCI) and add new Controlled Unclassified Information (CUI) security requirements for certain priority programs. DoD currently requires covered 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 Rev 2 to provide adequate security for sensitive unclassified DoD information that is processed, stored, or transmitted on contractor information systems and to document their implementation status, including any plans of action for any NIST SP 800-171 Rev 2 requirement not yet implemented, in a System Security Plan (SSP). 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.

DATES: Comments must be received by [INSERT DATE 60 DAYS FROM DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may use the following methods to submit comments on:

- the proposed rule, identified by docket number DoD-2023-OS-0063 and/or Regulatory Identifier Number (RIN) 0790-AL49 and title
- the guidance in the Appendix documents, identified by docket number DoD-2023-OS-0096 and title
- the information collection requirements, identified by docket number DoD-2023-OS-0097 and title

Comment Submission Methods include:

• Federal eRulemaking Portal: https://www.regulations.gov. Follow the instructions for submitting comments.

• Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number or RIN for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Diane Knight, Office of the DoD CIO, 202–770–9100.

SUPPLEMENTARY INFORMATION:

History of the Program

The CMMC Program is designed to verify protection of sensitive unclassified information shared between the Department and its contractors and subcontractors or generated by the contractors and subcontractors. CMMC increases assurance that contractors and subcontractors are meeting cybersecurity requirements applying to acquisition programs and systems processing CUI.

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 an interim rule, Defense Federal Acquisition Regulation Supplement (DFARS): Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)[4], which implemented the DoD's initial vision for the CMMC Program ("CMMC 1.0") 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 interim rule became effective on 30 November 2020, establishing a five-year phase-in period. In response to approximately 750 public comments on the CMMC 1.0 Program, in March 2021, the Department initiated an internal review of CMMC's implementation.

---

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

In November 2021, the Department announced "CMMC 2.0," 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 CMMC 2.0 Program has three key features:

- **Tiered Model**: CMMC requires companies entrusted with national security 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.
- **Implementation through Contracts**: Once CMMC is fully implemented, certain DoD contractors handling sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

CMMC 2.0 Overview as Proposed by This Rule

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 FAR clause 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*[5]. FAR clause 52.204-21 requires compliance with 15 security requirements, FAR 52.204-21 (b)(1), items (i) through (xv). These requirements are elementary for any entity wishing to achieve basic cybersecurity.

[5] https://www.acquisition.gov/far/52.204-21

Defense contracts involving the transfer of CUI to a non-Government organization may include applicable requirements of DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*[6]. The DFARS clause 252.204-7012 requires defense contractors to provide adequate security on all covered contractor information systems by implementing the 110 security requirements specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. The DFARS clause 252.204-7012 includes additional requirements; for example, defense contractors must meet Federal Risk and Authorization Management Program (FedRAMP) standards by confirming that their Cloud Service Providers (CSP) have achieved the FedRAMP Baseline Moderate or Equivalent standard. The DFARS clause 252.204-7012 also requires defense contractors to flow down all the requirements to their subcontractors.

Currently, to comply with DFARS clause 252.204-7012, contractors are required to develop a System Security Plan (SSP)[7] 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 self-assessment. Self-assessment scores, as referenced in DFARS clause 252.204-7020, must be submitted in the DoD's Supplier Performance Risk System (SPRS)[8]. The highest score is 110, meaning all 110 NIST SP 800-171 security requirements have been fully implemented. If a contractor's SPRS score is less than 110, indicating security gaps exist, then the contractor must create a Plan of Action (POA)[9] 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 go through each NIST SP 800-171 security

---

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

[7] Required since November 2016, NIST SP 800-171 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."

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

[9] The POA requirement described under DFARS clause 252.204-7012 is different from a Plan of Action and Milestones (POA&M) requirement in CMMC as POAs do not require milestones.

requirement and explain how the requirement is implemented, monitored, and enforced. This can be through policy, technology, or a combination of both. The SSP will also outline the roles and responsibilities of security personnel to ensure that CUI is appropriately protected.

In November 2020, the DoD released its DFARS Interim Rule, the *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements*[10]. The goal of this rule was to increase compliance with its cybersecurity regulations and improve security throughout the DIB. This rule introduced three new clauses – DFARS clause 252.204-7019, DFARS clause 252.204-7020, and DFARS clause 252.204-7021.

- DFARS clause 252.204-7019 strengthens DFARS clause 252.204-7012 by requiring contractors to conduct a NIST SP 800-171 self-assessment according to NIST SP 800-171 DoD Assessment Methodology[11]. Self-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 strengthens 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, DFARS clause 252.204-7021 requires contractors to achieve the CMMC level required in the DoD contract. DFARS clause 252.204-7021 also stipulates contractors will be responsible for flowing down the CMMC requirements to their subcontractors.

---

[10] https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of

[11]https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf

Additional Requirements for Defense Contractors and Subcontractors Discussed in This Proposed Rule

A key difference between the DFARS 252.204-7012 and CMMC Level 2 requirements is that compliance with NIST SP 800-171 under DFARS 252.204-7012 has not been consistently verified. Under CMMC, compliance will be checked by independent third-party assessors certified by DoD.

When this 32 CFR CMMC Program rule is finalized, solicitations for defense contracts involving the processing, storing, or transmitting of FCI or CUI on a non-Federal system will, in most cases, have a CMMC level and assessment type requirement a contractor must meet to be eligible for a contract award. CMMC-related contractual processes will be addressed in DoD's DFARS Case 2019-D041, *Assessing Contractor Implementation of Cybersecurity Requirements,* which will be proposed by the Department in a separate rulemaking[12].

This rule establishes the CMMC Program and defines requirements both in general and based on the specific CMMC level and assessment type required by the contract and applicable subcontract. Each CMMC level and assessment type is described.

1. Contracts or subcontracts with a CMMC Level 1 Self-Assessment Requirement

a. Security Requirements

For CMMC Level 1, contractors and applicable subcontractors are already required to implement the 15 security requirements currently required by the FAR clause 52.204-21.

b. Assessment Requirements (New)

At Level 1, CMMC adds a requirement for contractors and applicable subcontractors to verify through self-assessment that all applicable security requirements outlined in FAR clause 52.204-21 have been implemented. This self-assessment must be performed annually and the results must be entered electronically in the Supplier Performance Risk System (SPRS) (see § 170.15

[12] Information on the Department's agenda for all rulemakings can be found at https://www.reginfo.gov/public/do/eAgendaMain and then selecting the relevant agency and rule name.

for details on CMMC Level 1 Self-Assessment requirements and procedures, and specifically § 170.15(a)(1)(i) for the information collection).

c. Affirmation Requirements (New)

A senior official from the prime contractor and any applicable subcontractor will be required to annually affirm continuing compliance with the specified security requirements. Affirmations are entered electronically in SPRS (see § 170.22 for details on Affirmation requirements and procedures).

2. Contracts or subcontracts with a CMMC Level 2 Self-Assessment Requirement

a. Security Requirements

For CMMC Level 2, contractors and applicable subcontractors are already required to implement the 110 security requirements currently required by the DFARS clause 252.204-7012, which are aligned with NIST SP 800-171 Rev 2.

b. Assessment Requirements (New)

At Level 2, CMMC adds a requirement for contractors and applicable subcontractors to verify that all applicable security requirements outlined in NIST SP 800-171 Rev 2 and required via DFARS clause 252.204-7012 have been implemented. As determined by DoD, program contracts will include either a CMMC Level 2 Self-Assessment requirement or a CMMC Level 2 Certification Assessment requirement to verify a contractor's implementation of the CMMC Level 2 security requirements. Selected requirements are allowed to have a Plan of Action and Milestones (POA&M) that must be closed out within 180 days of the assessment (see § 170.21 for details on POA&M). This self-assessment must be performed on a triennial basis and the results must be entered electronically in SPRS (see § 170.16 for details on CMMC Level 2 Self-Assessment requirements and procedures, and specifically § 170.16(a)(1)(i) for information collection).

c. Affirmation Requirements (New)

A senior official from the prime contractor and any applicable subcontractor will be required to affirm continuing compliance with the specified security requirements after every assessment, including POA&M closeout, and annually thereafter. Affirmations are entered electronically in SPRS (see § 170.22 for details on Affirmation requirements and procedures).

3. Contracts or subcontracts with a CMMC Level 2 Certification Assessment Requirement

a. Security Requirements

For CMMC Level 2 Certification Assessment, contractors and applicable subcontractors are already required to implement the security requirements currently required by the DFARS clause 252.204-7012, which are aligned with NIST SP 800-171 Rev 2.

b. Assessment Requirements (New)

At Level 2, CMMC adds a requirement for contractors and applicable subcontractors to verify that all applicable security requirements outlined in NIST SP 800-171 Rev 2 and required via DFARS clause 252.204-7012 have been implemented. As determined by DoD, program contracts will include either a CMMC Level 2 Self-Assessment requirement or a CMMC Level 2 Certification Assessment requirement to verify a contractor's implementation of the CMMC Level 2 security requirements. Selected requirements are allowed to have a POA&M that must be closed out within 180 days of the assessment (see § 170.21 for details on POA&M). The final certification will have up to a three-year duration. The third-party assessment organization will enter the assessment information electronically into the CMMC Enterprise Mission Assurance Support Service (eMASS), that will electronically transmit the assessment results into SPRS (see § 170.17 for details on CMMC Level 2 Certification Assessment requirements and procedures, and specifically § 170.17(a)(1)(i) for information collection).

c. Affirmation Requirements (New)

A senior official from the prime contractor and any applicable subcontractor will be required to affirm continuing compliance with the specified security requirements after every assessment, including POA&M closeout, and annually thereafter. Affirmations are entered electronically in SPRS (see § 170.22 for details on Affirmation requirements, procedures, and information collection).

4. Contracts or subcontracts with a CMMC Level 3 Certification Assessment Requirement

a. Security Requirements (New)

For CMMC Level 3, when CMMC becomes a final rule, contractors and applicable subcontractors will be required to implement the 24 selected security requirements from NIST SP 800-172, as detailed in table 1 to § 170.14(c)(4). CMMC Level 2 is a prerequisite for CMMC Level 3.

b. Assessment Requirements (New)

At Level 3, CMMC adds a requirement for contractors and applicable subcontractors to verify through DoD assessment and receive certification that all applicable CMMC Level 3 security requirements from NIST SP 800-172 have been implemented. Selected requirements are allowed to have a POA&M that must be closed out within 180 days of the assessment (see § 170.21 for details on POA&Ms). The final certification will be valid for up to three years. The DoD assessor will enter the assessment information electronically into the eMASS, that will electronically transmit the assessment results into SPRS (see § 170.18 for details on CMMC Level 3 Certification Assessment requirements and procedures, and specifically § 170.18(a)(1)(i) for information collection).

c. Affirmation Requirements (New)\

A senior official from the prime contractor and any applicable subcontractor will be required to affirm continuing compliance with the specified security requirements after every assessment, including POA&M closeout, and annually thereafter. Affirmations are entered electronically in

SPRS (see § 170.22 for details on Affirmation requirements, procedures, and information collection).

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; NIST SP 800-171 Rev 2; and selected requirements from the NIST SP 800-172, 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 (as detailed in the Office of the Federal Register's Incorporation By Reference (IBR) Handbook, June 2023). 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, revision 2, titled "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" 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" 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. SP 800-39 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, revision 5, titled "Security and Privacy Controls for Information Systems and Organizations" 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 800-82, revision 2, titled "Guide to Industrial Control Systems (ICS) Security" 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" 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, revision 1, titled "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach" 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, revision 2, titled "Security Requirements for Controlled Unclassified Information" 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" provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST SP 800-171. 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 Controlled Unclassified Information" 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 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" 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. 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) government-sponsored 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) Committee on National Security Systems (CNSS) Instruction No. 4009 provides a glossary of terms and applies to all U.S. Government Departments, Agencies, Bureaus and Offices, supporting contractors and agents that collect, generate, process, store, display, transmit or receive classified or controlled unclassified information, or that operate, use, or connect to National Security Systems (NSS). This document is incorporated by reference as a source for definitions.

(n) ISO/IEC 17011:2017, titled "Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies" 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.

(o) ISO/IEC 17020:2012, titled "Conformity assessment — Requirements for the operation of various types of bodies performing inspection" 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, and it applies to any stage of inspection." This document is incorporated by reference as a source for requirements on the CMMC Ecosystem.

(p) ISO/IEC 17024:2012, titled "Conformity assessment — Requirements for the operation of various types of bodies performing inspection" 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, and private-sector businesses or other entities that are specified in Subpart C. Government information systems that are operated by contractors and subcontractors in support of the Government do not apply to this rule. 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 will apply to a contract or procurement. Applicability of the CMMC Level 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 the CMMC revision to DFARS 252.204-7021. More information regarding Phase 1 can be found in § 170.3(e)(1). Phase 2 begins six months 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 and welcomes comments on these definitions as part of the proposed rule:

- Accreditation
- Accreditation Body
- Assessment
- Self-Assessment
- CMMC Level 2 Certification Assessment
- CMMC Level 3 Certification Assessment
- Assessment Findings Report
- Assessment Team
- Asset Categories
- Authorized
- CMMC Assessment and Certification Ecosystem
- CMMC Assessment Scope

- CMMC Assessor and Instructor Certification Organization (CAICO)
- CMMC instantiation of eMASS
- CMMC Level 1 Self-Assessment
- CMMC Level 2 Conditional Certification Assessment
- CMMC Level 2 Conditional Self-Assessment
- CMMC Level 2 Final Certification Assessment
- CMMC Level 2 Final Self-Assessment
- CMMC Level 3 Conditional Certification Assessment
- CMMC Level 3 Final Certification Assessment
- CMMC Third-Party Assessment Organization (C3PAO)
- Contractor Risk Managed Assets
- Controlled Unclassified Information (CUI) Assets
- External Service Provider (ESP)
- Federal Contract Information (FCI) Assets
- 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
- Specialized Assets
- 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, safeguards defined in NIST SP 800-172 and DoD-specified parameters (see table 1 to § 170.14(c)(4)) may be required.

Program Managers and requiring activities identify the applicable CMMC Level. Factors used to determine which CMMC Level 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 52.204-21, DFARS subpart 204.73, or any other applicable safeguarding of information requirement. The CMMC Program verifies implementation of security requirements in FAR 52.204-21, NIST SP 800-171 Rev 2, and NIST SP 800-172, 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 assessments of the Accreditation Body and C3PAOs; conducting CMMC Level 3 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 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 and be compliant with ISO/IEC 17011:2017[13]. 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. Prior to the Accreditation Body being compliant with ISO/IEC 17011:2017 and completing a peer assessment of conformity with the IAAC in accordance with the ISO Committee on Conformity Assessment[14], the Accreditation Body may authorize but not accredit C3PAOs. After the Accreditation Body has achieved compliance with ISO/IEC 17011:2017 and completed a peer assessment of conformity with the IAAC in accordance with the ISO Committee on Conformity Assessment, the Accreditation Body may accredit C3PAOs.

The Accreditation Body also oversees the CAICO to ensure compliance with ISO/IEC 17024:2012[15] 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 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

[13] https://www.iso.org/standard/67198.html
[14] https://www.iso.org/committee/54998.html
[15] https://www.iso.org/standard/52993.html

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[16], a CMMC instance of the Enterprise Mission Assurance Support Service. C3PAOs grant a certificate of assessment when all security requirements are met, 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 CMMC 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, 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, the C3PAO may be authorized but not accredited. After a C3PAO is compliant with ISO/IEC 17020:2012, 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, authorizes, and certifies CMMC assessors, instructors, and related professionals. There is only one CAICO for the DoD CMMC Program at any given time. The CAICO must comply with ISO/IEC 17024:2012, as well as with the Accreditation Body's policies for CoI, CoPC, and Ethics. Section 170.10 addresses detailed requirements for the

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

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 (7). 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 Certified Instructor (CCI)

Section 170.12 addresses the roles and responsibilities of a CMMC Certified Instructor (CCI) to teach CMMC assessor candidates. The CAICO trains and tests candidate CCIs per the requirements set forth in § 170.12(b). Candidate CCIs are provided with a list of requirements to obtain and maintain certification, 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. 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 requirements listed in the FAR clause 52.204-21(b)(1). Secondly, § 170.14(3) defines CMMC Level 2 as the 110 requirements from the NIST SP 800-171 Rev 2. Lastly, § 170.14(4) defines CMMC Level 3 as 24 selected requirements from the NIST SP 800-172.

The CMMC security requirements are organized into domains following the approach taken in NIST SP 800-171 Rev 2. 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 and NIST SP 800-172A.

Section 170.15 CMMC Level 1 Self-Assessment and Affirmation Requirements

Section 170.15 addresses how an OSA will achieve and maintain compliance with CMMC Level 1 Self-Assessment. 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 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 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 CMMC Level 1 Self-Assessment requirement, the OSA must have a Level 1 Self-Assessment 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 CMMC Level 2 Self-Assessment. 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 for the corresponding CMMC Level 2 security requirements.

After implementation, the OSA must perform a 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 a Conditional Self-Assessment; if the minimum score has been achieved and no security requirements are in a POA&M, the OSA has a Final Self-Assessment. For Conditional Self-Assessments, a POA&M close-out must be conducted within 180 days as described in § 170.21(b).

After both Conditional Self-Assessment and Final Self-Assessment, 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 CMMC Level 2 Self-Assessment requirement, the OSA must have a Level 2 Conditional Self-Assessment or Level 2 Final Self-Assessment and have submitted an affirmation. The Level 2 Self-Assessment must be completed tri-annually and the affirmation must be completed annually.

Section 170.17 CMMC Level 2 Certification Assessment and Affirmation Requirements

Section 170.17 addresses how an OSC will achieve and maintain compliance with CMMC Level 2 Certification Assessment. 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 for the corresponding CMMC Level 2 security requirements.

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 a Conditional Certification Assessment; if the minimum score has been achieved and no security requirements are in a POA&M, the OSC has a Final Certification Assessment. For Conditional Certification Assessments, a POA&M close-out must be conducted within 180 days as described in § 170.21(b).

After both Conditional Certification Assessment and Final Certification Assessment, the C3PAO will input the OSC's results into the CMMC instantiation of eMASS as described in § 170.17(a)(1)(i). After both Conditional Certification Assessment and Final Certification Assessment, the OSC must submit an affirmation as described in § 170.22.

In order to be eligible for a contract with a CMMC Level 2 Certification Assessment requirement, the OSC must have a CMMC Level 2 Conditional Certification Assessment or CMMC Level 2 Final Certification Assessment and have submitted an affirmation. The CMMC

Level 2 Certification Assessment must be completed tri-annually and the affirmation must be completed annually.

Section 170.18 CMMC Level 3 Certification Assessment and Affirmation Requirements

Section 170.18 addresses how an OSC will achieve and maintain compliance with CMMC Level 3 Certification Assessment. The OSC must have a CMMC Level 2 Final Certification Assessment based on its Level 3 CMMC Assessment Scope. 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 for the corresponding CMMC Level 3 security requirements.

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 a Conditional Certification Assessment; if the minimum score has been achieved and no security requirements are in a POA&M, the OSC has a Final Certification Assessment. For Conditional Certification Assessments, a POA&M close-out must be conducted within 180 days as described in § 170.21(b).

After both Conditional Certification Assessment and Final Certification Assessment, DCMA DIBCAC will input the OSC's results into the CMMC instantiation of eMASS as described in § 170.18(a)(1)(i). After both Conditional Certification Assessment and Final Certification Assessment, the OSC must submit an affirmation as described in § 170.22.

In order to be eligible for a contract with a CMMC Level 3 Certification Assessment requirement, the OSC must have a CMMC Level 3 Conditional Certification Assessment or

CMMC Level 3 Final Certification Assessment and have submitted an affirmation. The CMMC Level 3 Certification Assessment must be completed tri-annually and the affirmation must be completed annually.

Section 170.19 CMMC Scoping

Section 170.19 addresses the requirements for the scoping of each CMMC Level assessment. Scoping 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 CMMC Level 2 Self-Assessment procedures in § 170.16(c) or the CMMC 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 1 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 1 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, other than a Cloud Service Provider (CSP), the ESP must have a CMMC certification level equal to or greater than the certification level the OSA is seeking. For example, if an OSA is seeking a CMMC Level 2 Certification Assessment the ESP must have either a CMMC Level 2 Certification Assessment or a CMMC Level 3 Certification Assessment.

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, are eligible for a CMMC Level 2 Certification Assessment.

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 initial assessment. To satisfy CMMC Level 1 requirements, a POA&M is not allowed. To satisfy CMMC Level 2 requirements, both self-assessment and certification assessment, 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 appropriate CMMC Self-Assessment or Certification Assessment: upon completion of any conditional or final assessment, annually following final assessment, and following a POA&M closeout assessment (as applicable).

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 requirements and is the starting value for assessment scoring. Any requirement that has one or more NOT MET objectives reduces the current score by the value of the specific 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 requirements and is the starting value for assessment scoring. Any requirement that has one or more NOT MET objectives reduces the current score by the value of the specific 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

As part of standing up version 1 of the CMMC Program, the Department of Defense published a DFARS interim final rule, "Assessing Contractor Implementation of Cybersecurity Requirements" in the Federal Register on September 29, 2020 (85 FR 61505). The Department received approximately 750 comments on the DFARS interim final rule pertaining to elements of the CMMC Program that are now being addressed in this rule. Those comments are summarized and addressed in the discussion and analysis.

In addition to comments on elements of the CMMC Program, DoD also received comments on the associated DFARS text, solicitation provisions, and contract clauses relating to the CMMC Program. The CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses relating to DoD's cybersecurity protection requirements, including DFARS clause 252.204-7021, CMMC Requirements. DoD will address comments regarding the DFARS clause 252.204-7021 in a separate 48 CFR rulemaking.

1. Service Providers

Comment: Multiple commenters asked about applicability of the CMMC Program to a variety of service providers. One commenter requested clarification regarding how CUI controls apply to Internet Service Providers and their globally sourced service support

because of the prohibition of foreign dissemination for CUI. Two commenters suggested that common carrier telecommunications (often termed as Plain-Old-Telephone-Services (POTS)) and similar commercial services (cloud services, external service providers) should be treated as commercial off-the-shelf (COTS), and so excluded from CMMC certification requirements. One commenter expressed concerns about the impact of the rule on the telecom industry. One commenter recommended that, to limit the burden of CMMC implementation, contractors providing commercial services to support COTS items, such as technical support for software, should receive the same exceptions as other COTS contracts.

Response: The CMMC Program will result in cybersecurity protection and assessment requirements for defense contractors and subcontractors. CMMC Level requirements will apply only if a defense contractor or subcontractor handles FCI or CUI on its own contractor information systems. If so, then under CMMC, the contractor or subcontractor will be required to comply with the cybersecurity protection and assessment requirements associated with the appropriate Level. As such, CMMC Level requirements will not apply to Internet Service Providers or other telecommunications service providers (i.e., common carriers), unless those entities themselves are or intend to become defense contractors or subcontractors. In addition, there is no general prohibition of foreign dissemination for CUI, although certain CUI may be subject to export restrictions. Commercial item determinations per 48 CFR 15, to include those relating to common carrier telecommunications or cloud services, are not defined by CMMC. With respect to the CMMC Assessment Scope, although they provide connectivity for contractor systems, and the common carrier link is within the boundary of the contractor's system, the common carrier's information system is not within the contractor's CMMC Assessment Scope as long as CUI is encrypted during transport across the common carrier's information system.

2. Joint Ventures

Comment: Multiple commenters asked for clarification on how to handle joint ventures with respect to DFARS clause 252.204-7021.

***Response*:** The CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses, including DFARS clause 252.204-7021. As such, DoD cannot address applicability of current DFARS clause 252.204-7021 at this time. With respect to joint ventures, CMMC Program requirements will apply to information systems associated with the contract efforts that process, store, or transmit FCI or CUI, and to any information system that provides security protections for such systems, or information systems not logically or physically isolated from all such systems.

3. Internet of Things /Operational Technology

Comment: Multiple commenters noted the applicability of the CMMC requirements to Internet of Things (IoT) and Operational Technology (OT) systems was unclear. Several commenters expressed concerns about the impact of the rule on factories and OT.

***Response**:* CMMC security requirements apply to information systems associated with the contract efforts that process, store, or transmit FCI or CUI, and to any information system that provides security protections for such systems~~;~~ or are not logically or physically isolated from all such systems. In accordance with § 170.19, an OSA's IoT or OT systems located within its Level 1 or Level 2 CMMC Assessment Scope are not assessed; however, for CMMC Level 2 they are required to be documented in the System Security Plan (SSP). When a CMMC Level 2 Certification Assessment is performed as a precursor to a CMMC Level 3 Certification Assessment, the IOT and OT (and all other Specialized Assets) should be assessed against all CMMC Level 2 security requirements as described in § 170.18(a)(1). For CMMC Level 3, an OSC's IoT or OT located within its CMMC Assessment Scope are assessed against all CMMC security requirements unless they are physically or logically isolated. However, for IoT and OT

(and all other Specialized Assets), it is permissible to use intermediary devices to provide the capability for the specialized asset to meet CMMC Level 3 security requirements.

4. Government Furnished Equipment:

Comment: One commenter questioned how the interim rule applies to Government Furnished Equipment (GFE) in a 'test' versus a 'production environment.'

Response: As described in § 170.3, CMMC security requirements will apply to any information system associated with the contract efforts that process, store, or transmit FCI or CUI, and to any information system that provides security protections for such systems~~;~~ or information systems not logically or physically isolated from all such systems. This includes when a 'Test Environment' processes, stores, or transmits FCI or CUI; provides security protections for such systems; or is not logically or physically isolated from such systems. See § 170.19 and the response to public comment under the heading 3. Internet of Things /Operational Technology in the Discussion of Comments and Changes section of this preamble for additional details on defining the scope of CMMC assessments.

If GFE cannot be configured to meet all the NIST SP 800-171 Rev 2 requirements or must be maintained in a specified configuration which does not comply with NIST SP 800-171 Rev 2, additional protections such as physical or logical isolation may be used for risk mitigation in accordance with the treatment of Specialized Assets as defined in table 1 to § 170.19(c)(1) CMMC Level 2 Scoping.

5. Fundamental Research:

Comment: Multiple commenters requested that DoD clarify the application of CMMC requirements to fundamental research. Commenters described adverse consequences of not explicitly exempting fundamental research from the CMMC requirements, noting that institutions of higher education will have to pull out of research agreements with the Department, may no longer accept DoD funds because the resource burden would be cost prohibitive to both the institution and its partners, and the burdens imposed by even CMMC Level 1 requirements

would hinder the progress of fundamental research. These commenters also noted that restrictions on posting of public information would inhibit open collaboration and the exchange of ideas that is critical to the advancement of scientific discovery. Commenters also requested that the Department clarify that subcontracts scoped as fundamental research also be exempt from CMMC requirements.

Response: CMMC Program requirements are designed to provide increased assurance to the Department that defense contractors can adequately protect FCI and CUI, in accordance with already applicable regulations and standards. Fundamental research is defined by National Security Defense Directive (NSDD)-189[17] as 'basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.' CMMC Program requirements apply only to defense contractors and subcontractors who handle FCI and CUI on an information system associated with a contract effort or any information system that provides security protections for such systems, or information systems not logically or physically isolated from all such systems. Fundamental research that is 'shared broadly within the scientific community' is not, by definition, FCI or CUI; however, other research-related information that is provided to or handled by contractors as part of contract performance may be FCI or CUI, thus may trigger application of CMMC Level requirements. If DoD determines the information handled by contractors pursuant to the fundamental research contract activities is or will become FCI or CUI, the information would be required to be processed, stored, or transmitted on an information system compliant with the appropriate CMMC Level.

6. International - Foreign DIB Partners / Non-U.S. Contractors

[17] https://irp.fas.org/offdocs/nsdd/nsdd-189.htm

Comment: Multiple commenters asked if international subcontractors of a U.S. prime will require CMMC certification. Commenters also asked if there is a strategy for legally implementing CMMC requirements beyond the U.S. DIB, and if an enterprise-level resolution has been developed to address foreign DIB sovereignty. One commenter suggested that some foreign governments have issued guidance to their local companies directing them not to accept CMMC flow down requirements.

One commenter expressed concern regarding the impact of CMMC to existing bilateral/multilateral security agreements. Another commenter asked if the foreign DIB will be authorized to evaluate U.S. DIB and vice versa. One non-U.S. commenter suggested using the existing Facility Security Clearance process to ensure a company is compliant with CMMC in accordance with national legislation.

Response: Contractors are required to comply with all terms and conditions of the contract, to include terms and conditions relating to cybersecurity protections and assessments. In addition, offerors will be required to comply with the pre-award CMMC requirement. This holds true when a contract clause is flowed down to subcontractors. The Facility Security Clearance process does not apply to unclassified information systems owned by, or operated on behalf of, a non-federal entity (e.g., contractors), and, therefore, does not apply to systems/networks that will be subject to CMMC requirements. This rule makes no distinction about which C3PAOs may assess which companies seeking certification. For more details on C3PAO requirements, see § 170.9.

7. CUI and FCI

a. Marking and identifying CUI

Comment: Multiple commenters asked for clarification regarding definition, marking, and identification of CUI as related to CMMC requirements and DFARS clause 252.204-7021. One commenter asked if the definition of DoD CUI applies to the CUI required to be safeguarded

under the CMMC clause. Another asked if DFARS clause 252.204-7021 includes information that requires protection under DFARS clause 252.204-7012.

One commenter requested that the Department confirm that, under CMMC, contractors will only be responsible for protecting CUI that is clearly marked upon receipt from the Department and created by contractors.

Response: If the contract includes a CMMC Level requirement, contractors will be required to protect FCI and CUI, as applicable, through fulfillment of the designated CMMC Level security requirements. CMMC does not in any way change the DoD requirements regarding the definition, marking, and protection of CUI.

If DFARS clause 252.204-7012 applies, contractors are required to safeguard covered defense information in accordance with the terms and conditions of the clause and contract, which includes information developed in support of the contract. CMMC does not change these requirements.

b. Relationship of FCI and CUI to the CMMC requirements

Comment: One commenter suggested that the inclusion of FCI in CMMC needs significant clarification. Others asked if FCI references within the CMMC Model [1.0] and nonpublic DoD information references in Department of Defense Instruction (DoDI) 8582.01[18] are the same type of information, and if DoDI 8582.01 is the definitive DoD policy for FCI and DoD standards regarding the requirements under FAR clause 52.204-21.

Response: The CMMC Program requirements for Level 1 will apply when the contract effort requires contractors to process, store, or transmit FCI on its unclassified information system. If CUI is processed, stored, or transmitted on a contractor information system, a higher level of CMMC compliance or certification is required. The CMMC Level required to protect CUI (i.e., CMMC Level 2 Self-Assessment as described in § 170.16, CMMC Level 2 Certification Assessment as described in § 170.17, or CMMC Level 3 Certification Assessment as described

[18] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DoDi/858201p.pdf?ver=2019-12-09-143118-860

in § 170.18) is determined by the Department based upon the sensitivity of the CUI and will be identified in the solicitation.

The CMMC Program uses the definitions of FCI from FAR 4.1901 and CUI from 32 CFR 2002, which are the definitive sources for these definitions. DoDI 8582.01, published on December 9, 2019, points to FAR clause 52.204-21 and DFARS clause 252.204-7012, both of which preceded it, to address the safeguarding requirements for FCI and CUI. CMMC builds from those requirements by requiring that defense contractors and subcontractors provide assurance, either with Self-Assessments, Third-Party Assessments, or Level 3 Assessments, as required, that they have implemented the required information protection requirements.

8. Small Business/Entities

a. Assistance/Support for Small Business

Comment: Several commenters suggested that in order to successfully implement cybersecurity requirements, contractors require support from the Department. One commenter suggested DoD should perform an analysis of each requirement and ensure that necessary support structures are in place and fully functioning prior to implementing this rule, and that access to tech support/solutions should be provided. Multiple commenters suggested that more support and guidance is needed for small businesses trying to comply with CMMC. One commenter suggested that DoD should relax affiliation rules (in conjunction with the Small Business Association (SBA)) to allow small companies to work together to meet CMMC requirements while spreading the cost over a larger base and expand mentor-protégé agreements for larger businesses to help smaller companies with CMMC appraisals.

One commenter expressed concern for non-traditional, innovative companies that are coming in through the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) process and asked what DoD is doing to help them become compliant. Another noted that if CMMC Level 1 will be the minimum requirement for SBIRs and STTRs, regardless

of whether they include FCI, it may significantly limit the number of universities that can partner with small businesses under these awards.

Response: DoD's Office of Small Business and Technology Partnerships (OSBTP) is working to provide SBIR/STTR programs with support for CMMC implementation through the use of Technical and Business Assistance. The SBA's affiliation rules are codified at 13 CFR 121.103, available at https://www.ecfr.gov/current/title-13/chapter-I/part-121. Any change to the SBA's affiliation rules is outside the scope of this rulemaking.

The CMMC Program is designed to increase assurance that defense contractors do in fact, comply with information protection requirements to adequately protect FCI and CUI. Additional information to assist contractors regarding DoD's current information security protection requirements may be found in Frequently Asked Questions (FAQs) Regarding the Implementation of DFARS subpart 204.73, published at https://DoDprocurementtoolbox.com/.

b. Impact of Cost

Comment: Multiple commenters commented on the cost impact of CMMC to small businesses, suggesting that the cost to become and remain compliant is too high. Several commenters added that small businesses limited by finances won't be able to compete, which could be detrimental to the supply chain and efforts to meet national defense goals, and that the rule fails to provide any consideration for the future loss of technology acquisition should small businesses be inadvertently precluded from participation. Other commenters suggested that the impact of CMMC will be a profound and significant obstacle to businesses due to their lack of resources as compared to their large business competitors, adding that the requirement to have the same measures in place for any company, regardless of size, incurs a higher percentage of indirect cost for small businesses. Multiple commenters remarked on the limited or lack of options for a small business to recover costs.

Response: The estimated costs attributed to this rule do not include the costs associated with compliance with existing cybersecurity requirements under FAR clause 52.204-21 or associated

with implementing NIST SP 800–171 requirements in accordance with DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. To the extent that defense contractors or subcontractors have already been awarded DoD contracts or subcontracts that include these clauses, and process, store, or transmit FCI or CUI in support of the performance of those contracts, costs for implementing those cybersecurity requirements should have already been incurred and are not attributed to this rule. Those costs are distinct from costs associated with undergoing a CMMC assessment to verify implementation of those security requirements. The CMMC Program does not levy additional information security protection requirements for CMMC Levels 1 and 2. The value of DoD's sensitive information (and impact of its loss to the Department) does not diminish when it moves to contractors - prime or sub, large or small.

A Regulatory Flexibility Analysis was conducted. In comparison to CMMC 1.0, DoD has now eliminated the requirement for organizations to hire a third-party assessment organization to comply with CMMC Level 1. The CMMC Program requirements further address cost concerns by permitting self-assessment at Level 1 and at Level 2 for some contracts that are not designated to require the added assurance of C3PAO assessment.

In addition, resources available through the DoD Office of Small Business Programs (OSBP) may help defray cybersecurity costs by helping companies stay up to date with the latest cybersecurity policies and best practices. The OSBP also partners with the NIST and its Manufacturing Extension Partnership (MEP) programs (https://www.nist.gov/mep), which operate across the U.S. to provide resource and funding assistance options.

The Department currently has no plans for separate reimbursement of costs to acquire cybersecurity capabilities or a required cybersecurity certification that may be incurred by an offeror on a DoD contract. Costs may be recouped via competitively set prices, as companies see fit.

c. Alternative Implementation

Comment: Multiple commenters requested that the government give small businesses time for CMMC compliance post-contract award. One commenter recommended that DoD consider only requiring government assessment of NIST SP 800-171 compliance (vice private third party) for small businesses, even at lower CMMC assessment levels, thus offsetting a higher burden level to small businesses. Several commenters commented on the need to include exemptions for small businesses that do not possess CUI and have never been contracted by the government. One added that DoD should identify portions of contracts which won't require CMMC so that small businesses are afforded maximum practicable opportunity regardless of their CMMC status.

Response: The DoD has determined that the assessment of the ability of a prospective contactor to adequately protect FCI and CUI that will be processed, stored, or transmitted on information systems during contract performance is a requirement prior to award of any prime contract or subcontract. Failure to assess a prospective contractor's ability to comply with applicable information security protection requirements, such as NIST SP 800-171 Rev 2, risks significant performance delays if information cannot be shared immediately at contract award due to lack of compliance. As applicable, the awardee must be capable of processing, storing, and transmitting FCI and CUI at the start of the performance period, regardless of the business size of the awardee. The CMMC Program has simplified requirements for Level 1 and 2 assessments in some contracts. Specifically, although contractors must still implement and maintain the security requirements set forth in FAR 52.204-21 to protect FCI and set forth in the NIST SP 800-171 Rev 2 to protect CUI, the requirement to hire a third-party assessment organization for CMMC Level 1 was eliminated, and for some contracts, contractors may be permitted to self-assess compliance with CMMC Level 2. Annual affirmations are also required for CMMC Level 1 and 2.

Prospective contractors must make a business decision regarding the type of DoD business they wish to pursue and understand the implications for doing so. If an offeror or current DoD

contractor or subcontractor has self-assessed then later decides to pursue a contract or subcontract requiring a certification at CMMC Level 2 or 3, it will need to factor in the time and investment necessary to hire a third-party assessment organization and achieve certification as a condition of contract award.

Public comments received illustrate that some small businesses may be unaware of how to propose cybersecurity-related costs for cost-type contracts. This rule does not change existing contract cost principles or procedures. For firm-fixed priced efforts, market supply and demand dictates profitability and bid prices, and underlying costs are not itemized.

9. Disputes regarding CMMC Assessments

***Comment**:* Multiple commenters asked about the CMMC assessment dispute resolution process, with regard to which standards would be followed, how much time would be available to appeal findings, the types of complaints that could be raised, any limits to the costs or schedule required for dispute resolution, and roles and responsibilities of the DoD, C3PAOs, and the Accreditation Body. Commenters also wanted to know whether a tiered recourse process would be available to resolve contractor objections to the initial resolution. Two commenters expressed concerns regarding potential impacts of C3PAO assessment errors. Two commenters requested clarification regarding whether the CMMC Level required by the DoD or a prime contractor could be contested.

***Response**:* The CMMC assessment appeal process (formerly referred to as dispute resolution) described in the DFARS Case 2019–D041 Supplementary Information has changed and is described in § 170.9(b)(20) and § 170.8(b)(16). The appeals process is derived from and consistent with ISO/IEC 17020:2012 and ISO/IEC 17011:2017. Each C3PAO is required to have a time-bound, internal appeals process to address disputes related to perceived assessor errors, malfeasance, and unethical conduct. Requests for appeals will be reviewed and approved by individual(s) within the C3PAO not involved in the original assessment activities in question.

OSCs can request a copy of the process from their C3PAO. If a dispute regarding assessment findings cannot be resolved by the C3PAO, it will be escalated to the Accreditation Body. The decision by the Accreditation Body will be final.

A request for an appeal about an assessor's professional conduct that is not resolved with the C3PAO will be escalated and resolved by the Accreditation Body.

The issue of C3PAO liability is between an OSC and the C3PAO with which it contracts to do the assessment.

Any questions about the CMMC Level required by the solicitation should be directed to the contracting officer for the affected contractor.

10. Acceptance of Alternate Standards

a. NIST SP 800-171 Rev 2 DoD Assessments and CMMC Assessments

Comment: Multiple commenters asked for clarification on reciprocity between NIST SP 800-171 Rev 2 DoD Assessments and CMMC assessments.

Response: As stated in § 170.20(a), DoD intends to allow qualified standards acceptance of High confidence assessment using NIST SP 800-171 Rev 2 for CMMC Level 2. However, the CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses relating to cybersecurity assessments.

b. Cloud Standards

Comment: Many commenters expressed concerns regarding CMMC recognition of Federal Risk and Authorization Management Program (FedRAMP) and requested guidance on which FedRAMP baselines, if any, would be granted standards acceptance at each CMMC Level. A few commenters sought assurance that DoD Cloud Computing Security Requirements Guide (SRG) Impact Levels 4 and 5 would not be applied to CMMC Level 3.

Response: CMMC does not offer comprehensive acceptance of FedRAMP. The CMMC Program allows the acceptance of FedRAMP environments in some cases to meet CMMC

requirements in connection with use of a Cloud Service Provider (CSP). If an OSC uses an external CSP to process, store, or transmit CUI or to provide security protection for any such component, the OSC must ensure the CSP's product or service offering either (1) is authorized as FedRAMP Moderate or High on the FedRAMP Marketplace; or (2) meets the security requirements equivalent to those established by the Department for the FedRAMP Moderate or High baseline. The CSP will provide evidence that its product or service offering meets the security requirements equivalent to FedRAMP Moderate or High by providing a body of evidence (BOE) that attests to and describes how the CSP's product or service offering meets the FedRAMP baseline security requirements. Note that for any portion of the on-premises (internal) network that interacts with the cloud service offering and is within the CMMC Assessment Scope, the OSC is required to meet all applicable CMMC requirements to achieve certification.

The DoD Cloud Computing SRG applies to DoD-provided cloud services and those provided by a contractor on behalf of the department, i.e., a commercial cloud service provider or integrator. Cloud Computing SRG does not apply to CMMC.

c. Other Standards

***Comment**:* Numerous commenters asked whether CMMC could leverage the results of other assessments, such as ISO/IEC 27001/27002, NIST SP 800-53, NIST SP 800-172, HITRUST, DoE Cybersecurity Capability Maturity Model, NIAP Common Criteria Testing Laboratory Services (CCEVS), Committee on National Security Systems (CNSS) Instruction No. 12533 (CNSSI 12533), ISA/IEC-62443, DoD's Security Technical Implementation Guides (STIG), NIST Cyber Security Framework (CSF), NIST Risk Management Framework (RMF), the American Institute of CPAs Service and Organizational Controls, Service and Organization Controls (SOC) Trust Services Criteria (SOC 2), ISA/IEC-62443, ITAR, Criminal Justice Information Services (CJIS) security standards, and non-ISO/IEC standards used by foreign partners such as the Australian Cybersecurity Centre Essential Eight Maturity Model.

Response: The CMMC Program standards acceptance is defined in § 170.20 of this rule.

11. CMMC Assessment Scope

Comment: Multiple commenters requested details on assessment boundaries and what systems are in-scope for a CMMC assessment. Questions included how assessment boundaries are defined, how networks composed of federal components (including systems operated on behalf of the government) and non-federal components are addressed, how centralized security services are treated, and how "enduring exceptions" are handled.

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. This section includes detailed guidance on how to define the CMMC Assessment Scope, how different categories of equipment are defined to be in- or out-of-scope for an assessment, how the security of specialized equipment is expected to be managed, External Service Providers considerations, and the incorporation of people, technology, and facilities into the boundary.

GFE, IoT, OT, and, as defined, Restricted Information Systems and Test Equipment are categorized as "Specialized Assets" in § 170.19. NIST SP 800-171 Rev 2 uses the term "enduring exceptions" to describe how to handle exceptions for Specialized Assets.

12. Applicability of Multiple CMMC Levels

Comment: Two commenters sought confirmation that it is acceptable for contractors with multiple business segments to have one or more CMMC assessments (e.g., one segment at Level 1, another at Level 2). Commenters also wanted to know if systems within the scope of an assessment require multiple assessments if the systems are used to support tasks under multiple contracts. Another asked, if a company has multiple Commercial and Government Entity (CAGE) codes, whether a single assessment can cover all CAGE codes.

Response: Yes, it is possible to have different business segments or different enclaves assessed or certified at different CMMC Levels. A CMMC assessment can be restricted to a particular segment or enclave based on the defined CMMC Assessment Scope, and an OSA can

define multiple CMMC Assessment Scopes. Thus, a business segment that only supports Level 1 (FCI) efforts can identify a boundary that is assessed against Level 1 requirements, and another segment that supports Level 2 (CUI) efforts can identify a different boundary that is assessed against Level 2. Offerors will be required to attain CMMC certification, when applicable, at or above the level required by the solicitation, by the time of award (or option period exercise) and must maintain their CMMC status throughout the life of the contract, task order, or delivery order.

13. CMMC Implementation Timeline and Pilot Program

a. CMMC Schedule

Comment: There were many comments requesting clarification or justification regarding the general roll-out schedule for DFARS clause 252.204-7021. Some commenters requested program acceleration and others advocated for delays. Two commenters were confused by statements in the Federal Register Notice that the timeline for implementation across the DoD contractor population would be seven years, but that all contracts would include the CMMC clause in five years, at the end of the roll-out.

Response: The DoD is implementing a phased implementation for the CMMC Program and intends to introduce CMMC requirements in solicitations over a three-year period to provide appropriate ramp-up time. The Department anticipates it will take two years for companies with existing contracts to become CMMC certified.

In response to public comment, assessment requirements in CMMC have been simplified to three tiers, and DoD is developing policy to guide Program Managers through a time-phased introduction of CMMC requirements. From the effective date of the DFARS rule that will implement CMMC requirements, DoD will include CMMC self-assessment requirements in solicitations when warranted by the FCI and CUI categories associated with the planned effort. A similar requirement for CUI has been in place since publication of the September 2020 rule that implemented DFARS provision 252.204-7019, which requires offerors to submit NIST SP

800-171 Rev 2 self-assessment results in the SPRS as a condition of award. DoD intends to include CMMC requirements for Levels 1, 2, and 3 in all solicitations issued on or after October 1, 2026, when warranted by any FCI or CUI information protection requirements for the contract effort. In the intervening period, DoD Program Managers will have discretion to include CMMC requirements in accordance with DoD policies.

b. CMMC Pilot Program

Comment*:* Multiple commenters wanted more information about the roll-out of the CMMC pilot program, including transparency about which acquisition programs are being considered for inclusion prior to the release of a solicitation. Commenters requested details on the "provisional period," whether there would be a break between the pilot program and the official launch of the CMMC Program, whether there would be an assessment on the effectiveness of the pilot, and if lessons learned from the pilot would be shared across the community.

Response*:* CMMC 1.0 did include a CMMC Pilot program; however, CMMC 2.0 does not include pilots. Instead, upon the effective date of the associated CMMC DFARS rule, the Department intends to begin including CMMC self-assessment requirements when applicable, for protection of FCI and CUI.

c. Communicating CMMC Requirements

Comment: Two commenters requested that, during the phased rollout of CMMC, defense contractors be forewarned of DoD plans to include a CMMC requirement in an upcoming solicitation. They asked for transparency with respect to which contracts were being considered for CMMC requirements.

Response*:* Offerors and contractors will be informed of CMMC requirements in solicitations through (1) the specification of a required CMMC Level, and (2) inclusion of the appropriate DFARS provisions or clauses. There is no plan to advertise a list of solicitations that will or may include CMMC requirements. The implementation plan described in § 170.3(e) addresses phase-in of CMMC requirements.

d. Market Capacity for Assessments

Comment: Multiple commenters wanted details about assessor availability and were concerned that a lack of assessors would impact the schedule for including CMMC requirements in solicitations and contractor planning to attain CMMC certification to meet those requirements.

Response*:* 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. An 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. If changes to the implementation plan occur, DoD policies that govern requirements definition in the acquisition process will be modified.

e. Certification Sustainment during Validity Period

***Comment*:** Three commenters asked about sustainment of CMMC certification during the three-year certificate validity period. They wanted to know how sustainment will be monitored and whether demonstrating continuous monitoring capabilities would be considered in lieu of a strict three-year recertification period. There were also questions about what the criteria or triggers would be that would lead to a loss of accreditation during this period, including what happens when a company with a certification is acquired by another company, and whether contractors are required to notify the DoD if systems fall out of compliance with CMMC requirements.

Response: The validity period is one (1) year for CMMC Level 1 and three (3) years for CMMC Levels 2 and 3. Contractors must continue to meet CMMC requirements during the period of performance of the contract. Under CMMC, contractors must submit affirmations into SPRS for each assessment, attesting that they have met the CMMC requirements and will maintain the applicable information systems at the required CMMC level as specified in § 170.22. Monitoring contractor compliance with the terms of the contract is the responsibility

of the contractor, with the government contracting officer. DoD is not utilizing a continuous monitoring capability in lieu of compliance requirements. DoD understands that information systems operating in a CMMC Assessment Scope will require upgrades and maintenance. For systems certified at CMMC Level 2 or above, a plan for addressing deficiencies is defined in § 170.21.

It is possible for an organization to need a new assessment during the validity period. CMMC self-assessments and certifications are valid for a defined CMMC Assessment Scope. If the CMMC Assessment Scope changes due to infrastructure modifications or expansion of the CMMC Assessment Scope due to new acquisition, a new assessment may be required. The original CMMC certification remains valid for the original CMMC Assessment Scope. The information system(s) in the new CMMC Assessment Scope may not be used to process, store, or transmit CUI for any contract until it is validated via a new CMMC assessment. The same applies to the annual affirmations. During the annual affirmation process, a senior organization official affirms that the organization is satisfying and will maintain the requirements of the specified CMMC level (e.g., CMMC Level 2 Self-Assessment). The affirmation applies to the CMMC Assessment Scope. At the time of a new self-assessment or certification, a new affirmation is submitted into SPRS affirming that the organization meets the CMMC requirements and will maintain the applicable information system (within the CMMC Assessment Scope) at the required CMMC level. For CMMC Levels 2 and 3, an affirmation is required to be submitted in SPRS annually for the duration of the triennial validity period and at the conclusion of any POA&M closeout assessments. Affirmation requirements are set forth in § 170.22.

14. CMMC Assessment Timeline

Comment: Several comments requested details about CMMC assessment timelines, including how long an assessment would take, how long after an assessment was completed would the assessment report be ready, and when SPRS content would be updated. One

commenter wanted to know how soon after a failed assessment a subsequent assessment could be scheduled. One commenter wanted details about the remediation period.

Response: The actual length of time it takes for an OSA to prepare for, and assessors to conduct an assessment and prepare the assessment report depends on many factors, including the number of systems and networks in the CMMC Assessment Scope, the level of assessment being conducted, staff preparedness for assessor questions, and the number of assessors conducting the assessment.

For CMMC assessments, C3PAOs will upload the results of the assessment and the signed CMMC certificate into the CMMC instantiation of eMASS. Certification is automatically posted to SPRS. There is no minimum time to wait after a failed assessment before scheduling another assessment.

A NOT MET requirement may be re-evaluated during the course of the assessment and for 10 business days following the active assessment period under certain conditions, as set forth in § 170.17(c)(2) and § 170.18(c)(2). A Level 2 or Level 3 conditional assessment and associated POA&M must be closed out within 180 days.

15. Assessment Delays and Award Impact

Comment: Several commenters expressed concerns about the impact that delays in the assessment process would have on contract award. For example, if an assessment is held up, by no fault of the contractor, such that the results will not be available until after the award date, will the contractor be ineligible to receive the award or is there a process for delaying the award? Would the answer be the same for a reassessment of a contractor whose three-year assessment or certificate is expiring? On a related issue, one comment asked about the timing of reassessment/recertification and whether work on an existing contract can continue after an assessment/certificate has expired if the reassessment is scheduled but delayed.

***Response**:* The CMMC Program rule does not provide mitigations for assessment delays that may impact timeliness of certification or recertification with regard to the closing date of a particular solicitation. Offerors will be required to attain CMMC certification, when applicable, at or above the level in the solicitation, by the time of award (or option period exercise) and must maintain their CMMC status throughout the life of the contract, task order, or delivery order. The three-year validity period should provide adequate time to prepare for and schedule subsequent assessments for certification. Timelines for meeting CMMC requirements for Level 1 or 2 self-assessment are within the control of the contractor.

16. Defense Contractor and Subcontractor Engagement

Comment: Several commenters suggested that defense contractors and subcontractors should be more engaged in the formulation of the rule and better informed in how the rule will be applied. They indicated that guidance is unclear, ad hoc, and inconsistent, and requested an authoritative source of information, such as FAQs, that are kept up to date and provide reliable responses to questions. They also expressed a desire for more transparency in how ambiguities are being resolved in early assessments.

Response: In September 2019, the CMMC PMO released the first draft publication of the CMMC Model v 0.4. The CMMC PMO received over 2,000 comments from individuals and industry associations. These comments informed changes included in CMMC Model 1.0 released in January 2020. In addition, DFARS Case 2019-D041 generated over 750 additional public comments that informed changes to the rule text and influenced the transition to CMMC 2.0. The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) held over 100 industry listening sessions in 2020 and 2021, engaged with the DIB through briefings and discussions with defense industry trade associations, academia, and government-based organizations with industry members (e.g., National Industrial Security Program Policy Advisory Committee). Many sessions were recorded and shared with the public on the Internet in social media, news releases, and the CMMC PMO website (https://DoDcio.defense.gov/CMMC/),

which was completely updated in 2021 and contains new information, FAQs, and allows the public direct contact with the CMMC PMO. As always, FAQs are to clarify content only, and do not interpret, define, or otherwise change the meaning of the regulatory text. The CMMC PMO continues to communicate with defense contractors and subcontractors, to include small businesses, and other members of the public.

The official website of the DoD CMMC Program is https://DoDcio.defense.gov/CMMC/. This website contains links to CMMC documents including, but not limited to, the CMMC Model Overview, CMMC Scoping Guidance (by level), CMMC Level 1 Self-Assessment Guide, CMMC Level 2 Assessment Guide, and the CMMC Glossary.

17. C3PAO Consistency

Comment: One commenter expressed concerns that C3PAOs would not conduct CMMC assessments in a uniform manner, leading to inconsistent results.

Response: C3PAOs use only certified CMMC assessors to perform CMMC assessments. To ensure assessments are conducted in a uniform manner, assessors are trained by certified instructors and required to pass CMMC assessor tests before becoming certified. The accredited CAICO manage and oversee the training, testing, authorizing, and certifying of candidate assessors and instructors. A CAICO must meet the DoD requirements set forth in § 170.10 and achieve compliance with ISO/IEC 17024:2012, Conformity Assessment – General Requirements for Bodies Operating Certification of Persons Conformity Assessment.

18. CMMC Cost Impacts

a. CMMC Cost Assumptions and Estimates

Comment: Several commenters questioned or refuted the cost estimates and/or the assumptions and mathematical approach upon which the cost estimates were based. Several commenters requested clarification around the cited difference in both cost and hours between the CMMC certification process and the DoD Assessment process, the accounting for completion of NIST SP 800-171 Rev 2 requirements, and cost distinction between enterprise and

enclave assessments. Two commenters stated that the estimated number of subcontractors was low, and one commenter suggested that the $5 million threshold for small businesses excluded a large number of small businesses from the calculations. One commenter asked whether duplication of assessments was considered for small businesses who support many prime contractors. Additional commenters believed costs were absent from the calculations, to include the cost of completing POA&M, management costs for small companies to achieve maturity, and costs for international suppliers. A number of comments requested additional estimates based on adjustments to labor rates for benefits and taxes, each of the assessment levels, and small, medium, and large companies. One commenter asked for clarification on the calculations used to estimate public savings. One commenter questioned why North American Industry Classification System (NAICS) code 54715 pertaining to sensitive CUI was not included in the calculations.

***Response**:* The cost estimates and assumptions referenced by the commenters pertain to CMMC 1.0 and are not reflective of the changes in CMMC, though public comment feedback has been incorporated into the cost estimation process for the CMMC Program where appropriate. The Department limited estimates for CMMC to those costs associated with preparing for, attaining, and publishing results of: (a) CMMC compliance via self-assessment for CMMC Levels 1 and 2, and (b) certification at CMMC Level 2 through a C3PAO and Level 3 through the DoD. Costs for companies to implement information security protections to comply with the existing FAR subpart 4.19 to achieve CMMC Level 1, and DFARS subpart 204.73 to achieve CMMC Level 2, are distinct from costs associated with CMMC assessment processes to verify and attest to the corresponding implementation of existing rules. Cost estimates were developed for companies to implement security requirements for CMMC Level 3. CMMC Level 3 security requirements are defined in table 1 to § 170.14(c)(4) CMMC Level 3 Requirements. For the vast majority of the DIB, CMMC does not levy additional information security protection requirements but is designed to provide increased assurance that defense contractors are contract compliant and can adequately protect FCI and CUI at a level commensurate with

risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. There is no recognized duplication of assessments for small companies that support many primes, because once assessed, an organization need only provide evidence of compliance or certification to prospective primes in order to satisfy the CMMC requirement in a solicitation. When information system or network boundaries differ, an additional assessment may apply.

b. CMMC Cost Burden

Comment: Several commenters suggested that costs were underestimated, particularly for small businesses who were perceived to be at risk of decreased participation in the marketplace due to the cost prohibitive nature of the CMMC requirement. Multiple commenters requested additional strategies to mitigate costs, including the promotion of new technologies.

Response*:* CMMC Levels 1 and 2, which represent the majority of the anticipated requirements, does not levy any additional information security protection requirements. To address assessment cost concerns, CMMC eliminates the third-party assessment requirement at CMMC Level 1 and permits self-assessment for certain contracts containing a CMMC Level 2 requirement. The DoD Office of Small Business Programs, available at https://business.defense.gov/, has informational resources that may help defray cybersecurity implementation costs by helping organizations stay up-to-date with the latest cybersecurity compliance and policy best practices.

c. CMMC Cost Effectiveness and Alternatives

Comment: Two commenters requested that the DoD measure the impact of implementing the additional security requirements. One commenter suggested an alternative strategy to protect CUI when generated.

Response*:* 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 Rev 2 for CMMC Levels 1 and Level 2, respectively. CMMC Level 3 requirements are new and based upon NIST SP 800-172.

19. CMMC Model

a. CMMC Level Requirement Selection

Comment: Multiple commenters requested clarification about who selects the CMMC Level that is specified in a solicitation and the criteria used. Commenters also wanted to know if the contractor's CMMC Level flows-down directly to subcontracts and if so, whether that level carries down to lower tier subcontracts. Numerous questions asked if the government or a contractor is responsible for determining the appropriate CMMC Level to include in a subcontract and, if it is the contractor's responsibility, what criteria is used to identify the appropriate level to flow-down. To that end, commenters requested guidance for identifying CUI and information sensitivity. One commenter asked for clarification on whether different CMMC Level requirements could be identified within a single Statement of Work (SOW).

Response: The solicitation will specify the required CMMC Level, and the level itself will be identified by the requiring activity. 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. Contractors must have achieved this level, or higher, to be awarded the resultant contract. For subcontracts, the prime contractor will identify for its subcontractor the required CMMC Level in accordance with § 170.23 if it is not already defined in the solicitation. If a prime contractor is uncertain about the appropriate CMMC Level to assign when creating a subcontract solicitation, it should consult with the government program office to determine what type of certification or assessment will be required given the information that will flow down. Policies for identification and clear marking of CUI materials are provided in CUI program materials and 32 CFR part 2002, when applicable. A solicitation may contain requirements for multiple CMMC Levels if, in support of the contract, different enclaves are expected to process, store, or transmit information that needs different levels of security.

b. Model Standard, CMMC Levels, and Model Updates

Comment: One commenter stated that the CMMC Model is not a configuration-controlled standard managed by a recognized standards body.

Response: This rule codifies the CMMC Program, elements of which are reflected in the CMMC Model. All CMMC Model requirements are derived from FAR 52.204-21, NIST SP 800-171 Rev 2, and NIST SP 800-172, which are configuration-controlled guidelines managed by NIST. As a result of the alignment of CMMC to NIST guidelines, the Department's requirements will continue to evolve as changes are made to the underlying NIST SP 800-171 Rev 2 and NIST SP 800-172 security requirements. Additional rulemaking may be necessary in the future to conform CMMC requirements described in this rule to any changes to the underlying information protection requirements defined in the foundational NIST guidelines.

Comment: Many comments were received requesting changes to CMMC Model 1.0. Several commenters requested changes to CMMC Level requirements and others had questions about the content and handling of CMMC Model updates. A few commenters made suggestions for restricting the current implementation, such as using only NIST SP 800-171 Rev 2 for the CMMC 1.0 implementation of Level 1-3 requirements and supplementing with additional requirements only in Levels 4 and 5. Similar comments recommended using NIST SP 800-171 Rev 2 for the initial CMMC rollout and later expanding to include additional CMMC requirements. A number of comments questioned the purpose and use of the CMMC 1.0 implementation of CMMC Level 2. Other comments requested information on updating CMMC requirements as new technology and threats emerge and new versions of NIST SP 800-171 Rev 2 and NIST SP 800-53 are released. Multiple comments were received on CMMC 1.0 Levels 4 and 5. Several commenters believed there to be a significant disconnect between NIST SP 800-171B/172 and CMMC 1.0 Levels 4 and 5, and issues with implementation of these levels. Many comments requested that Levels 4 and 5 be updated to allow for flexibility in implementation rather than require all the requirements as written. Reasons cited for allowing

flexibility include reducing cost and assessment complexity as well as allowing for the ability to adapt based on architectural environments and dynamic threat models.

Response: Changes were made in this rule to requirements in the former CMMC model based in part upon receipt of informal public comment. The CMMC Model was streamlined to three-tiers, which align to the protection requirements set forth in FAR 52.204-21, NIST SP 800-171 Rev 2, and NIST SP 800-172, and all CMMC-unique requirements and process maturity elements have been removed.

The CMMC Model and program requirements will be evaluated as new technology and threats emerge and revised as appropriate.

Comment: One comment included a request to identify instances where contractors would be better off using a classified environment, rather than CMMC version 1.0 Level 4 or 5, to protect the information.

Response*:* The CMMC Program is designed to enforce protection of unclassified information, to include FCI and CUI, not intended for public release that is shared by the Department with its contractors and subcontractors. The program provides the Department increased assurance that contractors and subcontractors are meeting the cybersecurity requirements that apply to acquisition programs and systems that process federal contract information and controlled unclassified information. Any discussion regarding the use of classified networks is outside of the scope of the CMMC Program.

20. CMMC Requirements

Comment: There were multiple comments suggesting additions, deletions, or changes to model requirements. One commenter noted multiple instances of CMMC requirements with the term 'information system' rather than 'system' used in NIST SP 800-171 Rev 2, asking if CMMC meant to change the intent by inserting 'information' in these requirements. Multiple commenters questioned the intent, clarity, or interpretation of several CMMC requirements/NIST SP 800-171 Rev 2 requirements, recommending clarification regarding vulnerability

management, protection of mobile devices, review of audit logs, disabling of identifiers, FIPS validated encryption, and malicious code scans. One comment suggested that CMMC 1.0 requirements RM.2.141 and RM.3.144 are redundant and recommended incorporating RM 3.146 into CA.2.159, justifying that a plan of action is essentially a risk management plan. Two commenters noted that two CMMC 1.0 requirements (RE.2.137 and RE.3.139) are unclear as they do not specify what data requires backup, or the meaning of resilient backup. One commenter said that CMMC 1.0 requirement MA.2.114 removed the qualifier of "maintenance" when describing personnel requiring supervision of maintenance activities, asking if this is an insignificant change to the NIST SP 800-171 Rev 2 security requirement, or whether there is some rationale or message that the CMMC specification is trying to adjust by deviating from the NIST SP 800-171 Rev 2. Two commenters stated that CMMC 1.0 requirement MP.1.1.18 requires only FCI be sanitized, but, for CMMC 1.0 Level 3 (CMMC Level 2 under CMMC 2.0) assessments, there is no requirement to sanitize CUI. One commenter wanted to know which CMMC requirement requires a medium assurance certificate for reporting cyber incidents.

Response: In CMMC 1.0, there was no intent to change the meaning of NIST requirements except those referenced as "modified." These minor discrepancies are now resolved as all FCI requirements use the exact FAR language and all CUI requirements use the exact language from the relevant NIST guidelines. The requirements in CMMC Level 3 are derived from NIST SP 800-172 with DoD-approved parameters. Commenters requesting revisions to NIST guidelines should respond to the NIST public comment periods. There is no CMMC-specific cyber incident reporting requirement or need for associated medium assurance certificate.

***Comment*:** Several comments sought clarification on the alignment and relative authority or precedence of the CMMC requirements to Federal, Legislative, Statutory, Regulatory, or DoD Organizational policy, DoD instructions, and FAQs.

Response: The CMMC Program requirements will be required once implemented in the DFARS and will have the same relative authority of any other DoD contract requirement. The

CMMC Program relates to and incorporates elements of the following authorities: Executive Order No. 13556, Controlled Unclassified Information, 75 FR 68675 (November 4, 2010), which establishes "an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls;" 32 CFR part 2002, which describes the executive branch's Controlled Unclassified Information Program and establishes policy for designating, handling, safeguarding, and decontrolling information that qualifies as CUI when processed, stored, or transmitted on a federal or non-federal information system; FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, which, as applicable, requires contractors to apply certain basic safeguarding procedures on covered contractor information systems that process, store, or transmit FCI; and DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, which, as applicable, requires defense contractors to implement NIST SP 800-171 Rev 2 requirements on unclassified covered contractor information systems that process, store, or transmit covered defense information. Additional DoD instructions and manuals address DoD information security policy, including DoDI 5200.48 CUI which establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD for federal and on non-federal information systems to include the implementation of NIST SP 800-171 Rev 2. A requirement for CMMC assessments provides DoD assurance that contractors have implemented required cybersecurity protections. The requirements of this rule will be implemented in an associated 48 CFR acquisition rule regarding CMMC.

21. CMMC Assessment

Comment: Multiple commenters pointed out that the rule does not specify an authoritative source for obtaining a CMMC certificate, leaving the pedigree of certificates in question. Two comments inquired about the security of record [data] collection and retention and whether the assessors' platforms would need to be CMMC Level 3 compliant to protect sensitive data used for the assessment/certification process.

Response: The processes for achieving compliance with a CMMC level are described in § 170.15 through § 170.18. CMMC Level 2 Certification Assessments are conducted by C3PAOs authorized by the CMMC Accreditation Body. C3PAOs grant CMMC Level 2 certificates of assessment. The DoD conducts CMMC Level 3 Certification Assessments and grants Level 3 certificates of assessment. A C3PAO's IT infrastructure must achieve at least a CMMC Level 2 Certification Assessment. Certified CMMC Assessors working at their place of business or from home must use their C3PAO's IT infrastructure. Assessment data and results are securely uploaded by the C3PAO into the CMMC instantiation of eMASS. The CMMC instantiation of eMASS automatically feeds compliance data into SPRS. Both eMASS and SPRS are Department owned and operated systems.

Comment: A few commenters requested resources for understanding CMMC requirements. There were also many comments related to the purpose, status, schedule, or content of the CMMC Assessment Guides. Additional comments requested clarification on the evaluation criteria and evidence described in the current Assessment Guides.

***Response*:** CMMC Assessment Guides are optional resources to aid in understanding CMMC requirements and are largely derived from NIST documentation, to include NIST SP 800-171 Rev 2 and NIST SP 800-172. The CMMC assessment process is defined in § 170.15 through § 170.18, and the CMMC Scoring Methodology is defined in § 170.24. The evaluation criteria (i.e., assessment procedures) and evidence (i.e., potential assessment methods and objects) required are taken directly from the NIST documentation, and revisions to NIST documentation are outside the scope of this rule. The CMMC Assessment Guides provide supplementary information, further discussion, examples, and references for assessors and contractors preparing for assessments. The guides do not identify specific solutions or baselines. These documents are available at: https://DoDcio.defense.gov/CMMC/. Updated CMMC Assessment Guides and associated CMMC documents were posted on the OUSD(A&S) CMMC website after the public comment period for DFARS Case 2019-D041 closed on November 30, 2020. These documents

reflected changes based on review of public comments. Future updates to CMMC guidance documentation will be made as needed.

Comment: One comment suggested that audit standards be determined for CMMC assessments. Two comments asked for clarification regarding references provided in the model, whether all references must be reviewed, and if the requirements within the references must also be achieved.

Response: The Department has reviewed definitions of audit and assessments and determined "assessment" best meets the goals of the CMMC Program. The cybersecurity standard requirements for the different CMMC Levels are set forth in § 170.14 and clarify references for the security requirements.

Comment: Many commenters were concerned about the lack of waivers or POA&Ms. Several commenters commented that not allowing waivers is impractical and will impact the ability of businesses to qualify for contract award. Commenters asked for clarification on the differences between POA&M that are not allowed by CMMC and the plans of action as required in the CMMC Level 3 control (now CMMC Level 2 under CMMC 2.0), CA.2.159 (now CA.L2-3.12.2 under CMMC 2.0). Many noted that POA&Ms are necessary when managing activities like system upgrades, vendor changes, and company acquisitions to avoid temporarily falling out of compliance.

Response: Under certain circumstances, the CMMC Program does permit contract award to organizations that have an approved and time limited POA&M. See § 170.21 for additional information on POA&Ms. There is no process for organizations to request waiver of CMMC solicitation requirements. DoD internal policies, procedures, and approval requirements will govern the process for DoD to waive inclusion of the CMMC requirement in the solicitation.

22. The Accreditation Body and C3PAOs

Comment: Many commenters had questions and concerns about the management of the Accreditation Body and C3PAOs. A few commenters suggested using a government entity

instead of the Accreditation Body construct to manage assessments. Commenters asked about the governance, resourcing, and oversight of the Accreditation Body with respect to CMMC training and assessments. Commenters expressed concerns such as who would make final decisions about CMMC issues, the lack of clearly defined roles and responsibilities for CMMC governance, and the long-term effectiveness of the Accreditation Body staffed by an all-volunteer workforce. One comment asked how the Accreditation Body can legally license training when CMMC Program information is available for free.

Response: The decision to use a non-governmental Accreditation Body was made because the DoD determined that there was insufficient capacity within the DoD to manage assessor training and assessments for all defense contractors who need to comply with CUI protection policies. The DoD CMMC PMO provides oversight of the Accreditation Body and is also responsible for developing, updating, maintaining, and publishing the CMMC Model, CMMC Assessment Guides, and policies for implementation of the CMMC Program.

Roles and responsibilities of the CMMC PMO, the Accreditation Body, and its organizations are described in SUBPART C of this rule. The Accreditation Body accredits C3PAOs and the CAICO. The Accreditation Body authorizes the CAICO to certify CMMC assessors and instructors and the C3PAOs to conduct assessments using CAICO-certified assessors.

Comment: Many commenters expressed concerns about how to ensure the necessary independence, quality assurance, integrity, and rigor of, and protection against potential conflicts of interest within the Accreditation Body and C3PAOs. Numerous commenters recommended the use of ISO/IEC standards to address these issues. Additionally, one commenter was concerned about high costs for assessments that could result if there is a lack of oversight for charging fees.

Response: The Accreditation Body is required to become compliant with the ISO/IEC 17011:2017 standard (the international benchmark used in demonstrating an accreditation body's impartiality, technical competency, and resources) and the requirements set forth in § 170.8.

Additionally, the C3PAOs and CAICO must comply with requirements as specified in § 170.9 and § 170.10, respectively, including the specified ISO/IEC standards.

Comment: To address a perceived shortage of CMMC C3PAO assessors, two commenters suggested authorizing the use of other ISO/IEC-compliant accreditation bodies to increase the numbers of assessors. Another commenter wanted to know how a company could become an accreditation body.

Response: Consistency in training is imperative due to the unique qualifications needed to understand requirements. Additionally, ISO/IEC 17024:2012 Conformity Assessment requirements are levied against the CAICO and may not be required by other entities. The number and level of assessors needed is relative to the number of companies seeking CMMC assessment. The demand level is influenced, but not solely determined by, the number of solicitations that include CMMC requirements, the CMMC Levels specified, and the estimated number of subcontractors that will also need to meet CMMC requirements, when flowed down by the prime contractor. To facilitate a smooth and orderly transition to CMMC, the Department will issue policy guidance to government Program Managers to govern the rate at which CMMC requirements are levied in new solicitations. The implementation phases are described in § 170.3(e). The CMMC PMO has visibility into the Accreditation Body's assessor training activities, tracks the anticipated number of trained assessors, and will use this information to inform policies that guide government Program Managers in identifying CMMC requirements in new solicitations.

23. Relationship to Existing Regulations

Comment: Several commenters asked about the implications of having DFARS clauses 252.204-7012 and 252.204-7021 coexist in contracts and wanted to know if all the 252.204-7012 requirements, including the requirements for "adequate security," incident reporting, and flow-down, apply in the presence of 252.204-7021. Others were concerned about a perceived conflict on the protection of CUI between NIST SP 800-171 Rev 2, which specifies the minimum

requirements to provide "adequate security" for CUI on nonfederal systems and DFARS clause 252.204-7021 based on the CMMC Program. Multiple commenters wanted to know if the 252.204-7021 clause and the CMMC requirements override contractor responsibility to comply with other applicable clauses of the contract, or other applicable U.S. Government statutory or regulatory requirements. Others were concerned about a continued proliferation of security requirements.

Response: CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract, including DFARS clause 252.204-7021. As such, DoD cannot address applicability of or changes to current DFARS clause 252.204-7021 or other current DFARS cybersecurity provisions or clauses at this time.

DoD does not intend to impose duplicative cybersecurity protection or assessment requirements. There is no conflict between the CMMC cybersecurity protection requirements described in this rule and DoD's current information safeguarding requirements, including those set forth in DFARS clause 252.204-7012. This CMMC rule adds new requirements for the assessment of contractor implementation of underlying information security standards and guidelines, as applicable, such as those set forth in FAR clause 52.204-21 and in the NIST SP 800-171 Rev 2. This rule also prescribes additional information security protection and assessment requirements for CMMC Level 3, derived from NIST SP 800-172, for certain limited scenarios.

As new cyber threats emerge, security requirements will continue to evolve to support efforts to protect information important to U.S. national security. However, alternate standards will continue to be reviewed, as described in § 170.20, to minimize the burden of new requirements.

24. Phase-out of Existing Cybersecurity Requirements

Comment: Several commenters asked whether DFARS clause 252.204-7012, DFARS provision 252.204-7019 and 252.204-7020 will be phased out since DFARS clause 252.204-7021 is now a requirement.

Response: The CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses, including DFARS clause 252.204-7021. As such, DoD cannot address applicability of or changes to current DFARS clause 252.204-7021 or other current DFARS cybersecurity provisions or clauses at this time.

The information safeguarding requirements and cyber incident reporting requirements set forth in DFARS clause 252.204-7012 will not be phased out as a result of this rule. CMMC Program requirements provide DoD with verification, through self or third-party assessment, that defense contractors have, in fact, implemented DoD's cybersecurity protection requirements.

In addition, the requirements of this rule will not be fully implemented (and will not appear in all DoD contracts) until 2026 or later. As such, DoD will continue to require the current cybersecurity protections as reflected in the identified DFARS provisions and clauses for contracts that do not include a CMMC requirements.

Applicability

The CMMC Program will require DoD to identify CMMC Level 1, 2, or 3 as a solicitation requirement 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 48 CFR, DoD will specify the required CMMC Level in the solicitation and the resulting contract.

Summary of Program Changes: DFARS Case 2019-D041 implemented DoD's original model for assessing contractor information security protections, which is referred to as "CMMC 1.0." CMMC 1.0 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 CMMC 2.0, 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 CMMC 1.0 Level 1;
    - Level 2 will be similar to CMMC 1.0 Level 3;
- Level 3 will be similar to CMMC 1.0 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 self-assessment rather than C3PAO assessment.
- For CMMC Level 3, requiring Department-conducted assessments; and
- Developing a time-bound and enforceable POA&M process.

The CMMC Program will be implemented through publication of rules for both title 32 CFR and title 48 CFR. Both rules will have public comment periods.

Background

A. Statement of Need for This Rule

The Department of Defense (DoD) requires defense contractors to protect sensitive unclassified information in accordance with requirements for 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 level. 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 its sensitive unclassified information 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 certification 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[19]. The Center for Strategic and International Studies estimates that the total global cost of cybercrime was as high as $600 billion in 2017.[20]

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[21] that process, store, or transmit CUI or FCI in support 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

[19] Based on information from the Council of Economic Advisors report: The Cost of Malicious Cyber Activity to the U.S. Economy, 2018.
[20] Based on information from the Center for Strategic and International Studies report on the Economic Impact of Cybercrime; https://www.csis.org/analysis/economic-impact-cybercrime.
[21] 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).

can achieve a specific CMMC Level for its 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 Subpart 204.73, as well as selected NIST SP 800-172 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 Rev 2. CMMC Level 3 requires implementation of the security requirements in NIST SP 800-171 Rev 2 as well as selected NIST SP 800-172 requirements, with DoD specified parameters. The CMMC requirements for all three Levels are provided in § 170.14. In general, CMMC assessments do not duplicate efforts from existing DoD assessments. In rare 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 Level and demonstrate implementation of the associated set of information protection requirements.

If CMMC Level 1 or Level 2 Self-Assessment is a contract requirement, the defense contractor will be required to self-assess its compliance with the CMMC Level 1 or Level 2 requirements and submit the assessment results and an affirmation of conformance in SPRS. CMMC Level 1 self-assessment and associated affirmation is required annually. CMMC Level 2 Self-Assessment is required triennially with an affirmation following self-assessment and annually thereafter.

If CMMC Level 2 Certification Assessment is a contract requirement, CMMC assessments must be performed by an authorized or accredited CMMC Third Party Assessment Organization (C3PAO). When CMMC Level 3 Certification Assessment is a contract requirement, an

assessment by DoD is required following a CMMC Level 2 Final Certification Assessment. Upon completion of a CMMC Level 2 or 3 Certification Assessment, the offeror may be granted a certification of assessment based on the results of the assessment at the appropriate CMMC Level (as described in the CMMC Model). The assessment results are documented in SPRS to enable contracting officers to verify the validity status of an offeror's certification level and currency (i.e., not more than three years old) prior to contract award. The offeror must also submit an affirmation of conformance in SPRS following the assessment and annually thereafter.

CMMC allows the use of a Plan of Action and Milestones (POA&Ms) for specified CMMC Level 2 and 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, third-party assessment, and affirmation for each CMMC Level, are provided in § 170.15 through § 170.18. POA&M requirements, including which requirements are allowed to be on a POA&M and POA&M closeout requirements, in addition to requirements for provision of an affirmation at closeout, contract eligibility, and continuation are provided in § 170.21 and § 170.22.

DoD's phased implementation of CMMC requirements is described in § 170.3(e). Once CMMC requirements have been implemented in the DFARS, the solicitation will identify the specific CMMC Level required for that procurement. To implement a phased transition, selection of a CMMC Level 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 third party assessment requirements to a particular procurement. In such cases, the solicitation will not include a CMMC assessment 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 Level. Furthermore, CMMC requirements are required to flow down to subcontractors as prescribed in the solicitation 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. (https://www.govinfo.gov/content/pkg/USCODE-2009-title5/pdf/USCODE-2009-title5-partI-chap3-sec301.pdf)

Section 1648 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92)[22] 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 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 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 sensitive unclassified information that is shared by the Department with or generated by its contractors and subcontractors. The

[22] https://www.govinfo.gov/content/pkg/PLAW-116publ92/pdf/PLAW-116publ92.pdf

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 Rev 2 guidelines, which is presently required by DFARS clause 252.204-7012 (CMMC Level 2), and additional selected requirements from the NIST SP 800-172 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 an interim rule to the DFARS in the Federal Register (DFARS Case 2019-D041), which implemented the DoD's initial vision for the CMMC Program ("CMMC 1.0") and outlined the basic features of the program (tiered model, required assessments, and implementation through contracts). The interim 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 interim DFARS rule. This comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

In November 2021, the Department announced CMMC 2.0, 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.

The CMMC requirements established pursuant to DFARS Case 2019-D041 have not been revised as of the date of publication of this rule. However, the CMMC Program requirements proposed in this 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.

Regulatory Impact Analysis

FAR Subpart 4.19 and DFARS Subpart 204.73 address safeguarding of FCI and CUI in contractor information systems and prescribe contract clauses requiring protection of FCI and 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 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, 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 in 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 Rev 2, 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 Level for contractors and subcontractors will be specified in the solicitation and Requests for Information (RFIs), if utilized.

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 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 https://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[23], Colonial Pipeline, Hafnium[24], and Kaseya[25] attacks, have been spearheaded or influenced by nation-state actors[26] 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 [27]. Protection of DoD's sensitive unclassified information is critically important, and the DoD needs assurance that contactor information

[23] https://www.gao.gov/assets/gao-22-104746.pdf
[24] https://www.ic3.gov/Media/News/2021/210310.pdf
[25] https://www.cisa.gov/uscert/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa
[26] https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf
[27] https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

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 DoD and defense contractor sensitive unclassified information in accordance with requirements for 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 DFARS interim rule (Case 2019-D041), which implemented DoD's initial vision for the Cybersecurity Maturity Model Certification (CMMC) Program ("CMMC 1.0") 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, and implementation of all security requirements by the time of a contract award. A total of 750 comments were received on the CMMC Program 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 CMMC 1.0. 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 Rev 2 to provide adequate security for sensitive unclassified DoD information that is processed, stored, or transmitted on contractor information systems and to document their implementation status, including any plans of action for any NIST SP 800-171 Rev 2 requirement not yet implemented, in a System Security Plan. 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 requirements that addressed many of the concerns identified in the public comments received relating to CMMC 1.0. These changes have been incorporated into the CMMC Program structure and policies, now referred to as "CMMC 2.0." 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 in CMMC 2.0 that are responsive to prior SBA concerns.

The CMMC Program will enhance the ability of the DoD to safely share sensitive unclassified information 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 third-party or DoD as a condition of a DoD contract award. CMMC is designed to validate the protection of sensitive unclassified information that is shared with and generated by the Department's contractors and subcontractors. Through protection of information by adherence to the requirements verified in CMMC 2.0, the Department and its contractors will prevent disruption in service and the loss of intellectual property and assets, and thwart access to sensitive unclassified information 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 level. 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 sensitive unclassified information (i.e., 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 its sensitive unclassified information 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 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[28] 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 252.204-7012, *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 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 Rev 2, 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.

---

[28] DODIG-2019-105 "Audit of Protection of DoD CUI on Contractor-Owned Networks and Systems"

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 52.204-21 nor the security requirements specified in NIST SP 800-171 Rev 2, 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.

CMMC 2.0 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 level for contractors will be specified in the solicitation. In accordance with the implementation plan described in 32 CFR 170.3(e), CMMC compliance or certification 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 level 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:

CMMC Level 1 Self-Assessment

- CMMC 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 52.204-21.
- Organizations Seeking Assessment (OSAs) will submit the following information in SPRS

prior to award of any prime contract or subcontract and annually thereafter:

1. the results of a self-assessment of the OSA's implementation of the basic safeguarding requirements set forth in 32 CFR 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 32 CFR 170.22.

3. the Level 1 Self-Assessment cost burden will be addressed as part of the 48 CFR acquisition rule.

CMMC Level 2 Self-Assessment

- CMMC Level 2 Self-Assessment requires compliance with the security requirements set forth in NIST SP 800-171 Rev 2 to protect CUI. CMMC Level 2 does not add any additional security requirements to those identified in NIST SP 800-171 Rev 2.
- OSAs will submit the following information in SPRS prior to award of any prime contract or subcontract:

1. the results of a self-assessment of the OSA's implementation of the NIST SP 800-171 Rev 2 requirements set forth in 32 CFR 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 32 CFR 170.22.

3. the Level 2 Self-Assessment cost burden will be addressed as part of the 48 CFR acquisition rule.

CMMC Level 2 Certification Assessment

- CMMC Level 2 Certification requires compliance with the security requirements set forth in in 32 CFR 170.17 to protect CUI. CMMC Level 2 does not add any additional security

requirements to those identified in NIST SP 800-171 Rev 2.

- A CMMC 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 Rev 2 security requirements prior to award of any prime contract or subcontract and exercise of option.
- The C3PAO will upload the CMMC Level 2 results in 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 thereafter, an affirmation of continued compliance as set forth in 32 CFR 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 Title 48 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.

CMMC Level 3 Certification Assessment

- CMMC Level 3 Certification Assessment requires a CMMC Level 2 Final Certification Assessment and compliance with the security requirements set forth in 32 CFR 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 CMMC 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. A CMMC Level 2 Final Certification is a

prerequisite to schedule a DIBCAC assessment for CMMC Level 3.

- DCMA DIBCAC will upload the CMMC Level 3 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 thereafter, an affirmation of continued compliance as set forth in 32 CFR 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 Title 48 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 its sensitive unclassified information 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 CMMC 2.0

Implementation of the CMMC Program is intended to solve the following policy problems:

Verifies the Contractor 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 Rev 2 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.

Implementation of Cybersecurity Requirements

Under DFARS clause 252.204-7012, defense contractors and subcontractors must document implementation of the security requirements in NIST SP 800-171 Rev 2 in a system security plan and may use a Plan of Action Milestones to describe how and when any unimplemented security requirements will be met. For the CMMC Program, the solicitation, will specify the required CMMC level, which will be determined considering program criticality, information sensitivity, and severity of cyber threat. Although the security requirements in NIST SP 800-171 Rev 2 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 800-172 to reduce the risk of APT threats.

The CMMC Program will require prime contractors to flow the appropriate CMMC 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.

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. CMMC 2.0 requires prime contractors to flow down appropriate CMMC Level 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 CMMC 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 CMMC Certification Assessment. 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 CMMC 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.

CMMC 2.0 Implementation

The DoD is implementing a phased implementation for CMMC 2.0 and intends to introduce CMMC 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 when warranted by the type of information that will be handled by the contractor of subcontractor(s). CMMC requirements for Levels 1, 2, and 3 will be included in solicitations 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 requirements or exclude them and rely upon existing DFARS Clause 252.204-7012 requirements, in accordance with DoD policy. As stated in 32 CFR 170.20(a), there is qualified standards acceptance between DCMA DIBCAC High Assessment and CMMC Level 2, which will result in staggering of the dates for new CMMC Level 2 assessments. The implementation period will consist of four (4) phases as set forth in 32 CFR 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 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.

CMMC 2.0 Flow Down

CMMC Level requirements will be flowed down to subcontractors at all tiers as set forth in

32 CFR 170.23; however, the specific CMMC Level 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 CMMC 2.0 Program

In November 2021, the Department announced "CMMC 2.0," which is an updated program structure with revised requirements. In CMMC 2.0, 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 CMMC 2.0 to NIST guidelines, the Department's requirements will continue to evolve as changes are made to the underlying NIST SP 800-171 Rev 2 and NIST SP 800-172 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.

CMMC Level 1 Self-Assessment

An annual CMMC 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 32 CFR 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 does not result in a CMMC certification. An OSA can be compliant with CMMC Level 1 requirements for an entire enterprise network or for a particular enclave(s), depending upon where the FCI is or will be processed, stored, or transmitted.

CMMC Level 2 Self-Assessment

A CMMC Level 2 Self-Assessment and triennial affirmation attests that an OSA has implemented all the security requirements to protect CUI as specified in 32 CFR 170.14(c)(3).

CMMC Level 2 Certification Assessment

A CMMC Level 2 Certification Assessment, conducted by a C3PAO, verifies that an OSC is conforming to the security requirements to protect CUI as specified in 32 CFR 170.14(c)(3). A CMMC Level 2 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.

CMMC Level 3 Certification Assessment

Receipt of a CMMC Level 2 Final Certification Assessment for information systems within the Level 3 CMMC Assessment Scope is a prerequisite for a CMMC Level 3 Certification Assessment. A CMMC 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 32 CFR 170.14(c)(4). A CMMC 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 CMMC 2.0

Summary of Impact

Public comment feedback on CMMC 1.0 indicated that cost estimates were too low. CMMC 2.0 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 CMMC 2.0 costs may be higher than those included in CMMC 1.0.

The CMMC 2.0 impact analysis includes estimated costs for implementation of CMMC 2.0 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 1 - 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 2 - 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 CMMC 1.0 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 3 - 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 4 - *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 5 - *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 6 - *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%).[29]

Public Cost Analysis

[29] 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.

The following is a summary of the estimated Public costs CMMC 2.0 for other than small[30] entities, per assessment of a contractor information system, at the required periodicity for each CMMC level.

Table 7 - Other Than Small Entities (per Assessment)

Assessment Phase ($)	Level 1 Self-Assessment [31]	Level 2 Self-Assessment[31]	Level 2 Certification	Level 3 Certification
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 CMMC 2.0 for Small Entities, per assessment of each contractor information system, estimated at one per entity, at the required periodicity for each CMMC level.

Table 8 - Small Entities (per Assessment)

[30] 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)
[31] The Level 1 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 acquisition rule.

Assessment Phase ($)	Level 1 Self-Assessment[32]	Level 2 Self-Assessment[32]	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**

*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 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 9 - 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[33], assessment costs, and affirmation costs for each CMMC Level. For CMMC Levels 1 and 2, the cost estimates are based only upon 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, 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 Rev 2. DoD did not

[32] The Level 1 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 acquisition rule.
[33] The terms nonrecurring engineering costs and recurring engineering costs are terms of art and do not only encompass actual engineering costs.

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, 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)
- entities (small and other than small) pursuing CMMC 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)) 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 cybersecurity 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 800-171 Rev 2 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 as described in 32 CFR 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 52.204-21 and NIST SP 800-171 Rev 2 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 52.204-21 and NIST SP 800-171 Rev 2 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 32 CFR 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 10 - Other than Small Entities - Labor Rates Used for Estimate

Code[34]	Rate per Hour[35]	Description	Background / Years' Experience[36]	With Master's Degree[36]
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	

[34] IT = Information Technology, MGMT = Management
[35] IT and MGMT rates represent an estimate for in-house labor and includes the labor rate plus fringe and employee-related expenses
[36] 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.

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[37]	$ 260.28	Cyber Subject Matter Expert	4 years	

Table 11 - Small Entities – Labor Rates Used for Estimate

Code[34]	Rate per Hour[35]	Description	Background / Years' Experience[36]	Master's Degree[36]
MGMT5	$ 190.52	Director	Chief Info. Systems Officer / Chief Info. Officer	
IT4-SB	$ 86.24	Staff IT Specialist	Cyber Background, 7-10 years	5-7 years
ESP / C3PAO[37]	$ 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.[38]
- ***Assessments Costs****:* It is estimated that the cost to support a CMMC Level 1 self-assessment and affirmation is ***$4,042** (as summarized in 4.1.2, Table 1). A Level I Self-Assessment is conducted annually, and is based on the assumptions detailed:

- **Phase 1: Planning and preparing for the 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)

[37] The ESP / C3PAO rate represents an estimate for outsourced labor and includes the labor rate, overhead expense, G&A expense, and profit.
[38] 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.

- A staff IT specialist (IT4) for 6 hours ($97.49/hrs x 6hrs = $585)

- **Phase 3: Reporting of 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 acquisition rule.

- **Summary:** The following is the annual other than small entities total cost summary for CMMC 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 12 – 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
Total	**36,191**		**$872,309,779**

- ***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.[39]
- ***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 4.1.2, Table 2). A Level I Self-Assessment is conducted annually, and is based on the assumptions detailed:
    - **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) 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 hours40 ($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-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 acquisition rule.
- ***Summary:*** The following is the annual small entities total cost summary for CMMC Level 1

[39] Again, it is assumed that that defense contractors and subcontractors have already implemented the 15 basic safeguarding requirements in FAR clause 52.204-21.
[40] A person needs to enter the information into SPRS, which should only take five minutes.

self-assessments and affirmations over a ten-year period: (Example calculation, Year 1: *$5,977 per entity x 699 entities (cumulative) = $4,177,845)

Table 13 – 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**

All Entities Summary

The following is a summary of the combined costs for both small and other than small entities for CMMC Level 1 Self-Assessments and Affirmations over a ten-year period:

Table 14 – 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 CMMC Level 2 Self-Assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 Rev 2 security requirements.

- ***Self-Assessment Costs and Initial Affirmation Costs:*** It is estimated that the cost to support a CMMC Level 2 self-assessment and affirmation is *$43,403. The three-year cost is $48,827 (as summarized in 4.1.2, Table 1), which includes the triennial assessment + affirmation, and two additional annual affirmations ($43,403 + $2,712 + $2,712).
  - **Phase 1: Planning and preparing for the 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 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 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 15 - 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 CMMC Level 2 Self-Assessment since it is assumed the

contractor or subcontractor has implemented the NIST SP 800-171 Rev 2 security requirements.

- ***Self-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 three-year cost is $37,196 (as summarized in 4.1.2, 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 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 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 CMMC Level 2 Self-Assessment annually is **$1,459** (three-year costs to reaffirm a CMMC 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 acquisition rule.
- ***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 16 - 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 CMMC Level 2 Self-Assessments and affirmations over a ten-year period:

Table 17 - 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 CMMC Level 2 Certification Assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 Rev 2 security requirements.

- ***Assessment and Initial Affirmation Costs:*** It is estimated that the cost to support a CMMC 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 1), 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 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 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 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 CMMC 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 acquisition rule.
- ***Summary****:* The following is the annual other than small entities total cost summary for CMMC Level 2 Certifications 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 18 - Level 2: Certification 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 CMMC Level 2 Certification Assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 Rev 2 security requirements.

- ***Assessment Costs and Initial Affirmation Costs****:* It is estimated that the cost to support a CMMC Level 2 Certification Assessment and affirmation for a small entity is ***$101,752.** The three-year cost is $104,670 (as summarized in 4.1.2, Table 2), 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 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 CMMC 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 acquisition rule.

- ***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 19 - Level 2: Certification 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 CMMC Level 2 Certification and Affirmation costs over a ten-year period:

Table 20 - Level 2: Certification 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 must have a CMMC Level 2 Final Certification Assessment, and also must demonstrate compliance with CMMC Level 3, which includes implementation of selected security requirements from NIST SP 800-172 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 requirements. The cost estimates account for time for an OSC to implement these security requirements and prepare for, support, participate in, and closeout a CMMC Level 3 Certification Assessment conducted by DCMA DIBCAC. The OSC should keep in mind that the total cost of a CMMC 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**[41]
- **Recurring Engineering Costs: $4,120,000**
- ***Assessment Costs and Initial Affirmation Costs**:* It is estimated that the cost to support a CMMC Level 3 Certification 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 1), and includes the triennial assessment + affirmation, plus two additional annual affirmations ($39,021 + $2,712 + $2,712)
    - **Phase 1: Planning and preparing for the 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)

[41] DoD utilized subject matter expertise from Defense Pricing and Contracting (DPC) and DCMA DIBCAC to estimate the Nonrecurring and Recurring Engineering Costs.

- 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 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 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[42] (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 CMMC 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)

[42] Costs for closing out POA&Ms are included at Level 3 because the requirement to implement a subset of NIST SP 800-172 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 Rev 2 security requirements are already required.

- 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 acquisition rule.

- ***Summary****:* The following is the annual other than 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 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) + Nonrecurring Engineering cost ($105,500,000) + Recurring Engineering cost ($24,720,000), or $145,432,897.

Table 21 - Level 3 Certification for Other Than Small Entities

Yr	Entities Performing Triennial Certification Including Initial Affirmation	Entities Performing Re-affirmation 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 CMMC Level 3 Certification Assessment for a small entity is ***$9,050** The three-year cost is $12,802 (summarized in 4.1.2, 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 assessment: $1,905**
    - A director (MGMT5) for 10 hours ($190.52/hr x 10hrs = $1,905)
  - **Phase 2: Conducting the assessment: $1,524**
    - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
  - **Phase 3: Reporting of 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[43] (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 CMMC 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)
  - The Level 3 Affirmations cost burden will be addressed as part of the 48 CFR acquisition rule.

[43] Costs for closing out POA&Ms are included at Level 3 because the requirement to implement a subset of NIST SP 800-172 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 Rev 2 security requirements are already required.

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 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 22 - Level 3 Certification for Small Entities

Yr	Entities Performing Triennial Certification Including Initial Affirmation	Entities Performing Re-affirmation 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 CMMC Certification Assessments and affirmations over a ten-year period:

Table 23 - Level 3 Certification for All Entities

Yr	Entities Performing Triennial Certification Including Initial Affirmation	Entities Performing Re-affirmation Actions Only	Triennial Certs and Affirmation Total Cost	Nonrecurring Engineering Cost	Recurring Engineering Cost	Total Cost
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 24 – 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 in 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.[44] 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.[45]

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 +

[44] Nonrecurring engineering costs were first incurred in FY20. The cost has inflation applied to put the value in 2023 base year (BY) dollars.

[45] The cost for the recurring engineering cost is based on the costs incurred in FY20 and FY21. The values for Year 1 (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.

$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 25 - 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 26 – 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 27 - 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 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 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. 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 their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI. The Department seeks public comment on the requirement to achieve a specified CMMC level by the time of contract award.

Benefits

The Department of Defense expects this proposed rule to protect DoD and industry from the loss of FCI and CUI, including intellectual property. The theft of intellectual property and sensitive unclassified information 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[46]. 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[47].

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.[48] The protection of FCI, CUI, and intellectual property on defense contractor systems can directly impact the ability of the federal government to successfully conduct its essential missions and

[46] https://www.govinfo.gov/content/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm
[47] https://www.nbr.org/program/commission-on-the-theft-of-intellectual-property/
[48] https://www.cybernc.us/fci-cui/

functions[49].

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[50].

In addition to stealing intellectual property for military gains, Russia may conduct cyber-attacks against the U.S. for retaliatory purposes. On March 21, 2022, that 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[51].

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

---

[49] GAO Report to Congress, Defense Contractor Cybersecurity Stakeholder Communication and Performance Goals Could Improve Certification Framework, Dec 2021.
[50] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-047a
[51] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

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 and NIST SP 800-172. 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 final certification assessment. 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
- 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 unclassified information by applying additional requirements. Implementation of CMMC will help protect DoD's sensitive unclassified information 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"

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 proposed rule is significant as defined by Section 3(f)(1) for purposes of Executive Order 12866.

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 https://www.regulations.gov (search for "DoD-2023-OS-0063" click "Open Docket" and view "Supporting Documents").

This initial regulatory flexibility analysis has been prepared consistent with 5 U.S.C. 603.

(1) Reasons for the Action

This proposed 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,"[52] emphasized that industrial security needs strengthening to ensure investments are not lost through intellectual property theft, among other supply chain risks.

[52] https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/technology-products-services/it-security/executive-order-14028?gclid=CjwKCAjwrranBhAEEiwAzbhNtbkRN9aYRpHsrVE6jJroenQW0tC_DGtCLYch8KBJ_f5dny_LtBNziBoCukIQAvD_BwE

Currently, the FAR and DFARS prescribe contract clauses intended to protect FCI and CUI within the DoD supply chain. 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. 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*, 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 Rev 2, 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 52.204-21 nor DFARS 252.204-7012, provide for DoD verification of a contractor's implementation of basic safeguarding requirements specified in FAR 52.204-21 nor the security requirements specified in DFARS 252.204-7012 which requires implementation of NIST SP 800-171 Rev 2 prior to contract award. Instead, DFARS clause 252.204-7012 requires prospective contractors or subcontractors to self-attest upon submission of their offer that they have implemented or will implement NIST SP 800-171 Rev 2.

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 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.

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.

The Cybersecurity Maturity Model Certification (CMMC) Program verifies compliance with DoD cyber protection standards by defense contractors and subcontractors. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. 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 implement cybersecurity requirements at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forth the process for information flow down to subcontractors.
    - **Assessment Requirement:** CMMC assessments allow the Department to verify the implementation of cybersecurity requirements.
    - **Implementation through Contracts:** Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

In September 2020, the DoD published an interim DFARS rule in the Federal Register (DFARS Case 2019-D041) that implemented the DoD's initial vision for the CMMC Program ("CMMC 1.0") and outlined the basic features of the program (tiered model, required assessments, and implementation through contracts). The interim 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 interim DFARS rule. This

comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

In November 2021, the Department announced "CMMC 2.0," which is an updated program structure and revised requirements designed to achieve the primary goals of an internal DoD review of the CMMC Program. With the implementation of CMMC 2.0, the Department 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 guidelines.
- 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.
- Allowing companies, under limited circumstances, to make Plan of Action & Milestones (POA&M) to achieve certification.

In July 2022, the CMMC PMO met with the Office of Advocacy for the U.S. SBA to address the revisions planned in CMMC 2.0 that are responsive to prior SBA concerns. As a result of the alignment of CMMC 2.0 to NIST guidelines, the Department's requirements will continue to evolve as changes are made to the underlying NIST SP 800-171 Rev 2 and NIST SP 800-172 requirements.

(2) 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 proposed rule (CMMC Program rule) is to provide the Department with increased assurance that a defense contractor can adequately protect sensitive unclassified information commensurate with the risk, 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 implement15 basic cyber hygiene requirements, as applicable, to protect contractor information systems that process, store, or transmit FCI.

December 31, 2017, was DoD's deadline for contractors to implement, as applicable, the cybersecurity protection requirements set forth in NIST SP 800-171 Rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, in accordance with DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. The current NIST 800-171A Assessment Guide 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 [in a Plan of Action].[53]" NIST's 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. As such, a contractor could be compliant with NIST SP 800-171 Rev 2 if some of NIST SP 800-171 Rev 2 requirements are implemented but others are listed in a Plan of Action. As a result, at present, defense contractors and subcontractors can process, store, or transmit CUI without having implemented all security requirements set forth in NIST SP 800-171 Rev 2 and without establishing concrete, prompt, and enforceable timelines for addressing shortfalls and gaps documented in the Plan of Action.

Findings from DoD Inspector General report (DODIG-2019-105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicated

[53] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf

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 a third-party assessment requirement, as applicable, to verify defense contractors and subcontractors have implemented the required security requirements prior to award. CMMC also adds affirmation processes at every CMMC level requiring contractors and subcontractors to attest to compliance with CMMC's security requirements and then provide annual affirmations thereafter.

(b) ***Comprehensive implementation of cybersecurity requirements***

Although the security requirements in NIST SP 800-171 Rev 2 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, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 Rev 2. CMMC Level 3 provides for government assessment of a contractor's implementation of a defined subset of NIST SP 800-172 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. CMMC 2.0 requires prime contractors to flow down appropriate CMMC Level 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 CMMC Level 2 Certification Assessments of actual and prospective DoD contractors and subcontractors. OSCs will directly contract with an authorized or accredited C3PAO to obtain a CMMC Certification Assessment. 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 CMMC 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 the 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 decreases costs to both DoD and industry.

(3) Anticipated Benefits and Costs

(a) Benefits

The CMMC Program validates implementation of DoD's required cyber protection standards for companies in the DIB. Furthermore, this rule benefits the efficient functioning of the

economy and private markets for all sizes of companies, including the smallest, most vulnerable companies, by: (1) protecting DoD from the loss of FCI and CUI; (2) promoting improvements in cybersecurity and accountability across DoD supply chains; (3) promoting continued innovation by helping to prevent significant loss of revenue, benefits, and jobs to the companies involved in developing those innovations for DoD; (4) promoting U.S. technical advantage and superiority; and (5) improving the safeguarding of competitive advantages and protections for proprietary information and capabilities through requirements flow-down throughout the defense contractor supply chain.

(b) 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 is available at www.regulations.gov (search for “DoD-2023-OS-0063" click “Open Docket" and view “Supporting Documents"). 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:

Table 28 - Total Estimated Cost 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 29 - 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

The following shows the estimated number of small entities[54] anticipated to pursue compliance or certification, at each CMMC level, over a phased implementation. These estimates were generated based upon prior year procurement data.

Table 30 - Number of Small Entities Pursuing CMMC Over a Phased Implementation

Year	Level 1 Self-Assess	Level 2 Self-Assess	Level 2 Certification	Level 3 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
Total	**103,010**	**2,961**	**56,689**	**1,327**	**163,987**

The following is a summary of the estimated public costs of CMMC for small entities, per assessment of each contractor information system, at the required periodicity for each CMMC level.

Table 31 - Small Entities (per Assessment)

Assessment Phase ($)	Level 1 Self-Assessment	Level 2 Self-Assessment	Level 2 Certification	Level 3 Certification
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**

*Reflects the 3-year cost to match the periodicity.
**Requirements "NOT MET" (if needed and if allowed) will be documented in a Plan of Action and Milestones.

The following estimates are Small Entity Public and Government costs for CMMC requirements calculated over a 20-year horizon in 2023 dollars at a 7 percent discount rate.

[54] Small entities are small business concerns.

Table 32 – Costs of CMMC Requirements for Small Businesses

	Public	Government	Total
Annualized Costs	$2,616,493,297	$7,238,247	$2,623,731,544
Present Value Costs	$27,719,167,263	$76,682,096	$27,795,849,359

4. Small Business Entities Impacted

This rule will impact small businesses that do business with the Department of Defense as a prime or subcontractor, except for contracts or orders that are exclusively for COTS items or valued at or below the micro-purchase threshold.

According to the Federal Procurement Data System (FPDS) there is an annual average of 30,145 unique small business contractors in DoD: FY 2019 (31,189), FY 2020 (29,166), FY 2021 (27,427) and FY 2022 (32,798).

Cost Assumptions and Analysis for CMMC 2.0

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 CMMC Program requirements are described in 32 CFR Subpart D.

(a) Comparison to CMMC 1.0 Cost Analysis

Public comment feedback on CMMC 1.0 indicated that cost estimates were too low. CMMC 2.0 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 CMMC 2.0 costs may be higher than those included in CMMC 1.0.

(b) Assumptions for CMMC 2.0 Cost Analysis

In estimating the public cost for a small defense contractor 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. These costs include labor and consulting.

Estimates include size and complexity assumptions to account for typical organizational differences between small companies and others 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)
- entities (small and other than small) pursuing CMMC 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 implementation (Non-recurring Engineering Costs (NRE)) or maintenance costs (Recurring Engineering (RE)[55]) 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 implementation of NIST SP 800-171 Rev 2 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 compliance

[55] The terms nonrecurring engineering costs and recurring engineering costs are terms of art and do not only encompass actual engineering costs.

with current 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. CMMC Level 3 security requirements are a selection of NIST SP 800-172 Enhanced Security Requirements as described in 32 CFR 170.14(c)(4) and are not currently required through other regulations. DoD expects that CMMC Level 3 will apply only to a small subset of defense contractors and subcontractors.

The Cost Categories used for each CMMC Level are described:

- ***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 52.204-21 and NIST SP 800-171 Rev 2 are assumed to have been 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.
- ***Recurring Engineering Costs****:* Estimates consist of annually recurring fees and associated labor for technology refresh. Costs associated with implementing the requirements defined in FAR 52.204-21 and NIST SP 800-171 Rev 2 are assumed to have been implemented and, therefore, are 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 company 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:

c) Labor hour estimates for a company (and any ESP support) to prepare for and participate in the assessment.

d) C3PAO cost estimates for companies pursuing a certification

- Labor hour estimates for certified or authorized assessors to work with the small business to conduct the actual assessment

e) 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 32 CFR 170.21.

Affirmations: Estimates consist of costs for a contractor or subcontractor to submit to SPRS an initial affirmation of compliance that the contractor information system is compliant with and will maintain compliance with the 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 comparable industry data and are defined in the table.

Table 33 - Small Entities - Labor Rates Used for Estimate

Code[56]	Rate per	Description	Background /	With Master's

[56] IT = Information Technology, MGMT = Management

	Hour[57]		Years' Experience[58]	Degree[58]
MGMT5	$ 190.52	Director	Chief Info. Systems Officer / Chief Info. Officer	
IT4-SB	$ 86.24	Staff IT Specialist	Cyber Background, 7-10 years	5-7 years
ESP / C3PAO[59]	$ 260.28	Cyber Subject Matter Expert	4 years	

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 or subcontractor has already implemented the basic safeguarding requirements set forth in FAR 52.204-21, which are the CMMC Level 1 security requirements.
- ***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 1) A Level I Self-Assessment is conducted annually, and is based on the assumptions detailed:
  - **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) 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)

[57] IT and MGMT rates represent an estimate for in-house labor and includes the labor rate plus fringe expenses
[58] 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.
[59] The ESP / C3PAO rate represents an estimate for outsourced labor and includes the labor rate, overhead expense, G&A expense, and profit

- A staff IT specialist (IT4-SB) for 0.08 hours[60] ($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-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 acquisition rule.

- **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 x 699 entities (cumulative) = $4,177,845)

Table 34 – 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[61]		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 account for a CMMC Level 2 Self-Assessment of the applicable contractor information system(s) with NIST SP 800-171 Rev 2 requirements based on assumptions defined.

---

[60] A person needs to enter the information into SPRS, which should only take five minutes.

[61] 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.

- ***Nonrecurring and recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with a CMMC Level 2 Self-Assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 Rev 2 security requirements.
- ***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 three-year cost is $37,196 (as summarized in 4.1.2, 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-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 CMMC Level 2 Self-Assessment annually is **$1,459** (three-year costs to reaffirm a CMMC 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 acquisition rule.

• ***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 35 - \ 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 account for a CMMC Level 2 Certification assessment and affirmation costs of the applicable contractor information system(s) with NIST SP 800-171 Rev 2 requirements based on the assumptions defined. 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 Rev 2 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), 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-SB) 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-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 acquisition rule.
- ***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 36 - 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

A company pursuing a Level 3 Certification must have an active, final CMMC Level 2 Certification, and also must demonstrate compliance with CMMC Level 3, which includes implementation of a subset of security requirements from NIST SP 800-172 that have DoD predefined selections and parameters. CMMC Level 3 requires compliance with certain security requirements 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 subset of NIST SP 800-172 requirements. The cost estimates account for time for a contractor or subcontractor to implement these security requirements and prepare for, support, and participate in a CMMC Level 3 assessment conducted by DoD. The company should keep in mind that the total cost of a Level 3 certification includes the cost of a Level 2 C3PAO assessment as well as the cost to implement and assess the requirements specific to Level 3. CMMC Level 3 is expected to affect a small subset of the DIB.

The estimated engineering costs per small entity associated with 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, 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-SB) 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-SB) 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-SB) for 4.08 hours ($86.24/hr x 4.08hrs = $352)

- The Level 3 Affirmations cost burden will be addressed as part of the 48 CFR acquisition rule.

- ***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 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 37 - Level 3 Certification for Small Entities

Yr	Entities Performing Triennial Certification including Initial Affirmation	Entities Re-affirmation 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**

Relevant Federal rules which may duplicate, overlap, or conflict with the rule.

The rule does not duplicate, overlap, or conflict with any other Federal rules. Rather, this rule allows DoD to validate and verify that defense contractors and subcontractors have implemented existing cybersecurity requirements set forth in FAR clause 52.204-21 and in the NIST SP 800-171 Rev 2, which are intended to protect FCI and CUI during contract performance.

D. Sec. 202, Public Law 104-4, "Unfunded Mandates Reform Act" (2 U.S.C. Chapter 25)

The Unfunded Mandates Reform Act requires agencies to assess anticipated costs and benefits before issuing a rule including mandates that require the spending of $100M dollars or more in a single year (in 1995 dollars and updated for inflation) by State, local, or Tribal governments, in the aggregate, or by the private sector. This rule's impact, if any, on State, local, or Tribal governments, in the aggregate, will not exceed $100M dollars or more in a single year, and it will not significantly or uniquely affect small governments. This rule is expected to have an impact on the private sector of $100M dollars or more annually; however, this rule is being published as a national security function of the United States as unauthorized disclosure of FCI or CUI information to parties outside the Department or foreign entities can cause significant harm to the interests of the United States. See the regulatory impact section of the preamble for an assessment of the costs and benefits for this rule.

E. Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

It has been determined that this rule, as proposed, does impose reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.) (PRA). DoD has submitted an information collection request (ICR) proposal to OMB. See the Supporting Statements in docket number DoD-2023-OS-0097 for specific details and to provide comments on the information collection requirements for the CMMC Program. Comments are invited on: (a) whether the proposed collections of information are necessary for the proper performance of the functions of DoD, including whether the information will have practical utility; (b) the accuracy of the estimate of the burden of the proposed information collections; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the information collections on respondents, including the use of automated collection techniques or other forms of information technology.

Part A: Estimation of Respondent Burden Hours and Labor Cost

For purposes of the proposed rule, DoD is proposing several separate information collections that will be addressed in the CMMC Title 32 Program rule and Title 48 acquisition rule.

CMMC Program Information Collections and Recordkeeping Requirements are discussed in four separate groupings:

(1) CMMC Level 1 Self-Assessment Collection

(2) CMMC Level 2 Self-Assessment Collection

(3) CMMC Level 2 Certification Assessment Collection

(4) CMMC Level 3 Certification Assessment Collection

CMMC Level 1 Self-Assessment Collection.

The Level 1 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 Title 48 acquisition rule. The information collection reporting and recordkeeping requirements include:

- OSAs conduct a self-assessment based on NIST guidelines as addressed in § 170.15 of this part.

  This is an assessment to validate implementation of the 15 security requirements listed in FAR clause 52.204-21(b)(1).

- OSAs upload assessment results and affirmations in SPRS in accordance with § 170.15 and §170.22 of this part.

CMMC Level 2 Self-Assessment Collection.

The 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 Title 48 acquisition rule. The information collection reporting and recordkeeping requirements include:

(a) OSAs conduct a self-assessment based on NIST guidelines as addressed in § 170.16.

This is an assessment to validate implementation of the 110 security requirements from NIST SP 800-171 Rev 2.

(b) OSAs upload assessment results and affirmations in SPRS in accordance with § 170.16 and §170.22.

(c) OSAs may have a POA&M at CMMC Level 2 as addressed in § 170.21(a)(2). OSAs must perform a POA&M closeout self-assessment and post compliance results in SPRS in accordance with § 170.16.

CMMC Level 2 Certification Assessment Collection.

The Level 2 Certification Assessment information collection reporting and recordkeeping requirements are included in this part with the exception of the requirement for the OSC to upload the affirmation in SPRS that will be included in the Title 48 acquisition rule and an update to the 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 information collection request (ICR) for this part and cover only those requirements pertaining to the CMMC process. The information collection reporting requirements for eMASS include:

- 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 as addressed in § 170.8(b)(9).
- C3PAOs submit pre-assessment and planning material, final assessment reports, and appropriate CMMC certificates of assessment into the CMMC instantiation of eMASS as addressed in § 170.9(b)(8). C3PAOs upload assessment data compliant with the CMMC assessment data standard into the CMMC instantiation of eMASS as addressed in § 170.9(b)(18).

- C3PAOs post POA&M closeout assessment compliance results into the CMMC instantiation of eMASS in accordance with § 170.17(a)(1)(ii)(B) of this part.
- C3PAOs upload artifacts (list of artifacts, hash of artifacts, and hashing algorithm used) into the CMMC instantiation of eMASS as addressed in § 170.9(b)(18)of this part.
- C3PAOs submit assessment appeals, review records, and decision results of assessment appeals using the CMMC instantiation of eMASS as addressed in § 170.9(b)(21) of this part.

Additional information collection reporting and recordkeeping requirements for this part include:

- OSCs prepare for assessments based on NIST guidelines as addressed in § 170.17.
- C3PAOs conduct assessments based on NIST guidelines as addressed in § 170.17.
- This is an assessment to validate implementation of the 110 security requirements from NIST SP 800-171 Rev 2.
- Prospective C3PAOs must complete and submit the Standard Form (SF) 328 Certificate Pertaining to Foreign Interests upon request from Defense Counterintelligence and Security Agency (DCSA) (OMB Control Number 0704-0579).
- OSCs may have a POA&M at CMMC Level 2 as addressed in § 170.21(a)(2). C3PAOs must perform a POA&M closeout assessment.
- OSCs may submit appeals to C3PAOs as addressed in §170.9(b)(20).
- 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 s addressed in § 170.8(b)(13).
- 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 and organizations for whom consulting services were provided; and working papers generated from Level 2 Certification Assessments as addressed in § 170.9(b)(10).

- CAICOs maintain records for a period of six (6) years of all procedures, processes, and actions related to fulfillment of the requirements set forth in § 170.10(b)(9).
- 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 (6) years from the date of certification assessment as addressed in § 170.17(c)(4).

The public respondent burden and labor cost for the information collection reporting and recordkeeping requirements under the CMMC Level 2 Certification Assessment are as follows:

NOTE: This respondent burden and labor cost does not include the requirement for the OSC to upload the affirmation in SPRS (addressed in Title 48 acquisition rule and ICR).

Table 38 - Public Respondent Burden and Labor Costs for the CMMC Instantiation of eMASS

Collection Instrument	Entity Type	Number of Responses[62]	Hours per Response	Burden Hours	Hourly Rate	Burden Per Response	Total Burden
	Computations	a	b	c = a * b	d	e = b * d	f = a * e
Level 2 Certification Assessment eMASS Reporting	Accreditation Board	240	0.08	19.2	$84.91	$7	$ 1,630
Level 2 Certification Assessment eMASS Reporting	C3PAOs (Small)	8,098	0.25	2,024.50	$239.89	$ 60	$ 485,657
	C3PAOs (Other Than Small)	2,844	0.25	711.00	$131.44	$ 33	$ 93,454

Table 39 - Public Respondent Burden and Labor Costs for the Other CMMC Program Reporting/Recordkeeping Requirements

Collection and Rule Citation	Entity Type	Number of Responses[63]	Hours per Response	Burden Hours	Hourly Rate	Burden Per Response	Total Burden
	Computations	a	b	c = a * b	d	e = b * d	f = a * e
Level 2 Certification Assessment	C3PAOs (Small) (Reporting and Recordkeeping)	8,098	417.83	3,383,587.34	$239.89	$100,233	$811,688,767

[62] Respondent is equivalent to an entity; an entity provides one response annually.
[63] Respondent is equivalent to an entity; an entity provides one response annually.

§170.17 (a) Reporting and Recordkeeping Requirements							
Level 2 Certification Assessment §170.17 (a) Reporting and Recordkeeping Requirements	C3PAOs (Other Than Small) (Reporting and Recordkeeping)	2,844	833.83	2,371,412.52	$131.44	$109,599	$311,698,462
Level 2 Certification Assessment §170.17 (a) Reporting and Recordkeeping Requirements	Accreditation Body (Recordkeeping)						
Level 2 Certification Assessment §170.17 (a) Reporting and Recordkeeping Requirements	CAICO (Recordkeeping)						

CMMC Level 3 Certification Assessment Collection.

The Level 3 Certification Assessment information collection reporting and recordkeeping requirements are included in this part with the exception of the requirement for the OSC to upload the affirmation in SPRS that will be included in the Title 48 acquisition rule and an update to the 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. The information collection reporting requirements for eMASS include:

- DCMA DIBCAC submits pre-assessment and planning material, final assessment reports, and appropriate CMMC certificates of assessment into the CMMC instantiation of eMASS as addressed in § 170.7 of this part. The DCMA DIBCAC uploads assessment data compliant with the CMMC assessment data standard into the CMMC instantiation of eMASS as addressed in § 170.7(a)(5) of this part.
- DCMA DIBCAC posts POA&M closeout assessment compliance results into the CMMC instantiation of eMASS in accordance with § 170.18(a)(1)(ii)(B) of this part.
- DCMA DIBCAC uploads artifacts (list of artifacts, hash of artifacts, and hashing algorithm used) into the CMMC instantiation of eMASS as addressed in § 170.7(a)(5) of this part.
- DCMA DIBCAC submits assessment appeals, review records, and decision results of assessment appeals using the CMMC instantiation of eMASS as addressed in § § 170.7(a)(2) and (6) of this part.

- Additional information collection reporting and recordkeeping requirements for this part include:

- OSCs prepare for assessment based on NIST guidelines as addressed in § 170.18.
- DCMA DIBCAC conducts assessment based on NIST guidelines as addressed in § 170.18. This is an assessment to validate implementation of 24 selected security requirements from NIST SP 800-172.
- OSCs may have a POA&M at CMMC Level 3 as addressed in § 170.21(a)(3). DCMA DIBCAC must perform a POA&M closeout assessment.
- OSCs may submit appeals to DCMA DIBCAC as addressed in § 170.7(a)(6).
- 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 (6) years from the date of certification assessment as addressed in § 170.18(c)(4).

- 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.

The public and government respondent burden and labor cost for the information collection reporting and recordkeeping requirements under the CMMC Level 3 Certification Assessment are as follows:

NOTE: This respondent burden and labor cost does not include the requirement for the OSC to upload the affirmation in SPRS (addressed in Title 48 acquisition rule and ICR).

Table 40 - Government Burden and Labor Costs for the CMMC Instantiation of eMASS

Collection Instrument	Entity Type	Number of Responses[64]	Hours per Response	Burden Hours	Hourly Rate[65]	Burden Per Response	Total Burden
	Computations	a	b	c = a * b	d	e = b * d	f = a * e
Level 3 Certification Assessment eMASS Reporting	DCMA DIBCAC (Small)	190	0.25	47.50	$108.47	$ 27	$ 5,152
Level 3 Certification Assessment eMASS Reporting	DCMA DIBCAC (Other Than Small)	23	0.25	5.75	$81.01	$ 20	$ 466

Table 41 - Public Respondent Burden And Labor Costs For The Other CMMC Program Reporting/Recordkeeping Requirements

[64] Respondent is equivalent to an entity; an entity provides one response annually.
[65] The hourly rate was calculated from base rates and 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 and other daily work activities such as recordkeeping).

Collection and Rule Citation	Entity Type	Number of Responses [66]	Hours per Response	Burden Hours	Hourly Rate	Burden Per Response	Total Burden
Level 3 Certification Assessment §170.18 (a)	OSC (Small)	190	42.08	7,995.20	$170.48	$ 7,174	$1,363,022
Reporting/ Recordkeeping Requirements	OSC (Other Than Small)	23	384.08	8,833.84	$ 94.53	$36,307	$ 835,063

Table 42 - Government Burden and Labor Costs for the Other CMMC Program Reporting/Recordkeeping Requirements

Collection and Rule Citation	Entity Type	Number of Responses [67]	Process Hours per Response	Total Process Hours	Hourly Rate	Process Cost Per Response	Total Cost to Process Responses
Level 3 Certification Assessment §170.18 (a) Reporting / Recordkeeping Requirements	DCMA DIBCAC (Small)	190	117.75	22,372.50	$ 108.47	$ 12,772	$ 2,426,745
Level 3 Certification Assessment §170.18 (a) Reporting / Recordkeeping Requirements	DCMA DIBCAC (Other Than Small)	23	435.75	10,022.25	$ 81.01	$ 35,300	$ 811,902

Part B: 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

[66] Respondent is equivalent to an entity; an entity provides one response annually.
[67] Each entity has one response annually; the public and the government are the respondents at Level 3.

reflects annually recurring fees and associated labor for technology refresh. The estimated amounts are average annual amounts for the entity types indicated.

Table 43 - Respondent Costs Other Than Burden

Rule Citation	Collection Requirement	Entity Type	Non-Recurring Cost	Recurring Cost	Total Costs
§170.18 (a)	Level 3	Small	$ 513,000,000	$ 93,100,000	$ 606,100,000
§170.18 (a)	Certification	Other Than Small	$ 485,300,000	$ 94,760,000	$ 580,060,000
TOTAL					**$ 1,186,160,000**

Part C: Operational and Maintenance Costs

Government operational and maintenance costs include the estimate to develop the operational CMMC instantiation of eMASS. The estimated average annual amount is $2,731,861.

ESTIMATION OF TOTAL PUBLIC AND GOVERNMENT BURDEN AND COST

Table 44 - Estimation of Total Public and Government Burden:

CMMC Level 2 and Level 3 Certification Assessments

Total Estimated Public Burden Hours	5,774,583.6
Total Estimated Government Burden Hours	32,448
Total Estimated Public & Government Burden Hours	5,807,031.6
Total Estimated Annual Public Labor Cost (Average Over Phase-In Period)	$1,126,166,055
Total Estimated Annual Government Labor Cost	$3,244,266
Estimated Respondent Non-Recurring and Recurring Cost (Average Annual)	$1,186,160,000
Estimated Government Operational and Maintenance Cost (Average Annual)	$2,731,861
Total Estimated Cost	**$2,318,302,182**

Needs and Uses: The CMMC Program provides for the assessment of contractor and subcontractor implementation of DoD cybersecurity requirements for contractor information

systems and enhances the protection of FCI and CUI within the DoD supply chain. The CMMC Program will be implemented in DFARS to incorporate CMMC Program requirements into defense contracts and subcontracts.

Affected Public: Businesses or other for-profit or not-for-profit entities.

Frequency: On occasion.

Commenter's Obligation: Voluntary

OMB Desk Officer: Written comments and recommendations on the proposed information collections should be sent to Ms. Jasmeet Seehra at the Office of Management and Budget, DoD Desk Officer, Room 10102, New Executive Office Building, Washington, DC 20503, with a copy to the Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Mailbox #24 Suite 08D09, Alexandria, VA 22350-1700. Comments can be received from 30 to 60 days after the date of this notice, but comments to OMB will be most useful if received by OMB within 30 days after the date of this notice.

You may also submit comments, identified by docket number **DoD-2023-OS-0063** and title through the Federal eRulemaking Portal at https://www.regulations.gov. Follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name, docket number and title for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

To request more information on these proposed information collections or to obtain a copy of the proposal and associated collection instruments, please write to Department of Defense, Office of the DoD Chief Information Officer, 4800 Mark Center Drive, Suite 11G14,

Alexandria, VA 22350 or contact Ms. Diane Knight at 202–770–9100- or diane.l.knight10.civ@mail.mil.

F. Executive Order 13132, "Federalism"

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. This proposed 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 proposed rule (and subsequent 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 proposed rule will not have a substantial effect on Indian Tribal governments.

List of Subjects in 32 CFR Part 170

CMMC, CMMC Program, CMMC Levels, Cybersecurity, Certification, Federal Contract Information, Controlled Unclassified Information, Contracts, Government procurement, Incorporation by reference.

Accordingly, the Department of Defense proposes to add 32 CFR part 170 to read as follows:

PART 170 - CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Subpart A—General Information.

Sec.

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 policy for requiring defense contractors and subcontractors to implement prescribed cybersecurity standards for safeguarding: Federal Contract Information (FCI), and Controlled Unclassified Information (CUI), as well as conduct an assessment of contractor information systems that process, store, or transmit FCI or CUI; provide security protections for such CUI systems; or are not logically or physically isolated from all such CUI systems, for compliance with the applicable prescribed cybersecurity standard.

(b) The CMMC Program is designed to enhance protection of FCI and CUI when it is processed, stored, or transmitted on defense contractor information systems to meet evolving threats and safeguard the sensitive 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 Federal Acquisition Regulation (FAR) clause 52.204-21; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev 2; and selected requirements from the NIST SP 800-172, as applicable (see table 1 to § 170.14(c)(4) CMMC Level 3 Requirements).

(c) 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.

(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) This part 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.html 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; (301) 975-8443; https://csrc.nist.gov/publications/.

(1) FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, published March 2006; IBR approved for § 170.4(b).

(2) FIPS PUB 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, published January 2022; IBR approved for § 170.4(b).

(3) SP 800-37, revision 2, Risk Management Framework for Information Systems and Organizations, published December 2018; IBR approved for § 170.4(b).

(4) SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, published March 2011; IBR approved for § 170.4(b).

(5) SP 800-53 revision 5, Security and Privacy Controls for Information Systems and Organizations, published September 2020 (includes updates as of Dec. 10, 2020); IBR approved for § 170.4(b).

(6) SP 800-82 revision 2, Guide to Industrial Control Systems (ICS) Security, published June 3, 2015, updated November 10, 2018; IBR approved for § 170.4(b).

(7) SP 800-115, Technical Guide to Information Security Testing and Assessment, published September 2008; IBR approved for § 170.4(b).

(8) SP 800-160, Volume 2, revision 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, published December 2021; IBR approved for §§ 170.4(b).

(9) SP 800-171 revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, published February 2020 (includes updates as of January 28, 2021); IBR approved for §§ 170.4(b); 170.14(a), (b), and (c).

(10) SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, published June 2018; IBR approved for §§ 170.11(a), 170.14(d), 170.15(c), 170.16(c), 170.17(c).

(11) SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171, published February 2021; IBR approved for §§ 170.5(a) and 170.14(a) and (c).

(12) SP 800-172A, Assessing Enhanced Security Requirements for Controlled Unclassified Information, published March 2022; IBR approved for §§ 170.4(b), 170.14(d), and 170.18(c).

(b) The Committee on National Security Systems (CNSS), National Security Agency, Savage Road, Suite 6165, Fort George G. Meade, MD 20755-6716; 410-854-6805; www.cnss.gov/CNSS/issuances/Instructions.cfm.

(1) Committee on National Security Systems Instruction No. 4009, Committee on National Security Systems (CNSS) Glossary, published March 2022; IBR approved for § 170.4(b).

(2) [Reserved].

(c) International Organization for Standardization (ISO) Chemin de Blandonnet 8, CP 401 - 1214 Vernier, Geneva, Switzerland; +41 22 749 01 11; www.iso.org/popular-standards.html.

(1) ISO/IEC 17011:2017, Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies, published 2017; IBR approved for §§ 170.8(b) and 170.98(b).

(2) ISO/IEC 17020:2012, Conformity assessment — Requirements for the operation of various types of bodies performing inspection, published 2012; IBR approved for §§ 170.8(a) and (b) and 170.9(a) and (b).

(3) ISO/IEC 17024:2012, Conformity assessment — General requirements for bodies operating certification of persons, published 2012; IBR approved for §§ 170.8(b) and 170.10(a) and (b).

Note to § 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.

§ 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 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 government 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 Level 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 Level 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 CMMC revision to DFARS 252.204-7021. DoD intends to include CMMC Level 1 Self-Assessment or CMMC Level 2 Self-Assessment for all applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, include CMMC Level 1 Self-Assessment or CMMC Level 2 Self-Assessment 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 CMMC Level 2 Certification Assessment in place of CMMC Level 2 Self-Assessment for applicable DoD solicitations and contracts.

(2) *Phase 2*. Begins six months following the start date of Phase 1. In addition to Phase 1 requirements, DoD intends to include CMMC Level 2 Certification Assessment all for applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, delay the inclusion of CMMC Level 2 Certification Assessment to an option period instead of as a condition of contract award. DoD may also, at its discretion, include CMMC Level 3 Certification Assessment 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 CMMC Level 2 Certification Assessment 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 prior to the effective date. DoD intends to include CMMC Level 3 Certification Assessment for all applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, delay the inclusion of CMMC Level 3 Certification Assessment 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, these acronyms and their terms are for the purposes of this part.

AC	Access Control
APT	Advanced Persistent Threat
APP	Approved Publisher Partner
AT	Awareness and Training
ATP	Approved Training Provider
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
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

MSP	Managed Service Provider
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
PIEE	Procurement Integrated Enterprise Environment
PLC	Programmable Logic Controller
POA&M	Plan of Action and Milestones
PRA	Paperwork Reduction Act
RM	Risk Management
SAM	System for 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
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 201-3 (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 organization 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. The current *Accreditation Body* is doing business as the Cyber AB at cyberab.org. (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, (incorporated by reference, see § 170.2).

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 to § 170.18. (CMMC-custom term)

(i) *Self-Assessment* is the term for the activity performed by an entity to evaluate its own CMMC Level, as applied to Level 1 and some Level 2.

(ii) *CMMC Level 2 Certification Assessment* is the term for the activity performed by a C3PAO to evaluate the CMMC Level of an OSC.

(iii) *CMMC Level 3 Certification Assessment* is the term for the activity performed by the Department of Defense to evaluate the CMMC Level of an OSC.

Assessment Findings Report means the delivery of the final written assessment results by the third-party or government assessment team to the OSC. (CMMC-custom term)

Assessment Team means participants in the CMMC assessment such as the CMMC Certified Assessors and CMMC Certified Professionals, or DCMA DIBCAC assessors. This does not include the OSC participants preparing for or participating in the assessment. (CMMC-custom term)

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 200 (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 (incorporated by reference, see § 170.2).

Cloud Service Provider (CSP) means an external company that provides a platform, infrastructure, applications, and/or storage services for its clients.(Source: CISA Cloud Security Technical Reference Architecture; see https://www.cisa.gov/sites/default/files/publications/CISA%20Cloud%20Security%20Technical%20Reference%20Architecture_Version%201.pdf; page 44.)

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 assessors, instructors, and related practitioners. (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). (CMMC-custom term)

CMMC Level 1 Self-Assessment is defined in § 170.15(c)(1). (CMMC-custom term)

CMMC Level 2 Conditional Certification Assessment is defined in § 170.17(a)(1)(ii). (CMMC-custom term)

CMMC Level 2 Conditional Self-Assessment is defined in § 170.16(a)(1)(ii). (CMMC-custom term)

CMMC Level 2 Final Certification Assessment is defined in § 170.17(a)(1)(iii). (CMMC-custom term)

CMMC Level 2 Final Self-Assessment is defined in § 170.16(a)(1)(iii). (CMMC-custom term)

CMMC Level 3 Conditional Certification Assessment is defined in § 170.18(a)(1)(ii). (CMMC-custom term)

CMMC Level 3 Final Certification Assessment is defined in § 170.18(a)(1)(iii). (CMMC-custom term)

CMMC Third-Party Assessment Organization (C3PAO) means an organization that has been accredited by the Accreditation Body to conduct CMMC 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) CMMC Level 2 Scoping.-(CMMC-custom 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 using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information 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 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: DFARS Clause 252.204-7020, see 48 CFR 252.204-7020).

Defense Industrial Base (DIB) is defined in 32 CFR 236.2.

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. (Source: CNSSI 4009; https://www.cnss.gov/CNSS/issuances/Instructions.cfm.)]

External Service Provider (ESP) means external people, technology, or facilities that an organization utilizes for provision and management of comprehensive 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.

Federal Contract Information (FCI) Assets means assets that process, store, or transmit FCI. FCI Assets are part of the Level 1 CMMC Assessment Scope and are assessed against all CMMC Level 1 requirements. (CMMC-custom term)

Government Furnished Equipment (GFE) has the same meaning as "government-furnished 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 such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. 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 800-82 R2 (incorporated by reference, see § 170.2).

Information System (IS) is defined in NIST SP 800-171 Rev 2 (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 (incorporated by reference, see § 170.2).

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 800-160v2 Rev 1 (incorporated by reference, see § 170.2).

Organization-Defined means as determined by the OSA being assessed except as defined in the case of Organization-Defined Parameter (ODP). (CMMC-custom term)

Organization-Defined Parameter (ODP) 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 (incorporated by reference, see § 170.2).

Note 1 to *ODP*: For CMMC Level 3, the organization defining the parameters is the DoD.

Organization Seeking Assessment (OSA) means the 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 Organizations Seeking Certification (OSCs). (CMMC-custom term)

Organization Seeking Certification (OSC) means the 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. (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 regular intervals. As used in many requirements within CMMC, the interval length is organization-defined to provided OSA flexibility, with an interval length of no more than one year. (CMMC-custom term)

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 (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). (CMMC-custom term)

Risk means a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence, as defined in CNSSI 4009 (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 (incorporated by reference, see § 170.2).

Security Protection Assets means assets providing security functions or capabilities to the OSA's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI. (CMMC-custom 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 800-82 Rev 2 (incorporated by reference, see § 170.2).

System Security Plan (SSP) means the formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact

assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan, as defined in CNSSI 4009 (incorporated by reference, see § 170.2).

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 Rev 5, (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 (incorporated by reference, see § 170.2), implementing DoD specified parameters to meet CMMC Level 3 requirements (see table 1 to § 170.14(c)(4) CMMC Level 3 Requirements). These additional requirements are necessary to protect CUI being processed, stored, or transmitted in contractor information systems, when designated by a CMMC Level 3 requirement as defined by a DoD program manager or requiring activity. In general, the Department will identify a CMMC Level 3 requirement for solicitations supporting its most critical programs and technologies.

(b) Program managers and requiring activities are responsible for identifying the CMMC Level that will apply to a procurement. Selection of the applicable CMMC Level 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) Potential for and 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, a Service Acquisition Executive or Component Acquisition Executive in the DoD may elect to waive inclusion of CMMC Program requirements in a solicitation or contract, and in accordance with all applicable policies, procedures, and requirements. 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 FAR 52.204-21 (48 CFR 52.204-21), Basic Safeguarding of Covered Contractor Information Systems, or covered defense information in accordance with DFARS subpart 204.73 (48 CFR2 04.73), 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 FAR 52.204-21, NIST SP 800-171 Rev 2, and NIST SP 800-172, 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. The CMMC PMO is responsible for the granting and revocation of the validity status of the appropriate CMMC certification level, which officially resides within SPRS based on inputs from the OSA, C3PAO, and or DCMA DIBCAC.

(b) The CMMC PMO is responsible for investigating and acting upon indications that an active CMMC Self-Assessment, described in §§ 170.15 and 170.16, or CMMC Certification Assessment, described in §§ 170.17 and 170.18, 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 require a DCMA DIBCAC assessment of the OSA, as provided for under the DFARS clauses 252.204-7012 and 252.204-7020 (48 CFR 252.204-7012 and 252.204-7020).

(c) If the investigative results show that adherence to the provisions of this rule have not been achieved or maintained, the CMMC PMO may revoke the validity status of the appropriate existing CMMC Self-Assessment(s) or CMMC Final Certification Assessment(s).

§ 170.7 DCMA DIBCAC.

(a) In support of the CMMC Program, DoD intends that the DCMA DIBCAC assessors performing Level 3 assessments will:

(1) Complete CMMC Level 2 and Level 3 training.

(2) Conduct CMMC Level 3 Certification Assessments and upload assessment results into the CMMC instantiation of eMASS.

(3) Issue CMMC Level 3 Certification Assessment certificates.

(4) Conduct CMMC Level 2 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 values 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 CMMC Level 3 Certification Assessment activities into the CMMC instantiation of eMASS.

(7) Retain all records in accordance with DCMA-MAN 4501-04.

(b) [Reserved].

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 (incorporated by reference, see § 170.2) and all applicable authorization and accreditation requirements set forth. At any given point in time, there will be only one Accreditation Body for the DoD CMMC Program.

(b) *Requirements*. The Accreditation Body shall:

(1) Become 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.

(2) Become 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 (incorporated by reference, see § 170.2).

(3) Achieve and maintain full compliance with ISO/IEC 17011:2017 (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, both within 24

months of DoD approval. If ISO/IEC 17011:2017 is revised or superseded, the Accreditation Body shall achieve full compliance with the updated standard within 12 months of the date of revision.

(i) Prior to achieving full compliance as set forth in this paragraph (b)(3), the Accreditation Body shall:

(A) Authorize, but not accredit, C3PAOs who meet all requirements set forth in § 170.9 to grant CMMC Level 2 Certification Assessments and issue certificates of assessment for OSCs.

(B) Require all C3PAOs to achieve and maintain the ISO/IEC 17020:2012 requirements within 27 months of authorization. If ISO/IEC 17020:2012 is revised or superseded, the Accreditation Body shall require full compliance with the updated standard within 12 months of the date of revision.

(ii) After achieving full compliance as set forth in this paragraph (b)(3), the Accreditation Body shall accredit C3PAOs, in accordance with ISO/IEC 17020:2012, or subsequent revisions, who meet all requirements set forth in § 170.9 to grant CMMC Level 2 Certification Assessments and issue certificates of assessment for OSCs.

(4) Ensure that the Accreditation Body's Board of Directors, professional staff, Information Technology (IT) staff, accreditation staff, and independent 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 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 title 5 CFR 1400.201(b) and (d) and the investigative requirements of title 5 CFR 731.106(c)(2).

(5) Comply with Foreign Ownership, Control or Influence (FOCI) by:

(i) Completing the Standard Form (SF) 328 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.

(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 CMMC 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 Level 2 Final Certification Assessment and will not result in a CMMC Level 2 certificate. The CMMC Level 2 assessment process must be performed on a triennial basis.

(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. If ISO/IEC 17024:2012 is revised or superseded, the Accreditation Body shall require full compliance with the updated standard within 12 months of the date of revision.

(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) 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, or subsequent revisions, 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 CMMC assessments, CMMC instruction, CMMC training

materials, or CMMC certification 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, or subsequent revisions.

(B) Require members of the Accreditation Body 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 members of the Accreditation Body who leave the board or organization to enter a "cooling off period" of six (6) months whereby they are prohibited from working with the Accreditation Body or participating in CMMC activities.

(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 as 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 certification 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 CMMC assessment process for a CMMC assessment in which they previously served as a consultant to prepare the organization for any CMMC assessment.

(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 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 granting CMMC Level 2 Certification Assessments and issuing certificates of assessment for OSCs. 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).

(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 (incorporated by reference, see § 170.2) within 27 months of authorization. If ISO/IEC 17020:2012 is revised or superseded, the C3PAO shall achieve full compliance with the updated standard within 12 months of the date of revision.

(3) Require all C3PAO company personnel participating in the CMMC 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. These positions are designated as non-critical sensitive with a risk designation of "Moderate Risk" in accordance with title 5 CFR 1400.201(b) and (d) and the investigative requirements of title 5 CFR 731.106(c)(2).

(4) Require all C3PAO company personnel participating in the CMMC 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 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) Obtain a CMMC 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 Level 2 Final Certification Assessment and will not result in a CMMC Level 2 certificate. The CMMC Level 2 assessment process must be performed on a triennial basis.

(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) Submit all assessment appeal investigations and decisions to include assessment results into the CMMC instantiation of eMASS.

(10) 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 provided by OSC, 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 inspection activities; contractual agreements with OSCs; and organizations for whom consulting services were provided.

(11) Provide any requested audit information, including any out-of-cycle from ISO/IEC 17020:2012 requirements, or subsequent revisions, to the Accreditation Body.

(12) Ensure that all personal information is encrypted and protected in all C3PAO information systems and databases.

(13) Meet the requirements for Assessment Team composition, comprised of a Lead CCA, CCAs, and any participating CCPs.

(14) 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)(15) of this section and the appeals process as required by paragraph (b)(21) of this section and in accordance with ISO/IEC 17020:2012 and ISO/IEC 17011:2017, or subsequent revisions.

(15) Conduct quality assurance reviews for each assessment, including observations of the Assessment Team's conduct and management of CMMC assessment processes.

(16) Ensure that all CMMC assessment activities are performed on the information system within the CMMC Assessment Scope.

(17) Maintain all facilities, personnel, and equipment involved in CMMC activities that are in scope of their CMMC Level 2 assessment and comply with all security requirements and procedures as prescribed by the Accreditation Body.

(18) Upload into the CMMC instantiation of eMASS assessment data 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[1].

(19) Issue certificates of assessment to OSCs in accordance with the certification requirements set forth in § 170.17.

(20) Address all OSC appeals arising from CMMC Level 2 assessment activities. Any appeal not resolved by the C3PAO will elevate to the Accreditation Body for final determination.

(21) 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 (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 full compliance with ISO/IEC 17024:2012 within 25 months of registration. If ISO/IEC 17024:2012

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

is revised or superseded, the CAICO shall achieve full compliance with the updated standard within 12 months of the date of revision.

(2) Provide all documentation and records in English.

(3) Train, test, certify, and recertify CCAs, CCIs, and CCPs in accordance with the requirements of this section.

(4) The CAICO's certification examinations must be certified under ISO/IEC 17024:2012, or subsequent revisions, by a recognized U.S- based accreditor who is not a member of the CMMC Accreditation Body and complies with ISO/IEC 17011:2017, or subsequent revisions.

(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, or subsequent revisions.

(8) Address all appeals arising from the CMMC assessor, instructor, and practitioner authorizations and certifications process through use of internal processes in accordance with ISO/IEC 17024:2012, or subsequent revisions.

(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 subcontractor, 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 personal information is encrypted and protected in all CAICO and CAICO subcontractor, as applicable, information systems and databases.

(14) Ensure the security of assessor and instructor examinations and the fair and credible administration of examinations.

(15) Neither disclose nor allow any subcontractor, 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 recertification of CCAs, CCIs, and CCPs upon significant change to DoD's CMMC Program requirements under this rule.

§ 170.11 CMMC Certified Assessor (CCA).

(a) *Roles and responsibilities*. CCAs, in support of a C3PAO, conduct CMMC Level 2 Certification Assessments of OSCs in accordance with NIST SP 800-171A (incorporated by reference, see § 170.2), the assessment processes defined in § 170.17, and the scoping requirements defined in § 170.19. CCAs are certified by the CAICO after successful completion of the CCA training and testing requirements set forth in paragraph (b) of this section. A CCA may conduct CMMC 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. These positions are designated as non-critical sensitive with a risk designation of "Moderate Risk" in accordance with title 5 CFR 1400.201(b) and (d) and the investigative requirements of title 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, 1 year of assessment or audit experience, and at least one baseline certification aligned to either paragraph (b)(6)(i) or (ii) of this section through 15 February 2025 and aligned to paragraph (b)(6)(ii) of this section only beginning 16 February 2025.

(i) IAT Level II from DoD Manual 8570 Information Assurance Workforce Improvement Program.

(ii) Intermediate Proficiency Level for Career Pathway Certified Assessor 612 from DoD Manual 8140.03 Cyberspace Workforce Qualification & Management Program.

(7) 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 baseline certification aligned to either paragraph (b)(7)(i) or (ii) of this section through 15 February 2025 and aligned to paragraph (b)(7)(ii) of this section only beginning 16 February 2025.

(i) IAM Level II from DoD Manual 8570 Information Assurance Workforce Improvement Program.

(ii) Advanced Proficiency Level for Career Pathway Certified Assessor 612 from DoD Manual 8140.03 Cyberspace Workforce Qualification & Management Program.

(8) Only use IT, cloud, cybersecurity services, and end-point devices provided by the authorized/accredited C3PAO that they support and has received a CMMC Level 2 Certification Assessment 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 store, process, handle, or transmit CMMC assessment reports or any other CMMC assessment-related information.

(9) Immediately notify the responsible C3PAO of any breach or potential breach of security to any CMMC-related assessment materials under the assessors' purview.

(10) Not share any CMMC assessment-related outcomes or advance information with any person not assigned to that specific assessment, except as otherwise required by law.

§ 170.12 CMMC Certified Instructor (CCI).

(a) *Roles and responsibilities*. A CMMC Certified Instructor (CCI) teaches CMMC assessor candidates. A CCI is trained, tested, and certified to perform CMMC instructional duties by the CAICO to teach CMMC assessor candidates. Candidate CCIs are certified by the CAICO after successful completion of the CCI training and testing requirements set forth in paragraph (b) of this section.

(b) *Requirements*. CCIs 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) Provide all documentation and records in English.

(4) Provide the Accreditation Body and the CAICO with the most up-to-date and accurate information detailing their qualifications, training experience, professional affiliations, and certifications, and, upon reasonable request, submit documentation verifying this information.

(5) Not provide CMMC consulting services while serving as a CMMC instructor.

(6) 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.

(7) Keep confidential all information obtained or created during the performance of CMMC training activities, including trainee records, except as required by law.

(8) Not disclose any CMMC-related data or metrics to anyone without prior coordination with and approval from DoD.

(9) Notify the Accreditation Body or the CAICO if required by law or authorized by contractual commitments to release confidential information.

(10) 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 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 CMMC 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. These positions are designated as non-critical sensitive with a risk designation of "Moderate Risk" in accordance with title 5 CFR 1400.201(b) and (d) and the investigative requirements of title 5 CFR 731.106(c)(2).

(4) Require all CCPs, 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) Provide all documentation and records in English.

(6) Not share any CMMC assessment-related outcomes or advance information with any person not assigned to 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) FAR 52.204-21 (48 CFR 52.204-21) *Basic Safeguarding of Covered Contractor Information Systems*;

(2) NIST SP 800-171 Rev 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (incorporated by reference, see § 170.2); and

(3) Selected requirements from NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 Rev 2*, (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 Rev 2.

(c) *CMMC level requirements*. CMMC Levels 1-3 utilize the safeguarding requirements and security requirements specified in FAR clause 52.204-21 (Level 1), NIST SP 800-171 Rev 2 (Level 2), and selected security requirements from NIST SP 800-172 (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 FAR clause 52.204-21 paragraph number, NIST SP 800-171 Rev 2, or NIST SP 800-172 requirement number.

(2) *CMMC Level 1 requirements*. The security requirements in CMMC Level 1 are those set forth in FAR clause 52.204-21(b)(1)(i) through (b)(1)(xv).

(3) *CMMC Level 2 requirements*. The security requirements in CMMC Level 2 are identical to the requirements in NIST SP 800-171 Rev 2.

(4) *CMMC Level 3 requirements*. The security requirements in CMMC Level 3 are selected from NIST SP 800-172, 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 requirements are italicized, where applicable:

Table 1 to § 170.14(c)(4)

Security Requirement Number[1]	**CMMC Level 3 Security Requirements (Selected NIST SP 800-172 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 up-to-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 purpose-specific 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 DoD-provided sources*, to guide and inform intrusion detection and threat hunting.

[1] 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 (incorporated by reference, see § 170.2) and NIST SP 800-172A (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 an Organization-Defined Parameter (ODP), organization-defined means as determined by the OSA being assessed. 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) *CMMC Level 1 Self-Assessment*. To comply with CMMC Level 1 requirements, the OSA must meet the requirements detailed in paragraphs (a)(1) and (2) of this section.

(1) *Self-Assessment*. The OSA must complete and achieve a MET result for all security requirements specified in § 170.14(c)(2). No POA&Ms are permitted for CMMC Level 1. 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 SPRS. To maintain compliance with CMMC Level 1 Self-Assessment requirements, the OSA must conduct a self-assessment of CMMC Level 1 on an annual basis and submit the results in SPRS.

(i) *SPRS inputs*. The self-assessment results in the Supplier Performance Risk System (SPRS) shall include, at minimum, the following items:

(A) CMMC Level.

(B) Assessment Date

(C) Assessment Scope.

(D) All industry CAGE code(s) associated with the information system(s) addressed by the CMMC Assessment Scope

(E) Compliance result.

(ii) *CMMC status revocation*. If the CMMC PMO determines that the provisions of Level 1 of this rule have not been achieved or maintained, as addressed in § 170.6, a revocation of the validity status of the CMMC Level 1 Self-Assessment may occur. At that time, standard contractual remedies will apply and the OSA will be ineligible for additional awards with CMMC Level 1 Self-Assessment or higher requirements for the information system within the CMMC Assessment Scope until such time as a valid CMMC Level 1 Self-Assessment is achieved.

(2) *Affirmation*. Affirmations are required for all CMMC 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 CMMC Level 1 requirement, OSAs must comply with all CMMC Level 1 Self-Assessment requirements and have submitted an affirmation of compliance into SPRS for all information systems within the CMMC Assessment Scope.

(c) *Procedures*.– (1) *Self-Assessment*. The OSA must perform a CMMC Level 1 Self-Assessment 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) *NIST SP 800-171A*. The CMMC Level 1 Self-Assessment must be performed using the objectives defined in NIST SP 800-171A (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 objectives.

Table 1 to § 170.15(c)(1)(i*i*)—CMMC Level 1 Security Requirements to NIST SP 800-171A

CMMC Level 1 Security Requirements as set forth in § 170.14(c)(2)	NIST SP 800-171A
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 FAR 52.204-21 requirements were broken apart by "phrase" when NIST SP 800-171 Rev 2 was developed.	

(iii) Additional explanatory material can be found in the CMMC Level 1 Assessment Guide located at https://DoDcio.defense.gov/CMMC/.

(2) [Reserved].

§ 170.16 CMMC Level 2 Self-Assessment and Affirmation requirements.

(a) *Level 2 Self-Assessment*. To comply with CMMC Level 2 Self-Assessment requirements, the OSA must meet the requirements detailed in paragraphs (a)(1) and (2) of this section. Meeting the CMMC Level 2 Self-Assessment requirements detailed in paragraphs (a)(1) and (2) of this section also satisfies the CMMC Level 1 Self-Assessment requirements detailed in § 170.15 for the same CMMC Assessment Scope.

(1) *Self-Assessment*. The OSA must complete and achieve a MET result for all security requirements specified in § 170.14(c)(3). 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 SPRS. To maintain compliance with CMMC Level 2 Self-Assessment requirements, the OSA must perform a CMMC Level 2 Self-Assessment on a triennial basis and submit the results in SPRS.

(i) *SPRS inputs*. The self-assessment results in the Supplier Performance Risk System (SPRS) shall include, at minimum, the following information:

(A) CMMC Level.

(B) Assessment Date.

(C) Assessment Scope.

(D) All industry CAGE code(s) associated with the information system(s) addressed by the CMMC Assessment Scope.

(E) Overall self-assessment score (e.g., 105 out of 110).

(F) POA&M usage and compliance status, as applicable.

(ii) *Conditional self-assessment*. OSAs have achieved CMMC Level 2 Conditional Self-Assessment 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 implement all CMMC Level 2 security requirements and close out the POA&M within 180 days of the initial self-assessment. Upon remediation of the remaining requirements, the OSA must perform a POA&M closeout self-assessment and post compliance results to SPRS. If the POA&M is not closed out within the 180-day timeframe, the Conditional Level 2 Self-Assessment status of the OSA will expire. If Conditional Level 2 Self-Assessment expires within the period of performance of a contract, standard contractual remedies will apply, and the OSA will be ineligible for additional awards with CMMC Level 2 Self-Assessment or higher requirements for the information system within the CMMC Assessment Scope.

(iii) *Final Self-Assessment*. The OSA will achieve CMMC Level 2 Final Self-Assessment compliance for the information system(s) within the CMMC Assessment Scope upon implementation of all security requirements and close out of the POA&M, as applicable.

(iv) *CMMC status revocation*. If the CMMC PMO determines that the provisions of Level 1 or Level 2 of this rule have not been achieved or maintained, as addressed in § 170.6, a revocation of the validity status of the CMMC Level 2 Self-Assessment may occur. At that time, standard contractual remedies will apply and the OSA will be ineligible for additional awards with CMMC Level 2 Self-Assessment or higher requirements for the information system within the CMMC Assessment Scope until such time as a valid CMMC Level 2 Self-Assessment is achieved.

(2) *Affirmation*. Affirmations are required at the time of each assessment, and annually thereafter, for all CMMC Level 2 Self-Assessments. Affirmation procedures are provided in § 170.22.

(b) *Contract eligibility*. In order to be awarded a contract from DoD with a CMMC Level 2 Self-Assessment requirement, the following two requirements must be met:

(1) OSAs must achieve, as specified in paragraph (a)(1) of this section, either CMMC Level 2 Conditional Self-Assessment or CMMC Level 2 Final Self-Assessment.

(2) OSAs must submit an affirmation of compliance into SPRS, as specified in § 170.16(a)(2).

(c) *Procedures*. – (1) *Self-Assessment*. The OSA must perform a CMMC Level 2 Self-Assessment in accordance with NIST SP 800-171A (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 assessment must be scored in accordance with the CMMC Scoring Methodology described in § 170.24. If a POA&M exists, a POA&M closeout assessment must be performed by the OSA when all remaining requirements have been remediated. The POA&M closeout assessment must be performed within the 180-day closeout period. Additional guidance can be found in the guidance document listed in paragraph (c) of appendix A to this part.

(2) *Self-Assessment of Cloud Service Provider*. An OSA may use a Federal Risk and Authorization Management Program (FedRAMP) Moderate (or higher) cloud environment to process, store, or transmit CUI in execution of a contract or subcontract with a requirement for CMMC Level 2 under the following circumstances:

(i) The Cloud Service Provider's (CSP) product or service offering is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or

(ii) The Cloud Service Provider's (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. Equivalency is met if the OSA has the CSP's System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 Rev 2 requirements. (See

https://www.fedramp.gov/assets/resources/documents/FedRAMP_Moderate_Security_Controls.xlsx.)

(iii) In accordance with § 170.19, 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 CRM must be documented or referred to in the OSA's System Security Plan (SSP).

§ 170.17 CMMC Level 2 Certification Assessment and Affirmation requirements.

(a) *Level 2 Certification Assessment requirements*. To comply with CMMC Level 2 Certification Assessment requirements, the OSC must meet the requirements set forth in paragraphs (a)(1) and (2) of this section. Meeting the CMMC Level 2 Certification Assessment requirements detailed in paragraphs (a)(1) and (2) of this section also satisfies the CMMC Level 2 Self-Assessment requirements set forth in § 170.16 for the same CMMC Assessment Scope.

(1) *Level 2 Certification Assessment*. The OSC must complete and achieve a MET result for all security requirements specified in table 1 to § 170.14(c)(4) CMMC Level 3 Requirements. After implementing the CMMC Level 2 security requirements, the OSC must achieve either CMMC Level 2 Conditional Certification or Final Certification through obtaining a CMMC Level 2 Certification Assessment by an authorized or accredited C3PAO following the procedures outlined in paragraph (c) of this section. Assessment results will be submitted into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS. The CMMC Level 2 Certification Assessment process must be performed on a triennial basis.

(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 and unique identifier.

(C) For each Assessor conducting the assessment, name and business contact information.

(D) All industry CAGE codes associated with the information systems addressed by the CMMC Assessment Scope.

(E) The name, date, and version of the SSP.

(F) Title 32 program rule (32 CFR part 170) at time of assessment

(G) Certification date.

(H) Assessment result for each requirement objective.

(I) POA&M usage and compliance, as applicable.

(J) List of the artifact names, the return values of the hashing algorithm, and the hashing algorithm used.

(ii) *Conditional Certification Assessment*. The OSC has achieved CMMC Level 2 Conditional Certification Assessment if a POA&M exists upon completion of the assessment 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 implement all CMMC Level 2 security requirements and close out their POA&M within 180 days of the initial assessment. Upon remediation of the remaining requirements, the OSC must obtain a POA&M closeout assessment performed by a C3PAO. Results will be submitted by the C3PAO into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS. If the POA&M is not closed out within the 180-day timeframe, the Conditional Level 2 Certification status will expire. If Conditional Level 2 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 Certification Assessment or higher requirements for the information systems within the CMMC Assessment Scope.

(iii) *Final Certification Assessment*. The OSC will achieve CMMC Level 2 Final Certification Assessment for the information systems within the CMMC Assessment Scope upon implementation of all security requirements and close out of the POA&M, as applicable.

(iv) *CMMC status revocation*. If the CMMC PMO determines that the provisions of Level 1 or Level 2 of this rule have not been achieved or maintained, as addressed in § 170.6, a revocation of the validity status of the CMMC Level 2 Final Certification Assessment may occur. At that time, standard contractual remedies will apply and the OSC will be ineligible for additional awards with CMMC Level 2 Certification Assessment or higher requirements for the information system within the CMMC Assessment Scope until such time as a valid CMMC Level 2 Certification Assessment is achieved. The revocation of a CMMC Level 2 Final Certification Assessment will automatically cause the revocation of any CMMC Level 3 Certification Assessments that were dependent upon that CMMC Level 2 Final Certification Assessment.

(2) *Affirmation*. Affirmations are required upon completion of each assessment, and annually thereafter, for all CMMC Level 2 Certification Assessments. Affirmation procedures are provided in § 170.22.

(b) *Contract eligibility*. In order to be awarded a contract from DoD with a CMMC Level 2 Certification Assessment requirement, the following two requirements must be met:

(1) OSCs must achieve, as specified in paragraph (a)(1) of this section, either CMMC Level 2 Conditional Certification Assessment or CMMC Level 2 Final Certification Assessment.

(2) OSCs must submit an affirmation of compliance into SPRS, as specified in paragraph (a)(2) of this section.

(c) *Procedures* – (1) *Assessment*. An authorized or accredited C3PAO must perform an assessment in accordance with NIST SP 800-171A (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 assessment must be scored in accordance

with the CMMC Scoring Methodology described in § 170.24 and final results are subsequently 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 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 assessment must be performed by a C3PAO when all remaining security requirements have been remediated. The POA&M closeout assessment must be performed within the 180-day closeout period to achieve the assessment requirement for a Final Certification. 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 artifacts used as evidence for the assessment must be retained by the OSC for the duration of the validity period of the certificate of assessment, and at minimum, for six (6) years from the date of certification assessment. To ensure that the artifacts have not been altered, the OSC must hash the artifact files using a NIST-approved hashing algorithm. The OSC must provide the C3PAO with a list of the artifact names, the return values 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) *Assessment of Cloud Service Provider*. An OSC may use a Federal Risk and Authorization Management Program (FedRAMP) Moderate (or higher) cloud environment to

process, store, or transmit CUI in execution of a contract or subcontract with a requirement for CMMC Level 2 under the following circumstances:

(i) The Cloud Service Provider's (CSP) product or service offering is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or

(ii) The Cloud Service Provider's (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. Equivalency is met if the OSA has the CSP's System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 Rev 2 requirements. (See https://www.fedramp.gov/assets/resources/documents/FedRAMP_Moderate_Security_Controls.xlsx.)

(iii) In accordance with § 170.19, 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.

§ 170.18 CMMC Level 3 Certification Assessment and Affirmation requirements.

(a) *Level 3 Certification Assessment requirements*. To comply with CMMC Level 3 Certification Assessment requirements, the OSC must meet the requirements set forth in paragraphs (a)(1) and (2) of this section. Receipt of a CMMC Level 2 Final Certification Assessment for information systems within the Level 3 CMMC Assessment Scope is a prerequisite for a CMMC Level 3 Certification Assessment.

(1) *Level 3 Certification Assessment*. The OSC must achieve a CMMC Level 2 Final Certification Assessment on the Level 3 CMMC Assessment Scope, as defined in § 170.19(c) and complete and implement all Level 3 security requirements specified in table 1 to § 170.14(c)(4) CMMC Level 3 Requirements prior to initiating a CMMC Level 3 Certification Assessment, which will be performed by DCMA DIBCAC[1] on behalf of the DoD. To achieve and maintain CMMC Level 3 Certification Assessment, OSCs must achieve both a CMMC Level 2 Final Certification Assessment in accordance with § 170.17 and a CMMC Level 3 Final Certification Assessment in accordance with this section on a triennial basis for all information systems within the Level 3 CMMC Assessment Scope. DCMA DIBCAC will submit the assessment results into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS.

(i) *Inputs into the CMMC instantiation of eMASS*. The 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 business contact 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) Certification date.

(F) Result for each security requirement objective.

(G) POA&M usage and compliance, as applicable.

(H) List of the artifact names, the return values of the hashing algorithm, and the hashing algorithm used.

---

[1] https://www.dcma.mil/DIBCAC

(ii) *Conditional Certification Assessment*. The OSC has achieved CMMC Level 3 Conditional Certification Assessment if a POA&M exists upon completion of the assessment 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 implement all CMMC Level 3 security requirements and close out the POA&M within 180 days of the initial assessment. Upon remediation of the remaining security requirements, the OSC must arrange to have DCMA DIBCAC perform a POA&M closeout assessment. Results will be submitted into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS. If the POA&M is not closed out within the 180-day timeframe, the Conditional Level 3 Certification status will expire. If Level 3 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 3 Certification Assessment requirements for the information systems within the CMMC Assessment Scope.

(iii) *Final Certification Assessment*. The OSC will achieve CMMC Level 3 Final Certification Assessment for the information systems within the CMMC Assessment Scope upon implementation of all security requirements and close out of any POA&M, as applicable.

(iv) *CMMC status revocation*. If the CMMC PMO determines that the provisions of this rule have not been achieved or maintained, as addressed in § 170.6, a revocation of the validity status of the CMMC Level 3 Final Certification Assessment may occur. At that time, standard contractual remedies will apply and the OSC will be ineligible for additional awards with CMMC Level 3 Certification Assessment or higher requirements for the information system within the CMMC Assessment Scope until such time as a valid CMMC Level 3 Certification Assessment is achieved. The revocation of a CMMC Level 2 Final Certification Assessment

will automatically cause the revocation of any CMMC Level 3 Certification Assessments that were dependent upon that CMMC Level 2 Final Certification Assessment.

(2) *Affirmation*. Affirmations are required upon completion of each assessment, and annually thereafter, for all CMMC Level 3 Certification Assessments. Affirmation procedures are provided in § 170.22.

(b) *Contract eligibility*. In order to be awarded a contract from DoD with a CMMC Level 3 Certification Assessment requirement, the following two requirements must be met:

(1) OSCs must achieve, as specified in paragraph (a)(1) of this section, either CMMC Level 3 Conditional Certification Assessment or CMMC Level 3 Final Certification Assessment.

(2) OSCs must submit an affirmation of compliance into SPRS, as specified in paragraph (a)(2) of this section.

(c) *Procedures* – (1) *Assessment*. The CMMC Level 3 Certification Assessment process includes:

(i) *CMMC Level 2 Final Certification Assessment*. CMMC Level 2 Final Certification Assessment must be obtained for information systems within the Level 3 CMMC Assessment Scope prior to assessment against the CMMC Level 3 security requirements of NIST SP 800-172A (incorporated by reference, see § 170.2). The OSC must have a CMMC Level 2 Final Certification Assessment for the same scope as the Level 3 assessment. Asset requirements differ for each CMMC Level. Scoping differences are set forth in § 170.19(e).

(ii) *CMMC Level 3 Certification Assessment*. DCMA DIBCAC will perform an assessment of the CMMC Level 3 security requirements in accordance with NIST SP 800-172A for information systems within the Level 3 CMMC Assessment Scope, determined in accordance with § 170.19(d). The assessment will be scored in accordance with the CMMC Scoring Methodology set forth in § 170.24 and final results are subsequently communicated to the OSC through a CMMC Assessment Findings Report. In the execution of the CMMC Level 3 Certification Assessment, DCMA DIBCAC may perform checks of CMMC Level 2 security

requirements in accordance with CMMC Level 3 scoping. If DCMA DIBCAC identifies that a Level 2 security requirement is NOT MET, the Level 3 assessment process may be placed on hold or terminated.

(2) *Security requirement re-evaluation*. A security requirement under assessment that is NOT MET may be re-evaluated during the course of the 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 after the initial assessment, a POA&M closeout assessment will be performed by DCMA DIBCAC when all remaining security requirements have been implemented. The POA&M closeout assessment must be performed within the 180-day closeout period to achieve the assessment requirement for Final Certification. Additional guidance is located in § 170.21 and in the guidance document listed in paragraph (a) of appendix A to this part.

(4) *Artifact retention and integrity*. The OSC shall retain the hashed artifacts used as evidence during the assessment process. The OSC shall retain the unedited artifacts for the duration of the validity period of the certificate of assessment, and at a minimum, for six (6) years from the date of certification assessment. 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 values 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) *Assessment of Cloud Service Provider*. An OSC may use a Federal Risk and Authorization Management Program (FedRAMP) Moderate (or higher) cloud environment to process, store, or transmit CUI in execution of a contract or subcontract with a requirement for CMMC Level 3 under the following circumstances:

(i) The Cloud Service Provider's (CSP) product or service offering is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or

(ii) The Cloud Service Provider's (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. Equivalency is met if the OSC has the CSP's System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 Rev 2 requirements. (See https://www.fedramp.gov/assets/resources/documents/FedRAMP_Moderate_Security_Controls.xlsx.)

(iii) In accordance with § 170.19, 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.

§ 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 CMMC Level 1 Self-Assessment, the OSA must specify the CMMC Assessment Scope.

(1) *Assets in scope for CMMC 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 CMMC Level 1 Self-Assessment.*–(i) *Out of Scope Assets*. OSA information systems which do not process, store, or transmit FCI are outside the scope of the CMMC Level 1 Self-Assessment. There are no documentation requirements for these 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) *CMMC Level 1 Self-Assessment scoping considerations.* To scope a CMMC 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 CMMC 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 1 to this paragraph. Additional information is available in the guidance document listed in paragraph (f) of appendix A to this part.

Table 1 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 in the System Security Plan (SSP) ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Assess against CMMC security requirements
Security Protection Assets	○ Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI	○ Document in the asset inventory ○ Document in SSP ○ Document in the network diagram of the CMMC Assessment Scope	○ Assess against CMMC security requirements

		○ Prepare to be assessed against CMMC security requirements	
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 in the SSP ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Review the SSP: i. If sufficiently documented, do not assess against other CMMC security requirements, except as noted ii. 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 iii. The limited check(s) shall not materially increase the assessment duration nor the assessment cost

			iv. 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 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	○ Prepare to justify the inability of an Out-of-	○ None

	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	Scope Asset to store, process, or transmit CUI	

(2) If the OSA utilizes an External Service Provider (ESP), other than a Cloud Service Provider (CSP), the ESP must have a CMMC Level 2 Final Certification Assessment. If the ESP is internal to the OSA, the security requirements implemented by the ESP should be listed in the OSA's SSP to show connection to its in-scope environment. 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. If using a CSP for Level 2 Self-Assessment, see § 170.16(c)(2). If using a CSP for Level 2 Certification Assessment, see § 170.17(c)(5).

(d) *CMMC Level 3 scoping*. Prior to performing a Level 3 CMMC 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 2 to this paragraph. Additional information is available in the guidance document listed in paragraph (g) of appendix A to this part.

Table 2 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 2 to paragraph (c)(1) of this section CMMC Scoping)	○ Document in the asset inventory ○ Document in the System Security Plan (SSP) ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Assess against all CMMC security requirements
Security Protection 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 in the System Security Plan (SSP) ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Assess against all 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 in the System Security Plan (SSP) ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Assess against all 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**			
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	○ Prepare to justify the inability of an Out-of-Scope Asset to store, process, or transmit CUI	○ None

(2) If the organization seeking CMMC Level 3 Certification Assessment utilizes an ESP, other than a CSP, the ESP must also have a CMMC Level 3 Final Certification Assessment. If the ESP is internal to the OSC, the security requirements implemented by the ESP should be listed in the OSC's SSP to show connection to its in-scope environment. If using a CSP, see § 170.18(c)(5). 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.

(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 CMMC Level 3 Certification Assessment. DCMA DIBCAC may check any

Level 2 security requirement of any in-scope asset, and if they determine a requirement is NOT MET, DCMA DIBCAC may allow for remediation or may immediately terminate the Level 3 Assessment. For further information or to contact DCMA DIBCAC regarding CMMC, please refer to https://www.dcma.mil/DIBCAC/ or email dcma_dibcac_cmmc@mail.mil.

§ 170.20 Standards acceptance.

(a) *NIST SP 800-171 Rev 2 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 eligible for CMMC Level 2 Final Certification Assessment 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, is eligible for a CMMC Level 2 Final Certification Assessment with a validity period of three (3) years from the date of the original DCMA DIBCAC High Assessment. Eligible DCMA DIBCAC High Assessments include ones conducted with Joint Surveillance in accordance with the DCMA Manual 2302-01 Surveillance. The scope of the CMMC Level 2 Final Certification Assessment is identical to the scope of the DCMA DIBCAC High Assessment. In accordance with § 170.17, 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*. An OSA shall maintain a POA&M, as applicable, as part of operations under the security requirement for Risk Assessments and Continuous Monitoring (CA.L2-3.12.2) for CMMC Levels 2 and 3 in accordance with § 170.14(c)(3) and (4), respectively. For purposes of conducting a CMMC assessment and satisfying the contractual eligibility requirements for

CMMC Level 1, 2, or 3, 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) *CMMC Level 1 Self-Assessment*. A POA&M is not permitted at any time for CMMC Level 1 Self-Assessments

(2) *CMMC Level 2 Self-Assessment and CMMC Level 2 Certification Assessment*. An OSA is only permitted to have a POA&M for CMMC Level 2 if all the following conditions are met:

(i) The assessment score divided by the total number of 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 it has a value of 1 or 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) PE.L2-3.10.3 Escort Visitors (CUI Data).

(D) PE.L2-3.10.4 Physical Access Logs (CUI Data).

(E) PE.L2-3.10.5 Manage Physical Access (CUI Data).

(3) *CMMC Level 3 Certification Assessment*. An OSC is only permitted to have a POA&M for CMMC Level 3 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*. The closing of a POA&M must be confirmed by a POA&M Closeout assessment within 180-days of the initial 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.

(1) *CMMC Level 2 Self-Assessment*. For a CMMC Level 2 Self-Assessment, the POA&M Closeout assessment shall be performed by the OSA in the same manner as the initial self-assessment.

(2) *CMMC Level 2 Certification Assessment*. For CMMC Level 2 Certification Assessment, the POA&M Closeout assessment must be performed by an authorized or accredited C3PAO.

(3) *CMMC Level 3 Certification Assessment*. For CMMC Level 3 Certification Assessment, DCMA DIBCAC will perform the POA&M Closeout Assessment of the CMMC Level 3 security requirements.

§ 170.22 Affirmation.

(a) *General*. The OSA must affirm continuing compliance with the appropriate level CMMC Self-Assessment or CMMC Certification Assessment. The affirmation shall be submitted in accordance with the following requirements:

(1) *Affirming official*. All CMMC affirmations shall be submitted by the OSA senior official who is responsible for ensuring OSA compliance with CMMC Program requirements.

(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 for all information systems within the relevant CMMC Assessment Scope at the applicable CMMC Level.

(3) *Affirmation submission*. The affirming official shall submit a CMMC affirmation in the following instances:

(i) Upon completion of the assessment (conditional or final);

(ii) Annually thereafter; and

(iii) 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) *CMMC Level 1 Self-Assessment*. At the completion of a self-assessment and annually thereafter, the affirming official shall submit a CMMC affirmation attesting to continuing compliance with all CMMC Level 1 security requirements.

(2) *CMMC Level 2 Self-Assessment*. At the completion of a self-assessment and annually thereafter, the affirming official shall submit a CMMC affirmation attesting to continuing compliance with all CMMC Level 2 security requirements. An affirmation shall also be submitted at the completion of a POA&M Closeout assessment.

(3) *CMMC Level 2 Certification Assessment*. At the completion of a C3PAO assessment and annually thereafter, the affirming official shall submit a CMMC affirmation attesting to continuing compliance with all CMMC Level 2 security requirements. An affirmation shall also be submitted at the completion of a POA&M Closeout assessment.

(4) *CMMC Level 3 Certification Assessment*. At the completion of a DCMA DIBCAC assessment and annually thereafter, the affirming official shall submit a CMMC affirmation attesting to continuing compliance with all CMMC Level 3 security requirements. This

requirement is in addition to the ongoing requirement for Level 2 affirmation. An affirmation shall also be submitted at the completion of a POA&M Closeout assessment.

§ 170.23 Application to subcontractors.

(a) *Procedures*. CMMC Level requirements apply to prime contractors and subcontractors throughout the supply chain at all tiers that will process, store, or transmit FCI or CUI on contractor information systems in the performance of the contract or subcontract. 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 follows:

(1) If a subcontractor will only process, store, or transmit FCI (and not CUI) in performance of the contract, then CMMC Level 1 Self-Assessment is required for the subcontractor.

(2) If a subcontractor will process, store, or transmit CUI in performance of the subcontract, CMMC Level 2 Self-Assessment is the minimum requirement for the subcontractor.

(3) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the Prime contractor has a requirement of Level 2 Certification Assessment, then CMMC Level 2 Certification Assessment is the minimum requirement for the subcontractor.

(4) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the Prime contractor has a requirement of Level 3 Certification Assessment, then CMMC Level 2 Certification Assessment is the minimum requirement for the subcontractor.

(b) [Reserved].

§ 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 Rev 2 security requirements (incorporated by reference elsewhere in this part, see § 170.2) and the specified NIST SP 800-172 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, CMMC Level 2 security requirement IA.L2-3.5.3, a Derived Security Requirement).

(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 working papers, drafts, and unofficial or unapproved policies.

(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, CMMC security requirement SC.L1-3.13.5 "Public-Access System Separation" 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 self-assessment results are scored as MET or NOT MET in their entirety; therefore, no score is calculated, and no scoring methodology is needed.

(2) *CMMC Level 2 Scoring Methodology*. The maximum score achievable for a CMMC Level 2 assessment is equal to the total number of CMMC Level 2 security requirements. If all CMMC Level 2 security requirement objectives are MET, OSAs are awarded the maximum score. For each requirement objective 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 CMMC Level 2 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).

(*1*) For NIST SP 800-171 Rev 2 Basic and Derived Security Requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration of CUI, 5 points are subtracted from the maximum score. The Basic and Derived security requirements with a value of 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.L2-3.1.17, 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, 3 points are subtracted from the maximum score. The Basic and Derived security requirements with a value of 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 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 FIPS-validated, three (3) points are subtracted from the maximum score; if encryption is not employed; five (5) points are subtracted from the maximum score.

(5) Future revisions of NIST SP 800-171 Rev 2 may add, delete, or substantively revise security requirements. When this occurs, a value is assigned by the Department to any new or modified security requirements in accordance with the scoring methodology in accordance with paragraph (c) of this section.

(6) OSAs must have a system security plan (CMMC Level 2 security requirement CA.L2-3.12.4) in place to describe each information system within the CMMC Assessment Scope, and a POA&M (CMMC Level 2 security requirement CA.L2-3.12.2) in place for each NOT MET security requirement in accordance with § 170.21.

(7) 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.'

(8) Specialized Assets (referred to as "enduring exceptions" in NIST SP 800-171 Rev 2) must be evaluated for their asset category per the CMMC scoping guidance for the level in question and handled accordingly (insert references L1-3).

(9) If an OSC previously received a favorable adjudication from the DoD CIO for an alternative security measure (in accordance with DFARS provision 252.204-7008 (48 CFR 252.204-7008) or DFARS clause 252.204-7012 (48 CFR 252.204-7012)), 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 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. Future revisions of NIST SP 800-171 Rev 2 may add, delete, or substantively revise security requirements. If this occurs, a value will be assigned by the Department to any new or modified security requirements in accordance with the table 1 scoring methodology:

Table 1 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 "1" point for each security requirement. As a result, the maximum score achievable for a CMMC Level 3 is equivalent to the total number of CMMC Level 3 security requirements. 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 CMMC Level 2 assessment score is required to be eligible for conduct of a CMMC Level 3 Certification Assessment. The CMMC Level 3 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/.

See these guidance documents in docket number DoD-2023-OS-0096 for specific details and to provide comments on the guidance.

Patricia L. Toppings,

OSD Federal Register Liaison Officer,

Department of Defense.

[FR Doc. 2023-27280 Filed: 12/22/2023 8:45 am; Publication Date: 12/26/2023]