PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Subpart A—General Information.

[**170.1**](#sectno-reference-170.1)Purpose.

[**170.2**](#sectno-reference-170.2)Incorporation by reference.

[**170.3**](#sectno-reference-170.3)Applicability.

[**170.4**](#sectno-reference-170.4)Acronyms and definitions.

[**170.5**](#sectno-reference-170.5)Policy.

Subpart B—Government Roles and Responsibilities.

[**170.6**](#sectno-reference-170.6)CMMC PMO.

[**170.7**](#sectno-reference-170.7)DCMA DIBCAC.

Subpart C—CMMC Assessment and Certification Ecosystem.

[**170.8**](#sectno-reference-170.8)Accreditation Body.

[**170.9**](#sectno-reference-170.9)CMMC Third-Party Assessment Organizations (C3PAOs).

[**170.10**](#sectno-reference-170.10)CMMC Assessor and Instructor Certification Organization (CAICO).

[**170.11**](#sectno-reference-170.11)CMMC Certified Assessor (CCA).

[**170.12**](#sectno-reference-170.12)CMMC Certified Instructor (CCI).

[**170.13**](#sectno-reference-170.13)CMMC Certified Professional (CCP).

Subpart D—Key Elements of the CMMC Program.

[**170.14**](#sectno-reference-170.14)CMMC model.

[**170.15**](#sectno-reference-170.15)CMMC Level 1 Self-Assessment and Affirmation requirements.

[**170.16**](#sectno-reference-170.16)CMMC Level 2 Self-Assessment and Affirmation requirements.

[**170.17**](#sectno-reference-170.17)CMMC Level 2 Certification Assessment and Affirmation requirements.

[**170.18**](#sectno-reference-170.18)CMMC Level 3 Certification Assessment and Affirmation requirements.

[**170.19**](#sectno-reference-170.19)CMMC scoping.

[**170.20**](#sectno-reference-170.20)Standards acceptance.

[**170.21**](#sectno-reference-170.21)Plan of Action and Milestones requirements.

[**170.22**](#sectno-reference-170.22)Affirmation.

[**170.23**](#sectno-reference-170.23)Application to subcontractors.

[**170.24**](#sectno-reference-170.24)CMMC scoring methodology.

Appendix A to Part 170—Guidance

Authority: [5 U.S.C. 301](https://www.govinfo.gov/link/uscode/5/301); Sec. 1648, [Pub. L. 116–92](https://www.govinfo.gov/link/plaw/116/public/92), 133 Stat. 1198.

# Subpart A—General Information.

## [§ 170.1](#sectno-citation-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](#sectno-citation-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)](https://www.govinfo.gov/link/uscode/5/552) and [1 CFR part 51](https://www.ecfr.gov/current/title-1/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/​*](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*](http://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/​*](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*](http://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*](http://www.iso.org/popular-standards.html)*.[[1]](#footnote-1)*

(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).

## [§ 170.3](#sectno-citation-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](#sectno-citation-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*](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](https://www.ecfr.gov/current/title-48/section-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)](https://www.ecfr.gov/current/title-32/section-2002.4#p-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](https://www.ecfr.gov/current/title-48/section-252.204-7020)).

*Defense Industrial Base (DIB)* is defined in [32 CFR 236.2](https://www.ecfr.gov/current/title-32/section-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*](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](https://www.ecfr.gov/current/title-48/section-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](https://www.ecfr.gov/current/title-48/section-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). [[2]](#footnote-2)

*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](https://www.ecfr.gov/current/title-48/section-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](https://www.ecfr.gov/current/title-48/section-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](#sectno-citation-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](https://www.ecfr.gov/current/title-48/section-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](https://www.ecfr.gov/current/title-48/section-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](#sectno-citation-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](https://www.ecfr.gov/current/title-48/section-252.204-7012) and [252.204–7020](https://www.ecfr.gov/current/title-48/section-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](#sectno-citation-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](#sectno-citation-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](https://www.ecfr.gov/current/title-5) 1400.201(b) and (d) and the investigative requirements of [title 5 CFR](https://www.ecfr.gov/current/title-5) 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)](https://www.ecfr.gov/current/title-32/section-117.11#p-117.11(b)) using the procedures outlined in [32 CFR 117.11(c)](https://www.ecfr.gov/current/title-32/section-117.11#p-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](#sectno-citation-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](https://www.ecfr.gov/current/title-5) 1400.201(b) and (d) and the investigative requirements of [title 5 CFR](https://www.ecfr.gov/current/title-5) 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)](https://www.ecfr.gov/current/title-32/section-117.11#p-117.11(b)) using the procedures outlined in [32 CFR 117.11(c)](https://www.ecfr.gov/current/title-32/section-117.11#p-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*](https://cmmc.emass.apps.mil)*.*  [[1](#footnote-1-p89126)]

(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](#sectno-citation-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 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](#sectno-citation-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](https://www.ecfr.gov/current/title-5) 1400.201(b) and (d) and the investigative requirements of [title 5 CFR](https://www.ecfr.gov/current/title-5) 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](#sectno-citation-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](#sectno-citation-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](https://www.ecfr.gov/current/title-5) 1400.201(b) and (d) and the investigative requirements of [title 5 CFR](https://www.ecfr.gov/current/title-5) 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](#sectno-citation-170.14) CMMC Model.

(a) *Overview.* The CMMC Model incorporates the security requirements from:

(1) FAR 52.204–21 ([48 CFR 52.204–21](https://www.ecfr.gov/current/title-48/section-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 No. [[3]](#footnote-3)** | **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. |
|  |

(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](#sectno-citation-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)( ii )—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/​*](https://DoDcio.defense.gov/CMMC/)*.*

(2) [Reserved].

## [§ 170.16](#sectno-citation-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*](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](#sectno-citation-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](https://www.ecfr.gov/current/title-32/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*](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](#sectno-citation-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](#footnote-1-p89132)] 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.

(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*](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](#sectno-citation-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. | ○ Assess against CMMC security requirements. |
|   |  | ○ Prepare to be assessed 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. ○ Prepare to be assessed against CMMC security requirements. | ○ Assess 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 do not provide security protections for CUI Assets | ○ Prepare to justify the inability of an Out-of-Scope Asset to store, process, or transmit CUI | ○ None. |
|   | ○ 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 |  |  |

(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/​*](https://www.dcma.mil/DIBCAC/) or email *dcma\_dibcac\_cmmc@mail.mil**.*

## [§ 170.20](#sectno-citation-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](#sectno-citation-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](#sectno-citation-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](#sectno-citation-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](#sectno-citation-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](https://www.ecfr.gov/current/title-48/section-252.204-7008)) or DFARS clause 252.204–7012 ([48 CFR 252.204–7012](https://www.ecfr.gov/current/title-48/section-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/​*](https://DoDcio.defense.gov/CMMC/)*.*

(b) “CMMC Assessment Guide—Level 1” available at [*https://DoDcio.defense.gov/​CMMC/​*](https://DoDcio.defense.gov/CMMC/)*.*

(c) “CMMC Assessment Guide—Level 2” available at [*https://DoDcio.defense.gov/​CMMC/​*](https://DoDcio.defense.gov/CMMC/)*.*

(d) “CMMC Assessment Guide—Level 3” available at [*https://DoDcio.defense.gov/​CMMC/​*](https://DoDcio.defense.gov/CMMC/)*.*

(e) “CMMC Scoping Guide—Level 1” available at [*https://DoDcio.defense.gov/​CMMC/​*](https://DoDcio.defense.gov/CMMC/)*.*

(f) “CMMC Scoping Guide—Level 2” available at [*https://DoDcio.defense.gov/​CMMC/​*](https://DoDcio.defense.gov/CMMC/)*.*

(g) “CMMC Scoping Guide—Level 3” available at [*https://DoDcio.defense.gov/​CMMC/​*](https://DoDcio.defense.gov/CMMC/)*.*

(h) “CMMC Hashing Guide” available at [*https://DoDcio.defense.gov/​CMMC/​*](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.

# Footnotes

1.   [*https://www.federalregister.gov/​citation/​75-FR-68675*](https://www.federalregister.gov/citation/75-FR-68675) (November 4, 2010).

[Back to Citation](#citation-1-p89058)

2.   [*https://www.federalregister.gov/​citation/​75-FR-707*](https://www.federalregister.gov/citation/75-FR-707) (December 29, 2009).

[Back to Citation](#citation-2-p89058)

3.   [*https://www.govinfo.gov/​link/​uscode/​42/​2011*](https://www.govinfo.gov/link/uscode/42/2011)*, et seq.*

[Back to Citation](#citation-3-p89058)

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

[Back to Citation](#citation-4-p89058)

5.   [*https://www.acquisition.gov/​far/​52.204-21*](https://www.acquisition.gov/far/52.204-21)*.*

[Back to Citation](#citation-5-p89059)

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

[Back to Citation](#citation-6-p89059)

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.”

[Back to Citation](#citation-7-p89059)

8.   [*https://www.sprs.csd.disa.mil/​*](https://www.sprs.csd.disa.mil/) under OMB control number 0750–0004.

[Back to Citation](#citation-8-p89059)

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.

[Back to Citation](#citation-9-p89059)

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

[Back to Citation](#citation-10-p89059)

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*](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)

[Back to Citation](#citation-11-p89059)

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

[Back to Citation](#citation-12-p89059)

13.   [*https://www.iso.org/​standard/​67198.html*](https://www.iso.org/standard/67198.html)*.*

[Back to Citation](#citation-13-p89064)

14.   [*https://www.iso.org/​committee/​54998.html*](https://www.iso.org/committee/54998.html)*.*

[Back to Citation](#citation-14-p89064)

15.   [*https://www.iso.org/​standard/​52993.html*](https://www.iso.org/standard/52993.html)*.*

[Back to Citation](#citation-15-p89064)

16.  This system is accessible only to authorized users.

[Back to Citation](#citation-16-p89064)

17.   [*https://irp.fas.org/​offdocs/​nsdd/​nsdd-189.htm*](https://irp.fas.org/offdocs/nsdd/nsdd-189.htm)*.*

[Back to Citation](#citation-17-p89068)

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

[Back to Citation](#citation-18-p89069)

19.  Based on information from the Council of Economic Advisors report: The Cost of Malicious Cyber Activity to the U.S. Economy, 2018.

[Back to Citation](#citation-19-p89078)

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*](https://www.csis.org/analysis/economic-impact-cybercrime)*.*

[Back to Citation](#citation-20-p89078)

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).

[Back to Citation](#citation-21-p89078)

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

[Back to Citation](#citation-22-p89079)

23.   [*https://www.gao.gov/​assets/​gao-22-104746.pdf*](https://www.gao.gov/assets/gao-22-104746.pdf).

[Back to Citation](#citation-23-p89080)

24.   [*https://www.ic3.gov/​Media/​News/​2021/​210310.pdf*](https://www.ic3.gov/Media/News/2021/210310.pdf).

[Back to Citation](#citation-24-p89080)

25.   [*https://www.cisa.gov/​uscert/​ncas/​current-activity/​2021/​07/​04/​cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa*](https://www.cisa.gov/uscert/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa).

[Back to Citation](#citation-25-p89080)

26.   [*https://www.mitre.org/​sites/​default/​files/​publications/​pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf*](https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf).

[Back to Citation](#citation-26-p89080)

27.   [*https://www.cisa.gov/​uscert/​ncas/​alerts/​aa22-057a*](https://www.cisa.gov/uscert/ncas/alerts/aa22-057a).

[Back to Citation](#citation-27-p89080)

28.  DODIG–2019–105 “Audit of Protection of DoD CUI on Contractor-Owned Networks and Systems”

[Back to Citation](#citation-28-p89081)

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.

[Back to Citation](#citation-29-p89086)

30.  Includes all businesses with the exception of those defined under the small business criteria and size standards provided in [13 CFR 121.201](https://www.ecfr.gov/current/title-13/section-121.201) (See FAR Part 19.102)

[Back to Citation](#citation-30-p89086)

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.

[Back to Citation](#citation-31-p89086)

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.

[Back to Citation](#citation-32-p89087)

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

[Back to Citation](#citation-33-p89087)

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.

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

[Back to Citation](#citation-34-p89089)

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.

[Back to Citation](#citation-38-p89089)

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.

[Back to Citation](#citation-39-p89090)

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

[Back to Citation](#citation-40-p89090)

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

[Back to Citation](#citation-41-p89096)

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.

[Back to Citation](#citation-42-p89096)

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.

[Back to Citation](#citation-43-p89097)

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

[Back to Citation](#citation-44-p89099)

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.

[Back to Citation](#citation-45-p89099)

46.   [*https://www.govinfo.gov/​content/​pkg/​CHRG-113hhrg86391/​html/​CHRG-113hhrg86391.htm*](https://www.govinfo.gov/content/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm)*.*

[Back to Citation](#citation-46-p89101)

47.   [*https://www.nbr.org/​program/​commission-on-the-theft-of-intellectual-property/​*](https://www.nbr.org/program/commission-on-the-theft-of-intellectual-property/)*.*

[Back to Citation](#citation-47-p89101)

48.   [*https://www.cybernc.us/​fci-cui/​*](https://www.cybernc.us/fci-cui/)*.*

[Back to Citation](#citation-48-p89101)

49.  GAO Report to Congress, Defense Contractor Cybersecurity Stakeholder Communication and Performance Goals Could Improve Certification Framework, Dec. 2021.

[Back to Citation](#citation-49-p89101)

50.   [*https://www.cisa.gov/​news-events/​cybersecurity-advisories/​aa22-047a*](https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-047a)*.*

[Back to Citation](#citation-50-p89101)

51.   [*https://www.whitehouse.gov/​briefing-room/​statements-releases/​2022/​03/​21/​statement-by-president-biden-on-our-nations-cybersecurity/​*](https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/)*.*

[Back to Citation](#citation-51-p89101)

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*](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)*.*

[Back to Citation](#citation-52-p89102)

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

[Back to Citation](#citation-53-p89103)

54.  Small entities are small business concerns.

[Back to Citation](#citation-54-p89104)

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

[Back to Citation](#citation-55-p89106)

56.  IT = Information Technology, MGMT = Management.

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.

[Back to Citation](#citation-56-p89107)

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

[Back to Citation](#citation-60-p89107)

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

[Back to Citation](#citation-62-p89113)

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

[Back to Citation](#citation-63-p89115)

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).

[Back to Citation](#citation-64-p89115)

66.  Respondent is equivalent to an entity; an entity provides one response annually.

[Back to Citation](#citation-66-p89116)

67.  Each entity has one response annually; the public and the government are the respondents at Level 3.

[Back to Citation](#citation-67-p89117)

1.  This system is accessible only to authorized users.

[Back to Citation](#citation-1-p89126)

1.   [*https://www.dcma.mil/​DIBCAC*](https://www.dcma.mil/DIBCAC).

[Back to Citation](#citation-1-p89132)

BILLING CODE 6001–FR–P

BILLING CODE 6001–FR–C

[[FR Doc. 2023–27280](https://www.federalregister.gov/d/2023-27280) Filed 12–22–23; 8:45 am]

BILLING CODE 6001–FR–P

1. **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*](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. [↑](#footnote-ref-1)
2. **Note 1 to *ODP:*** For CMMC Level 3, the organization defining the parameters is the DoD. [↑](#footnote-ref-2)
3. 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. [↑](#footnote-ref-3)