PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Subpart A—General Information

Subpart B—Government Roles and Responsibilities

Subpart C—CMMC Assessment and Certification Ecosystem

Subpart D—Key Elements of the CMMC Program

AUTHORITY: 5 U.S.C. 301; Sec. 1648, Pub. L. 116–92, 133 Stat. 1198.

SOURCE: 89 FR 83214, Oct. 15, 2024, unless otherwise noted.

Subpart A—General Information.

§ 170.1 Purpose.

(a) This part describes the Cybersecurity Maturity Model Certification (CMMC) Program of the Department of Defense (DoD) and establishes requirements for defense contractors and subcontractors to implement prescribed cybersecurity standards for safeguarding Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). This part (the CMMC Program) also establishes requirements for conducting an assessment of compliance with the applicable prescribed cybersecurity standard for contractor information systems that: process, store, or transmit FCI or CUI; provide security protections for systems which process, store, or transmit CUI; or are not logically or physically isolated from systems which process, store, or transmit CUI.

(b) The CMMC Program provides DoD with a viable means of conducting the volume of assessments necessary to verify contractor and subcontractor implementation of required cybersecurity requirements.

(c) The CMMC Program is designed to ensure defense contractors are properly safeguarding FCI and CUI that is processed, stored, or transmitted on defense contractor information systems. FCI and CUI must be protected to meet evolving threats and safeguard nonpublic, unclassified information that supports and enables the warfighter. The CMMC Program provides a consistent methodology to assess a defense contractor's implementation of required cybersecurity requirements. The CMMC Program utilizes the security standards set forth in the 48 CFR 52.204–21; National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, *Basic Safeguarding of Covered Contractor Information Systems*, Revision 2, February 2020 (includes updates as of January 28, 2021) (NIST SP 800–171 R2); and selected requirements from the NIST SP 800–172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800–171*, February 2021 (NIST SP 800–172 Feb2021), as applicable (see table 1 to § 170.14(c)(4) for requirements, see § 170.2 for availability of NIST publications).

(d) The CMMC Program balances the need to safeguard FCI and CUI and the requirement to share information appropriately with defense contractors in order to develop capabilities for the DoD. The CMMC Program is designed

to ensure implementation of cybersecurity practices for defense contractors and to provide DoD with increased assurance that FCI and CUI information will be adequately safeguarded when residing on or transiting contractor information systems.

(e) The CMMC Program creates no right or benefit, substantive or procedural, enforceable by law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

§ 170.2 Incorporation by reference.

Certain material is incorporated by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. Material approved for incorporation by reference (IBR) is available for inspection at the Department of Defense (DoD) and at the National Archives and Records Administration (NARA). Contact DoD online: *https://DoDcio.defense.gov/CMMC/*; email: *osd.mc-alex.DoD-cio.mbx.cmmc-rule@mail.mil*; or phone: (202) 770–9100. For information on the availability of this material at NARA, visit: *www.archives.gov/federal-register/cfr/ibr-locations* or email: *fr.inspection@nara.gov*. The material may be obtained from the following sources:

(a) National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Gaithersburg, MD 20899; phone: (301) 975–8443; website: *https://csrc.nist.gov/publications/*.

(1) FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006 (FIPS PUB 200 Mar2006); IBR approved for § 170.4(b).

(2) FIPS PUB 201–3, Personal Identity Verification (PIV) of Federal Employees and Contractors, January 2022 (FIPS PUB 201–3 Jan2022); IBR approved for § 170.4(b).

(3) SP 800–37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018 (NIST SP 800–37 R2); IBR approved for § 170.4(b).

(4) SP 800–39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011 (NIST SP 800–39 Mar2011); IBR approved for § 170.4(b).

(5) SP 800–53, Security and Privacy Controls for Information Systems and Organizations, Revision 5, September 2020 (includes updates as of December 10, 2020) (NIST SP 800–53 R5); IBR approved for § 170.4(b).

(6) SP 800–82r3, Guide to Operational Technology (OT) Security, September 2023 (NIST SP 800–82r3); IBR approved for § 170.4(b).

(7) SP 800–115, Technical Guide to Information Security Testing and Assessment, September 2008 (NIST SP 800–115 Sept2008); IBR approved for § 170.4(b).

(8) SP 800–160, Volume 2, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, Revision 1, December 2021 (NIST SP 800–160 V2R1); IBR approved for § 170.4(b).

(9) SP 800–171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Revision 2, February 2020 (includes updates as of January 28, 2021), (NIST SP 800–171 R2); IBR approved for §§ 170.4(b) and 170.14(a) through (c).

(10) SP 800–171A, Assessing Security Requirements for Controlled Unclassified Information, June 2018 (NIST SP 800–171A Jun2018); IBR approved for §§ 170.11(a), 170.14(d), 170.15(c), 170.16(c), 170.17(c), and 170.18(c).

(11) SP 800–172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800–171, February 2021 (NIST SP 800–172 Feb2021); IBR approved for §§ 170.4(b), 170.5(a), and 170.14(a) and (c).

(12) SP 800–172A, Assessing Enhanced Security Requirements for Controlled Unclassified Information, March 2022 (NIST SP 800–172A Mar2022); IBR approved for §§ 170.4(b), 170.14(d), and 170.18(c).

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

(1) ISO/IEC 17011:2017(E), Conformity assessment—Requirements for accreditation bodies accrediting conformity

assessment bodies, Second edition, November 2017 (ISO/IEC 17011:2017(E)); IBR approved for §§ 170.8(b)(3), 170.9(b)(13), and 170.10(b)(4).

(2) ISO/IEC 17020:2012(E), Conformity assessment—Requirement for the operation of various types of bodies performing inspection, Second edition, March 1, 2012 (ISO/IEC 17020:2012(E)); IBR approved for §§ 170.8(a), (b)(1), (b)(3) and 170.9(b)(2) and (b)(13).

(3) ISO/IEC 17024:2012(E), Conformity assessment—General requirements for bodies operating certification of persons, second edition, July 1, 2012 (ISO/IEC 17024:2012(E)); IBR approved for §§ 170.8(b)(2) and 170.10(a) and (b)(4), (7), and (8).

NOTE 1 TO PARAGRAPH (b): The ISO/IEC standards incorporated by reference in this part may be viewed at no cost in ''read only'' format at *https://ibr.ansi.org*.

§ 170.3 Applicability.

(a) The requirements of this part apply to:

(1) All DoD contract and subcontract awardees that will process, store, or transmit information, in performance of the DoD contract, that meets the standards for FCI or CUI on contractor information systems; and,

(2) Private-sector businesses or other entities comprising the CMMC Assessment and Certification Ecosystem, as specified in subpart C of this part.

(b) The requirements of this part do not apply to Federal information systems operated by contractors or subcontractors on behalf of the Government.

(c) CMMC Program requirements apply to all DoD solicitations and contracts pursuant to which a defense contractor or subcontractor will process, store, or transmit FCI or CUI on unclassified contractor information systems, including those for the acquisition of commercial items (except those exclusively for COTS items) valued at greater than the micro-purchase threshold except under the following circumstances:

(1) The procurement occurs during Implementation Phase 1, 2, or 3 as described in paragraph (e) of this section, in which case CMMC Program requirements apply in accordance with the requirements for the relevant phase-in period; or

(2) Application of CMMC Program requirements to a procurement or class of procurements may be waived in advance of the solicitation at the discretion of DoD in accordance with all applicable policies, procedures, and approval requirements.

(d) DoD Program Managers or requiring activities are responsible for selecting the CMMC Status that will apply for a particular procurement or contract based upon the type of information, FCI or CUI, that will be processed on, stored on, or transmitted through a contractor information system. Application of the CMMC Status for subcontractors will be determined in accordance with § 170.23.

(e) DoD is utilizing a phased approach for the inclusion of CMMC Program requirements in solicitations and contracts. Implementation of CMMC Program requirements will occur over four (4) phases:

(1) *Phase 1.* Begins on the effective date of the complementary 48 CFR part 204 CMMC Acquisition final rule. DoD intends to include the requirement for CMMC Statuses of Level 1 (Self) or Level 2 (Self) for all applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, include the requirement for CMMC Status of Level 1 (Self) or Level 2 (Self) for applicable DoD solicitations and contracts as a condition to exercise an option period on a contract awarded prior to the effective date. DoD may also, at its discretion, include the requirement for CMMC Status of Level 2 (C3PAO) in place of the Level 2 (Self) CMMC Status for applicable DoD solicitations and contracts.

(2) *Phase 2.* Begins one calendar year following the start date of Phase 1. In addition to Phase 1 requirements, DoD intends to include the requirement for CMMC Status of Level 2 (C3PAO) for applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, delay the inclusion of requirement for CMMC Status of Level 2 (C3PAO) to an option period instead of as a condition of contract award. DoD may also, at its discretion, include the requirement for CMMC Status of Level 3 (DIBCAC) for

applicable DoD solicitations and contracts.

(3) *Phase 3*. Begins one calendar year following the start date of Phase 2. In addition to Phase 1 and 2 requirements, DoD intends to include the requirement for CMMC Status of Level 2 (C3PAO) for all applicable DoD solicitations and contracts as a condition of contract award and as a condition to exercise an option period on a contract awarded after the effective date. DoD intends to include the requirement for CMMC Status of Level 3 (DIBCAC) for all applicable DoD solicitations and contracts as a condition of contract award. DoD may, at its discretion, delay the inclusion of requirement for CMMC Status of Level 3 (DIBCAC) to an option period instead of as a condition of contract award.

(4) *Phase 4, full implementation*. Begins one calendar year following the start date of Phase 3. DoD will include CMMC Program requirements in all applicable DoD solicitations and contracts including option periods on contracts awarded prior to the beginning of Phase 4.

§ 170.4 Acronyms and definitions.

(a) *Acronyms*. Unless otherwise noted, the following acronyms and their terms are for the purposes of this part.

AC—Access Control
APT—Advanced Persistent Threat
AT—Awareness and Training
C3PAO—CMMC Third-Party Assessment Organization
CA—Security Assessment
CAICO—CMMC Assessors and Instructors Certification Organization
CAGE—Commercial and Government Entity
CCA—CMMC-Certified Assessor
CCI—CMMC-Certified Instructor
CCP—CMMC-Certified Professional
CFR—Code of Federal Regulations
CIO—Chief Information Officer
CM—Configuration Management
CMMC—Cybersecurity Maturity Model Certification
CMMC PMO—CMMC Program Management Office
CNC—Computerized Numerical Control
CoPC—Code of Professional Conduct
CSP—Cloud Service Provider
CUI—Controlled Unclassified Information
DCMA—Defense Contract Management Agency
DD—Represents any two-character CMMC Domain acronym
DFARS—Defense Federal Acquisition Regulation Supplement
DIB—Defense Industrial Base
DIBCAC—DCMA's Defense Industrial Base Cybersecurity Assessment Center
DoD—Department of Defense
DoDI—Department of Defense Instruction
eMASS—Enterprise Mission Assurance Support Service
ESP—External Service Provider
FAR—Federal Acquisition Regulation
FCI—Federal Contract Information
FedRAMP—Federal Risk and Authorization Management Program
GFE—Government Furnished Equipment
IA—Identification and Authentication
ICS—Industrial Control System
IIoT—Industrial Internet of Things
IoT—Internet of Things
IR—Incident Response
IS—Information System
IEC—International Electrotechnical Commission
ISO/IEC—International Organization for Standardization/International Electrotechnical Commission
IT—Information Technology
L#—CMMC Level Number
MA—Maintenance
MP—Media Protection
MSSP—Managed Security Service Provider
NARA—National Archives and Records Administration
NAICS—North American Industry Classification System
NIST—National Institute of Standards and Technology
N/A—Not Applicable
ODP—Organization-Defined Parameter
OSA—Organization Seeking Assessment
OSC—Organization Seeking Certification
OT—Operational Technology
PI—Provisional Instructor
PIEE—Procurement Integrated Enterprise Environment
PII—Personally Identifiable Information
PLC—Programmable Logic Controller
POA&M—Plan of Action and Milestones

PRA—Paperwork Reduction Act
RM—Risk Management
SAM—System of Award Management
SC—System and Communications Protection
SCADA—Supervisory Control and Data Acquisition
SI—System and Information Integrity
SIEM—Security Information and Event Management
SP—Special Publication
SPD—Security Protection Data
SPRS—Supplier Performance Risk System
SSP—System Security Plan

(b) *Definitions.* Unless otherwise noted, these terms and their definitions are for the purposes of this part.

Access Control (AC) means the process of granting or denying specific requests to obtain and use information and related information processing services; and/or entry to specific physical facilities (*e.g.*, Federal buildings, military establishments, or border crossing entrances), as defined in FIPS PUB 201–3 Jan2002 (incorporated by reference, see §170.2).

Accreditation means a status pursuant to which a CMMC Assessment and Certification Ecosystem member (person or organization), having met all criteria for the specific role they perform including required ISO/IEC accreditations, may act in that role as set forth in §170.8 for the Accreditation Body and §170.9 for C3PAOs. (CMMC-custom term)

Accreditation Body is defined in §170.8 and means the one organization DoD contracts with to be responsible for authorizing and accrediting members of the CMMC Assessment and Certification Ecosystem, as required. The Accreditation Body must be approved by DoD. At any given point in time, there will be only one Accreditation Body for the DoD CMMC Program. (CMMC-custom term)

Advanced Persistent Threat (APT) means an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (*e.g.*, cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period-of-time, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives, as is defined in NIST SP 800–39 Mar2011 (incorporated by reference, see §170.2).

Affirming Official means the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations. (CMMC-custom term)

Assessment means the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization, as defined in §§170.15 through 170.18. (CMMC-custom term)

(i) *Level 1 self-assessment* is the term for the activity performed by an OSA to evaluate its own information system when seeking a CMMC Status of Level 1 (Self).

(ii) *Level 2 self-assessment* is the term for the activity performed by an OSA to evaluate its own information system when seeking a CMMC Status of Level 2 (Self).

(iii) *Level 2 certification assessment* is the term for the activity performed by a C3PAO to evaluate the information system of an OSC when seeking a CMMC Status of Level 2 (C3PAO).

(iv) *Level 3 certification assessment* is the term for the activity performed by the DCMA DIBCAC to evaluate the information system of an OSC when seeking a CMMC Status of Level 3 (DIBCAC).

(v) *POA&M closeout self-assessment* is the term for the activity performed by an OSA to evaluate only the NOT MET

requirements that were identified with POA&M during the initial assessment, when seeking a CMMC Status of Final Level 2 (Self).

(vi) *POA&M closeout certification assessment* is the term for the activity performed by a C3PAO or DCMA DIBCAC to evaluate only the NOT MET requirements that were identified with POA&M during the initial assessment, when seeking a CMMC Status of Final Level 2 (C3PAO) or Final Level 3 (DIBCAC) respectively.

Assessment Findings Report means the final written assessment results by the third-party or government assessment team. The Assessment Findings Report is submitted to the OSC and to the DoD via CMMC eMASS. (CMMC-custom term)

Assessment objective means a set of determination statements that, taken together, expresses the desired outcome for the assessment of a security requirement. Successful implementation of the corresponding CMMC security requirement requires meeting all applicable assessment objectives defined in NIST SP 800–171A Jun2018 (incorporated by reference, see §170.2) or NIST SP 800–172A Mar2022 (incorporated by reference, see §170.2). (CMMC-custom term)

Assessment Team means participants in the Level 2 certification assessment (CMMC Certified Assessors and CMMC Certified Professionals) or the Level 3 certification assessment (DCMA DIBCAC assessors). This does not include the OSC participants preparing for or participating in the assessment. (CMMC-custom term)

Asset means an item of value to stakeholders. An asset may be tangible (*e.g.*, a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (*e.g.*, humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns, as defined in NIST SP 800–160 V2R1 (incorporated by reference, see §170.2).

Asset Categories means a grouping of assets that process, store or transmit information of similar designation, or provide security protection to those assets. (CMMC-custom term)

Authentication is defined in FIPS PUB 200 Mar2006 (incorporated by reference, see §170.2).

Authorized means an interim status during which a CMMC Ecosystem member (person or organization), having met all criteria for the specific role they perform other than the required ISO/IEC accreditations, may act in that role for a specified time as set forth in §170.8 for the Accreditation Body and §170.9 for C3PAOs. (CMMC-custom term)

Capability means a combination of mutually reinforcing controls implemented by technical means, physical means, and procedural means. Such controls are typically selected to achieve a common information security or privacy purpose, as defined in NIST SP 800–37 R2 (incorporated by reference, see §170.2).

Cloud Service Provider (CSP) means an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This definition is based on the definition for cloud computing in NIST SP 800–145 Sept2011. (CMMC-custom term)

CMMC Assessment and Certification Ecosystem means the people and organizations described in subpart C of this part. This term is sometimes shortened to CMMC Ecosystem. (CMMC-custom term)

CMMC Assessment Scope means the set of all assets in the OSA's environment that will be assessed against CMMC security requirements. (CMMC-custom term)

CMMC Assessor and Instructor Certification Organization (CAICO) is defined in §170.10 and means the organization responsible for training, testing, authorizing, certifying, and recertifying

CMMC certified assessors, certified instructors, and certified professionals. (CMMC-custom term)

CMMC Instantiation of eMASS means a CMMC instance of the Enterprise Mission Assurance Support Service (eMASS), a government owned and operated system. (CMMC-custom term)

CMMC Security Requirements means the 15 Level 1 requirements listed in the 48 CFR 52.204–21(b)(1), the 110 Level 2 requirements from NIST SP 800–171 R2 (incorporated by reference, see §170.2), and the 24 Level 3 requirements selected from NIST SP 800–172 Feb2021 (incorporated by reference, see §170.2).

CMMC Status is the result of meeting or exceeding the minimum required score for the corresponding assessment. The CMMC Status of an OSA information system is officially stored in SPRS and additionally presented on a Certificate of CMMC Status, if the assessment was conducted by a C3PAO or DCMA DIBCAC. The potential CMMC Statuses are outlined in the paragraphs that follow. (CMMC-custom term)

(i) *Final Level 1 (Self)* is defined in §170.15(a)(1) and (c)(1). (CMMC-custom term)

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

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

(iv) *Conditional Level 2 (C3PAO)* is defined in §170.17(a)(1)(ii). (CMMC-custom term)

(v) *Final Level 2 (C3PAO)* is defined in §170.17(a)(1)(iii). (CMMC-custom term)

(vi) *Conditional Level 3 (DIBCAC)* is defined in §170.18(a)(1)(ii). (CMMC-custom term)

(vii) *Final Level 3 (DIBCAC)* is defined in §170.18(a)(1)(iii). (CMMC-custom term)

CMMC Status Date means the date that the CMMC Status results are submitted to SPRS or the CMMC instantiation of eMASS, as appropriate. The date of the Conditional CMMC Status will remain as the CMMC Status Date after a successful POA&M closeout. A new date is not set for a Final that follows a Conditional. (CMMC-custom term)

CMMC Third-Party Assessment Organization (C3PAO) means an organization that has been authorized or accredited by the Accreditation Body to conduct Level 2 certification assessments and has the roles and responsibilities identified in §170.9. (CMMC-custom term)

Contractor is defined in 48 CFR 3.502–1.

Contractor Risk Managed Assets are defined in table 3 to §170.19(c)(1). (CMMC-custom term)

Controlled Unclassified Information (CUI) is defined in 32 CFR 2002.4(h).

Controlled Unclassified Information (CUI) Assets means assets that can process, store, or transmit CUI. (CMMC-custom term)

DCMA DIBCAC High Assessment means an assessment that is conducted by Government personnel in accordance with NIST SP 800–171A Jun2018 and leveraging specific guidance in the DoD Assessment Methodology that:

(i) Consists of:

(A) A review of a contractor's Basic Assessment;

(B) A thorough document review;

(C) Verification, examination, and demonstration of a contractor's system security plan to validate that NIST SP 800–171 R2 security requirements have been implemented as described in the contractor's system security plan; and

(D) Discussions with the contractor to obtain additional information or clarification, as needed; and

(ii) Results in a confidence level of ''High'' in the resulting score. (Source: 48 CFR 252.204–7020).

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

DoD Assessment Methodology (DoDAM) documents a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800–171 R2, a requirement for compliance with 48 CFR 252.204–7012. (Source: DoDAM Version 1.2.1)

Enduring Exception means a special circumstance or system where remediation and full compliance with CMMC security requirements is not feasible. Examples include systems required to replicate the configuration of 'fielded' systems, medical devices, test equipment, OT, and IoT. No operational plan of action is required but the circumstance must be documented within a system security plan. Specialized Assets and GFE may be enduring exceptions. (CMMC-custom term)

Enterprise means an organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (*e.g.,* budgets), human resources, security, and information systems, information and mission management, as defined in NIST SP 800–53 R5 (incorporated by reference, see §170.2).

External Service Provider (ESP) means external people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (*e.g.,* log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. (CMMC-custom term)

Federal Contract Information (FCI) is defined in 48 CFR 4.1901.

Government Furnished Equipment (GFE) has the same meaning as ''government-furnished property'' as defined in 48 CFR 45.101.

Industrial Control Systems (ICS) means a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations that are often found in the industrial sectors and critical infrastructures, such as Programmable Logic Controllers (PLC). An ICS consists of combinations of control components (*e.g.,* electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (*e.g.,* manufacturing, transportation of matter or energy), as defined in NIST SP 800–82r3 (incorporated by reference, see §170.2).

Information System (IS) is defined in NIST SP 800–171 R2 (incorporated by reference, see §170.2).

Internet of Things (IoT) means the network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information, as defined in NIST SP 800–172A Mar2022 (incorporated by reference, see §170.2).

Operational plan of action as used in security requirement CA.L2–3.12.2, means the formal artifact which identifies temporary vulnerabilities and temporary deficiencies (*e.g.,* necessary information system updates, patches, or reconfiguration as threats evolve) in implementation of requirements and documents how they will be mitigated, corrected, or eliminated. The OSA defines the format (*e.g.,* document, spreadsheet, database) and specific content of its operational plan of action. An operational plan of action does not identify a timeline for remediation and is not the same as a POA&M, which is associated with an assessment for remediation of deficiencies that must be completed within 180 days. (CMMC-custom term)

Operational Technology (OT) means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms, as defined in NIST SP 800–160 V2R1 (incorporated by reference, see §170.2).

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

Organization-Defined Parameters (ODPs) means selected enhanced security requirements contain selection and assignment operations to give organizations flexibility in defining variable parts of those requirements, as defined in NIST SP 800–172A Mar2022 (incorporated by reference, see §170.2).

Note 1 to ODPs: The organization defining the parameters is the DoD.

Organization Seeking Assessment (OSA) means the entity seeking to undergo a self-assessment or certification assessment for a given information system for the purposes of achieving and maintaining any CMMC Status. The term OSA includes all Organizations Seeking Certification (OSCs). (CMMC-custom term)

Organization Seeking Certification (OSC) means the entity seeking to undergo a certification assessment for a given information system for the purposes of achieving and maintaining the CMMC Status of Level 2 (C3PAO) or Level 3 (DIBCAC). An OSC is also an OSA. (CMMC-custom term)

Out-of-Scope Assets means assets that cannot process, store, or transmit CUI because they are physically or logically separated from information systems that do process, store, or transmit CUI, or are inherently unable to do so; except for assets that provide security protection for a CUI asset (see the definition for *Security Protection Assets*). (CMMC-custom term)

Periodically means occurring at a regular interval as determined by the OSA that may not exceed one year. (CMMC-custom term)

Personally Identifiable Information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual, as defined in NIST SP 800–53 R5 (incorporated by reference, see §170.2).

Plan of Action and Milestones (POA&M) means a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones, as defined in NIST SP 800–115 Sept2008 (incorporated by reference, see §170.2).

Prime Contractor is defined in 48 CFR 3.502–1.

Process, store, or transmit means data can be used by an asset (*e.g.*, accessed, entered, edited, generated, manipulated, or printed); data is inactive or at rest on an asset (*e.g.*, located on electronic media, in system component memory, or in physical format such as paper documents); or data is being transferred from one asset to another asset (*e.g.*, data in transit using physical or digital transport methods). (CMMC-custom term)

Restricted Information Systems means systems (and associated IT components comprising the system) that are configured based on government requirements (*e.g.*, connected to something that was required to support a functional requirement) and are used to support a contract (*e.g.*, fielded systems, obsolete systems, and product deliverable replicas). (CMMC-custom term)

Risk means a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of:

(i) The adverse impacts that would arise if the circumstance or event occurs; and

(ii) The likelihood of occurrence, as defined in NIST SP 800–53 R5 (incorporated by reference, see §170.2).

Risk Assessment means the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Risk Assessment is part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis, as defined in NIST SP 800–39 Mar2011 (incorporated by reference, see §170.2).

Security Protection Assets (SPA) means assets providing security functions or capabilities for the OSA's CMMC Assessment Scope. (CMMC-custom term)

Security Protection Data (SPD) means data stored or processed by Security Protection Assets (SPA) that are used to protect an OSC's assessed environment. SPD is security relevant information and includes but is not limited to: configuration data required to operate an SPA, log files generated by or ingested by an SPA, data related to the configuration or vulnerability status of in-scope assets, and passwords that grant access to the in-scope environment. (CMMC-custom term)

Specialized Assets means types of assets considered specialized assets for CMMC: Government Furnished Equipment, Internet of Things (IoT) or Industrial Internet of Things (IIoT), Operational Technology (OT), Restricted Information Systems, and Test Equipment. (CMMC-custom term)

Subcontractor is defined in 48 CFR 3.502–1.

Supervisory Control and Data Acquisition (SCADA) means a generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (*e.g.*, delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated, as defined in NIST SP 800–82r3 (incorporated by reference, see §170.2).

System Security Plan (SSP) means the formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The system security plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems, as defined in NIST SP 800–53 R5 (incorporated by reference, see §170.2).

Temporary deficiency means a condition where remediation of a discovered deficiency is feasible, and a known fix is available or is in process. The deficiency must be documented in an operational plan of action. A temporary deficiency is not based on an 'in progress' initial implementation of a CMMC security requirement but arises after implementation. A temporary deficiency may apply during the initial implementation of a security requirement if, during roll-out, specific issues with a very limited subset of equipment is discovered that must be separately addressed. There is no standard duration for which a temporary deficiency may be active. For example, FIPS-validated cryptography that requires a patch and the patched version is no longer the validated version may be a temporary deficiency. (CMMC-custom term)

Test Equipment means hardware and/or associated IT components used in the testing of products, system components, and contract deliverables. (CMMC-custom term)

User means an individual, or (system) process acting on behalf of an individual, authorized to access a system, as defined in NIST SP 800–53 R5 (incorporated by reference, see §170.2).

§170.5 Policy.

(a) Protection of FCI and CUI on contractor information systems is of paramount importance to the DoD and can directly impact its ability to successfully conduct essential missions and functions. It is DoD policy that defense contractors and subcontractors shall be required to safeguard FCI and CUI that is processed, stored, or transmitted on contractor information systems by applying specified security requirements. In addition, defense contractors and subcontractors may be required to implement additional safeguards defined in NIST SP 800–172 Feb2021 (incorporated by reference, see §170.2), implementing DoD specified parameters to meet CMMC Level 3 security requirements (see table 1 to §170.14(c)(4)). These additional requirements are necessary to protect CUI being processed, stored, or transmitted in contractor information systems, when designated by a requirement for CMMC Status of Level 3 (DIBCAC) as defined by a DoD program manager or requiring activity. In general, the Department will identify a requirement for a CMMC Status of Level 3 (DIBCAC) for solicitations and resulting contracts supporting its most critical programs and technologies.

(b) Program managers and requiring activities are responsible for identifying the CMMC Status that will apply to a procurement. Selection of the applicable CMMC Status will be based on factors including but not limited to:

(1) Criticality of the associated mission capability;

(2) Type of acquisition program or technology;

(3) Threat of loss of the FCI or CUI to be shared or generated in relation to the effort;

(4) Impacts from exploitation of information security deficiencies; and

(5) Other relevant policies and factors, including Milestone Decision Authority guidance.

(c) In accordance with the implementation plan described in §170.3, CMMC

Program requirements will apply to new DoD solicitations and contracts, and shall flow down to subcontractors who will process, store, or transmit FCI or CUI in performance of the subcontract, as described in §170.23.

(d) In very limited circumstances, and in accordance with all applicable policies, procedures, and requirements, a Service Acquisition Executive or Component Acquisition Executive in the DoD, or as delegated, may elect to waive inclusion of CMMC Program requirements in a solicitation or contract. In such cases, contractors and subcontractors will remain obligated to comply with all applicable cybersecurity and information security requirements.

(e) The CMMC Program does not alter any separately applicable requirements to protect FCI or CUI, including those requirements in accordance with 48 CFR 52.204–21, *Basic Safeguarding of Covered Contractor Information Systems*, or covered defense information in accordance with 48 CFR 252.204–7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, or any other applicable information protection requirements. The CMMC Program provides a means of verifying implementation of the security requirements set forth in 48 CFR 52.204–21, NIST SP 800–171 R2, and NIST SP 800–172 Feb2021, as applicable.

Subpart B—Government Roles and Responsibilities.

§170.6 CMMC PMO.

(a) The Office of the Department of Defense Chief Information Officer (DoD CIO) Office of the Deputy CIO for Cybersecurity (DoD CIO(CS)) provides oversight of the CMMC Program and is responsible for establishing CMMC assessment, accreditation, and training requirements as well as developing and updating CMMC Program policies and implementing guidance.

(b) The CMMC PMO is responsible for monitoring the CMMC AB's performance of roles assigned in this rule and acting as necessary to address problems pertaining to effective performance.

(c) The CMMC PMO retains, on behalf of the DoD CIO(CS), the prerogative to review decisions of the CMMC Accreditation Body as part of its oversight of the CMMC program and evaluate any alleged conflicts of interest purported to influence the CMMC Accreditation Body's objectivity.

(d) The CMMC PMO is responsible for sponsoring necessary DCSA activities including FOCI risk assessment and Tier 3 security background investigations for the CMMC Ecosystem members as specified in §§170.8(b)(4) and (5), 170.9(b)(3) through (5), 170.11(b)(3) and (4), and 170.13(b)(3) and (4).

(e) The CMMC PMO is responsible for investigating and acting upon indications that an active CMMC Status has been called into question. Indications that may trigger investigative evaluations include, but are not limited to, reports from the CMMC Accreditation Body, a C3PAO, or anyone knowledgeable of the security processes and activities of the OSA. Investigative evaluations include, but are not limited to, reviewing pertinent assessment information, and exercising the right to conduct a DCMA DIBCAC assessment of the OSA, as provided for under the 48 CFR 252.204–7020.

(f) If a subsequent DCMA DIBCAC assessment shows that adherence to the provisions of this rule and the required CMMC Status have not been achieved or maintained, the DIBCAC results will take precedence over any pre-existing CMMC Status recorded in SPRS, or its successor capability. The DoD will update SPRS to reflect that the OSA is out of compliance and does not meet DoD CMMC requirements. If the OSA is working on an active contract requiring CMMC compliance, then standard contractual remedies will apply.

§170.7 DCMA DIBCAC.

(a) DCMA DIBCAC assessors in support of the CMMC Program will:

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

(2) Conduct Level 3 certification assessments and upload assessment results into the CMMC instantiation of eMASS, or its successor capability.

(3) Issue Certificates of CMMC Status resulting from Level 3 certification assessments.

(4) Conduct Level 2 certification assessments of the Accreditation Body

and prospective C3PAOs' information systems that process, store, and/or transmit CUI.

(5) Create and maintain a process for assessors to collect the list of assessment artifacts to include artifact names, their return value of the hashing algorithm, the hashing algorithm used, and upload that data into the CMMC instantiation of eMASS.

(6) As authorized and in accordance with all legal requirements, enter and track, OSC appeals and updated results arising from Level 3 certification assessment activities into the CMMC instantiation of eMASS.

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

(8) Conduct an assessment of the OSA, when requested by the CMMC PMO per §§170.6(e) and (f), as provided for under the 48 CFR 252.204–7019 and 48 CFR 252.204–7020.

(9) Identify assessments that meet the criteria in §170.20 and verify that SPRS accurately reflects the CMMC Status.

(b) An OSC, the CMMC AB, or a C3PAO may appeal the outcome of its DCMA DIBCAC conducted assessment within 21 days by submitting a written basis for appeal with the requirements in question for DCMA DIBCAC consideration. Appeals may be submitted for review by visiting *www.dcma.mil/DIBCAC* for contact information, and a DCMA DIBCAC Quality Assurance Review Team will provide a written response or request additional supporting documentation.

Subpart C—CMMC Assessment and Certification Ecosystem.

§170.8 Accreditation Body.

(a) *Roles and responsibilities.* The Accreditation Body is responsible for authorizing and ensuring the accreditation of CMMC Third-Party Assessment Organizations (C3PAOs) in accordance with ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2) and all applicable authorization and accreditation requirements set forth. The Accreditation Body is responsible for establishing the C3PAO authorization requirements and the C3PAO Accreditation Scheme and submitting both for approval by the CMMC PMO. At any given point in time, there will be only one Accreditation Body for the DoD CMMC Program.

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

(1) Be US-based and be and remain a member in good standing of the Inter-American Accreditation Cooperation (IAAC) and become an International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA) signatory, with a signatory status scope of ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2).

(2) Be and remain a member in good standing of the International Accreditation Forum (IAF) with mutual recognition arrangement signatory status scope of ISO/IEC 17024:2012(E) (incorporated by reference, see §170.2).

(3) Achieve and maintain full compliance with ISO/IEC 17011:2017(E) (incorporated by reference, see §170.2) and complete a peer assessment by other ILAC signatories for competence in accrediting conformity assessment bodies to ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2), both within 24 months of DoD approval.

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

(A) Authorize C3PAOs who meet all requirements set forth in §170.9 as well as administrative requirements as determined by the Accreditation Body to conduct Level 2 certification assessments and issue Certificates of CMMC Status to OSCs based on the assessment results.

(B) Require all C3PAOs to achieve and maintain the ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2) requirements within 27 months of authorization.

(ii) The Accreditation Body shall accredit C3PAOs, in accordance with ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2), who meet all requirements set forth in §170.9 to conduct Level 2 certification assessments and issue Certificates of CMMC Status to OSCs based on the results.

(4) Ensure that the Accreditation Body's Board of Directors, professional staff, Information Technology (IT) staff, accreditation staff, and independent CMMC Certified Assessor staff

complete a Tier 3 background investigation resulting in a determination of national security eligibility. This Tier 3 background investigation will not result in a security clearance and is not being executed for the purpose of government employment. The Tier 3 background investigation is initiated using the Standard Form (SF) 86 (*www.gsa.gov/reference/forms/questionnaire-for-national-security-positions*) and submitted by DoD CIO Security to Washington Headquarters Services (WHS) for coordination for processing by the Defense Counterintelligence and Security Agency (DCSA). These positions are designated as non-critical sensitive with a risk designation of ''Moderate Risk'' in accordance with 5 CFR 1400.201(b) and (d) and the investigative requirements of 5 CFR 731.106(c)(2).

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

(i) Completing the Standard Form (SF) 328 (*www.gsa.gov/reference/forms/certificate-pertaining-to-foreign-interests*), *Certificate Pertaining to Foreign Interests*, and submit it directly to Defense Counterintelligence and Security Agency (DCSA) and undergo a National Security Review with regards to the protection of controlled unclassified information based on the factors identified in 32 CFR 117.11(b) using the procedures outlined in 32 CFR 117.11(c). The Accreditation Body must receive a non-disqualifying eligibility determination by the CMMC PMO to be recognized by the Department of Defense.

(ii) Reporting any change to the information provided on its SF 328 by resubmitting the SF 328 to DCSA within 15 business days of the change being effective. A disqualifying eligibility determination, based on the results of the change, will result in the Accreditation Body losing its authorization or accreditation under the CMMC Program.

(iii) Identifying all prospective C3PAOs to the CMMC PMO. The CMMC PMO will sponsor the prospective C3PAO for a FOCI risk assessment conducted by the DCSA using the SF 328 as part of the authorization and accreditation processes.

(iv) Notifying prospective C3PAOs of the CMMC PMO's eligibility determination resulting from the FOCI risk assessment.

(6) Obtain a Level 2 certification assessment in accordance with the procedures specified in §170.17(a)(1) and (c). This assessment, conducted by DCMA DIBCAC, shall meet all requirements for a Final Level 2 (C3PAO) but will not result in a CMMC Status of Level 2 (C3PAO). The Level 2 certification assessment process must be performed every three years.

(7) Provide all documentation and records in English.

(8) Establish, maintain, and manage an up-to-date list of authorized and accredited C3PAOs on a single publicly accessible website and provide the list of these entities and their status to the DoD through submission in the CMMC instantiation of eMASS.

(9) Provide the CMMC PMO with current data on C3PAOs, including authorization and accreditation records and status in the CMMC instantiation of eMASS. This data shall include the dates associated with the authorization and accreditation of each C3PAO.

(10) Provide the DoD with information about aggregate statistics pertaining to operations of the CMMC Ecosystem to include the authorization and accreditation status of C3PAOs or other information as requested.

(11) Provide inputs for assessor supplemental guidance to the CMMC PMO. Participate and support coordination of these and other inputs through DoD-led Working Groups.

(12) Ensure that all information about individuals is encrypted and protected in all Accreditation Body information systems and databases.

(13) Provide all plans that are related to potential sources of revenue, to include but not limited to: fees, licensing, processes, membership, and/or partnerships to the Department's CMMC PMO.

(14) Ensure that the CMMC Assessors and Instructors Certification Organization (CAICO) is compliant with ISO/IEC 17024:2012(E)

(15) Ensure all training products, instruction, and testing materials are of high quality and subject to CAICO quality control policies and procedures, to include technical accuracy and

alignment with all applicable legal, regulatory, and policy requirements.

(16) Develop and maintain an internal appeals process, as required by ISO/IEC 17020:2017(E), and render a final decision on all elevated appeals.

(17) Develop and maintain a comprehensive plan and schedule to comply with all ISO/IEC 17011:2017(E), and DoD requirements for Conflict of Interest, Code of Professional Conduct, and Ethics policies as set forth in the DoD contract. All policies shall apply to the Accreditation Body, and other individuals, entities, and groups within the CMMC Ecosystem who provide Level 2 certification assessments, CMMC instruction, CMMC training materials, or Certificates of CMMC Status on behalf of the Accreditation Body. All policies in this section must be approved by the CMMC PMO prior to effectivity in accordance with the following requirements.

(i) *Conflict of Interest (CoI) policy*. The CoI policy shall:

(A) Include a detailed risk mitigation plan for all potential conflicts of interest that may pose a risk to compliance with ISO/IEC 17011:2017(E).

(B) Require employees, Board directors, and members of any accreditation committees or appeals adjudication committees to disclose to the CMMC PMO, in writing, as soon as it is known or reasonably should be known, any actual, potential, or perceived conflict of interest with sufficient detail to allow for assessment.

(C) Require employees, Board directors, and members of any accreditation committees or appeals adjudication committees who leave the board or organization to enter a ''cooling off period'' of one (1) year whereby they are prohibited from working with the Accreditation Body or participating in any and all CMMC activities described in Subpart C.

(D) Require CMMC Ecosystem members to actively avoid participating in any activity, practice, or transaction that could result in an actual or perceived conflict of interest.

(E) Require CMMC Ecosystem members to disclose to Accreditation Body leadership, in writing, any actual or potential conflict of interest as soon as it is known, or reasonably should be known.

(ii) *Code of Professional Conduct (CoPC) policy*. The CoPC policy shall:

(A) Describe the performance standards by which the members of the CMMC Ecosystem will be held accountable and the procedures for addressing violations of those performance standards.

(B) Require the Accreditation Body to investigate and resolve any potential violations that are reported or are identified by the DoD.

(C) Require the Accreditation Body to inform the DoD in writing of new investigations within 72 hours.

(D) Require the Accreditation Body to report to the DoD in writing the outcome of completed investigations within 15 business days.

(E) Require CMMC Ecosystem members to represent themselves and their companies accurately; to include not misrepresenting any professional credentials or status, including CMMC authorization or CMMC Status, nor exaggerating the services that they or their company are capable or authorized to deliver.

(F) Require CMMC Ecosystem members to be honest and factual in all CMMC-related activities with colleagues, clients, trainees, and others with whom they interact.

(G) Prohibit CMMC Ecosystem members from participating in the Level 2 certification assessment process for an assessment in which they previously served as a consultant to prepare the organization for any CMMC assessment within 3 years.

(H) Require CMMC Ecosystem members to maintain the confidentiality of customer and government data to preclude unauthorized disclosure.

(I) Require CMMC Ecosystem members to report results and data from Level 2 certification assessments and training objectively, completely, clearly, and accurately.

(J) Prohibit CMMC Ecosystem members from cheating, assisting another in cheating, or allowing cheating on CMMC examinations.

(K) Require CMMC Ecosystem members to utilize official training content

developed by a CMMC training organization approved by the CAICO in all CMMC certification courses.

(iii) *Ethics policy*. The Ethics policy shall:

(A) Require CMMC Ecosystem members to report to the Accreditation Body within 30 days of convictions, guilty pleas, or no contest pleas to crimes of fraud, larceny, embezzlement, misappropriation of funds, misrepresentation, perjury, false swearing, conspiracy to conceal, or a similar offense in any legal proceeding, civil or criminal, whether or not in connection with activities that relate to carrying out their role in the CMMC Ecosystem.

(B) Prohibit harassment or discrimination by CMMC Ecosystem members in all interactions with individuals whom they encounter in connection with their roles in the CMMC Ecosystem.

(C) Require CMMC Ecosystem members to have and maintain a satisfactory record of integrity and business ethics.

§ 170.9 CMMC Third-Party Assessment Organizations (C3PAOs).

(a) *Roles and responsibilities*. C3PAOs are organizations that are responsible for conducting Level 2 certification assessments and issuing Certificates of CMMC Status to OSCs based on the results. C3PAOs must be accredited or authorized by the Accreditation Body in accordance with the requirements set forth.

(b) *Requirements*. C3PAOs shall:

(1) Obtain authorization or accreditation from the Accreditation Body in accordance with §170.8(b)(3)(i) and (ii).

(2) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in §170.8(b)(17); and achieve and maintain compliance with ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2) within 27 months of authorization.

(3) Require all C3PAO company personnel participating in the Level 2 certification assessment process to complete a Tier 3 background investigation resulting in a determination of national security eligibility. This includes the CMMC Assessment Team and the quality assurance individual. This Tier 3 background investigation will not result in a security clearance and is not being executed for the purpose of government employment. The Tier 3 background investigation is initiated using the Standard Form (SF) 86 (*www.gsa.gov/reference/forms/questionnaire-for-national-security-positions*). These positions are designated as noncritical sensitive with a risk designation of ''Moderate Risk'' in accordance with 5 CFR 1400.201(b) and (d) and the investigative requirements of 5 CFR 731.106(c)(2).

(4) Require all C3PAO company personnel participating in the Level 2 certification assessment process who are not eligible to obtain a Tier 3 background investigation to meet the equivalent of a favorably adjudicated Tier 3 background investigation. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only.

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

(i) Completing and submitting Standard Form (SF) 328 (*www.gsa.gov/reference/forms/certificate-pertaining-to-foreign-interests*), *Certificate Pertaining to Foreign Interests*, upon request from DCSA and undergo a National Security Review with regards to the protection of controlled unclassified information based on the factors identified in 32 CFR 117.11(b) using the procedures outlined in 32 CFR 117.11(c).

(ii) Receiving a non-disqualifying eligibility determination from the CMMC PMO resulting from the FOCI risk assessment in order to proceed to a DCMA DIBCAC CMMC Level 2 assessment, as part of the authorization and accreditation process set forth in paragraph (b)(6) of this section.

(iii) Reporting any change to the information provided on its SF 328 by resubmitting the SF 328 to DCSA within 15 business days of the change being effective. A disqualifying eligibility determination, based on the results of the change, will result in the C3PAO losing its authorization or accreditation.

(6) Undergo a Level 2 certification assessment meeting all requirements for a Final Level 2 (C3PAO) in accordance with the procedures specified in

§170.17(a)(1) and (c), with the following exceptions:

(i) The assessment will be conducted by DCMA DIBCAC.

(ii) The assessment will not result in a CMMC Status of Level 2 (C3PAO) nor receive a Certificate of CMMC Status.

(7) Provide all documentation and records in English.

(8) Submit pre-assessment and planning material, final assessment reports, and CMMC certificates of assessment into the CMMC instantiation of eMASS.

(9) Unless disposition is otherwise authorized by the CMMC PMO, maintain all assessment related records for a period of six (6) years. Such records include any materials generated by the C3PAO in the course of an assessment, any working papers generated from Level 2 certification assessments; and materials relating to monitoring, education, training, technical knowledge, skills, experience, and authorization of all personnel involved in assessment activities; contractual agreements with OSCs; and organizations for whom consulting services were provided.

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

(11) Ensure that all personally identifiable information (PII) is encrypted and protected in all C3PAO information systems and databases.

(12) Meet the requirements for Assessment Team composition. An Assessment Team must include at least two people: a Lead CCA, as defined in §170.11(b)(10), and at least one other CCA. Additional CCAs and CCPs may also participate on an Assessment Team.

(13) Implement a quality assurance function that ensures the accuracy and completeness of assessment data prior to upload into the CMMC instantiation of eMASS. Any individual fulfilling the quality assurance function must be a CCA and cannot be a member of an Assessment Team for which they are performing a quality assurance role. A quality assurance individual shall manage the C3PAO's quality assurance reviews as defined in paragraph (b)(14) of this section and the appeals process as required by paragraphs (b)(19) and (20) of this section and in accordance with ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2) and ISO/IEC 17011:2017(E) (incorporated by reference, see §170.2).

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

(15) Ensure that all Level 2 certification assessment activities are performed on the information system within the CMMC Assessment Scope.

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

(17) Ensure that all assessment data and information uploaded into the CMMC instantiation of eMASS assessment data is compliant with the CMMC assessment data standard as set forth in eMASS CMMC Assessment Import Templates on the CMMC eMASS website: *https://cmmc.emass.apps.mil*. This system is accessible only to authorized users.

(18) Issue Certificates of CMMC Status to OSCs in accordance with the Level 2 certification assessment requirements set forth in §170.17, that include, at a minimum, all industry CAGE codes associated with the information systems addressed by the CMMC Assessment Scope, the C3PAO name, assessment unique identifier, the OSC name, and the CMMC Status date and level.

(19) Address all OSC appeals arising from Level 2 certification assessment activities. If the OSC or C3PAO is not satisfied with the result of the appeal either the OSC or the C3PAO can elevate the matter to the Accreditation Body for final determination.

(20) Submit assessment appeals, review records, and decision results of assessment appeals to DoD using the CMMC instantiation of eMASS.

§ 170.10 CMMC Assessor and Instructor Certification Organization (CAICO).

(a) *Roles and responsibilities.* The CAICO is responsible for training, testing, authorizing, certifying, and recertifying CMMC assessors, instructors, and related professionals. Only the CAICO may make decisions relating to examination certifications, including the granting, maintaining, recertifying, expanding, and reducing the scope of certification, and suspending or withdrawing certification in accordance with current ISO/IEC 17024:2012(E) (incorporated by reference, see §170.2). At any given point in time, there will be only one CAICO for the DoD CMMC Program.

(b) *Requirements.* The CAICO shall:

(1) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in §170.8(b)(17); and achieve and maintain ISO/IEC 17024(E) accreditation within 12 months of December 16, 2024.

(2) Provide all documentation and records in English.

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

(4) Ensure the instructor and assessor certification examinations are certified under ISO/IEC 17024:2012(E) (incorporated by reference, see §170.2), by a recognized US-based accreditor who is not a member of the CMMC Accreditation Body. The US-based accreditor must be a signatory to International Laboratory Accreditation Cooperation (ILAC) or relevant International Accreditation Forum (IAF) Mutual Recognition Arrangement (MRA) and must operate in accordance with ISO/IEC 17011:2017(E) (incorporated by reference, see §170.2).

(5) Establish quality control policies and procedures for the generation of training products, instruction, and testing materials.

(6) Oversee development, administration, and management pertaining to the quality of training and examination materials for CMMC assessor and instructor certification and recertification.

(7) Establish and publish an authorization and certification appeals process to receive, evaluate, and make decisions on complaints and appeals in accordance with ISO/IEC 17024:2012(E) (incorporated by reference, see §170.2).

(8) Address all appeals arising from the CCA, CCI, and CCP authorizations and certifications process through use of internal processes in accordance with ISO/IEC 17024:2012(E) (incorporated by reference, see §170.2).

(9) Maintain records for a period of six (6) years of all procedures, processes, and actions related to fulfillment of the requirements set forth in this section and provide the Accreditation Body access to those records.

(10) Provide the Accreditation Body information about the authorization and accreditation status of assessors, instructors, training community, and publishing partners.

(11) Ensure separation of duties between individuals involved in testing activities, training activities, and certification activities.

(12) Safeguard and require any CAICO training support service providers, as applicable, to safeguard the confidentiality of applicant, candidate, and certificate-holder information and ensure the overall security of the certification process.

(13) Ensure that all PII is encrypted and protected in all CAICO information systems and databases and those of any CAICO training support service providers.

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

(15) Neither disclose nor allow any CAICO training support service providers, as applicable, to disclose CMMC data or metrics related to authorization or certification activities to any entity other than the Accreditation Body and DoD, except as required by law.

(16) Require retraining and redesignation of PIs upon significant change to DoD's CMMC Program requirements. Require retraining and recertification of CCPs, CCAs, and CCIs upon significant change to DoD's CMMC Program

requirements, as determined by the DoD or the CAICO.

(17) Require CMMC Ecosystem members to report to the CAICO within 30 days of convictions, guilty pleas, or no contest pleas to crimes of fraud, larceny, embezzlement, misappropriation of funds, misrepresentation, perjury, false swearing, conspiracy to conceal, or a similar offense in any legal proceeding, civil or criminal, whether or not in connection with activities that relate to carrying out their role in the CMMC Ecosystem.

§ 170.11 CMMC Certified Assessor (CCA).

(a) *Roles and responsibilities.* CCAs, in support of a C3PAO, conduct Level 2 certification assessments of OSCs in accordance with NIST SP 800–171A Jun2018 (incorporated by reference, see §170.2), the assessment processes defined in §170.17, and the scoping requirements defined in §170.19(c). CCAs must meet all of the requirements set forth in paragraph (b) of this section. A CCA may conduct Level 2 certification assessments and participate on a C3PAO Assessment Team.

(b) *Requirements.* CCAs shall:

(1) Obtain and maintain certification from the CAICO in accordance with the requirements set forth in §170.10. Certification is valid for 3 years from the date of issuance.

(2) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in §170.8(b)(17).

(3) Complete a Tier 3 background investigation resulting in a determination of national security eligibility. This Tier 3 background investigation will not result in a security clearance and is not being executed for the purpose of government employment. The Tier 3 background investigation is initiated using the Standard Form (SF) 86 (*www.gsa.gov/reference/forms/questionnaire-for-national-security-positions*). These positions are designated as noncritical sensitive with a risk designation of ''Moderate Risk'' in accordance with 5 CFR 1400.201(b) and (d) and the investigative requirements of 5 CFR 731.106(c)(2).

(4) Meet the equivalent of a favorably adjudicated Tier 3 background investigation when not eligible for a Tier 3 background investigation. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only.

(5) Provide all documentation and records in English.

(6) Be a CCP who has at least 3 years of cybersecurity experience, at least 1 year of assessment or audit experience, and at least one foundational qualification, aligned to at least the Intermediate Proficiency Level of the DoD Cyberspace Workforce Framework's Security Control Assessor (612) Work Role, from DoD Manual 8140.03, *Cyberspace Workforce Qualification and Management Program* (*https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf*). Information on the Work Role 612 can be found at *https://public.cyber.mil/dcwf-work-role/security-control-assessor/*.

(7) Only use IT, cloud, cybersecurity services, and end-point devices provided by the authorized/accredited C3PAO that has been engaged to perform that OSA's Level 2 certification assessment and which has undergone a Level 2 certification assessment by DCMA DIBCAC (or higher) for all assessment activities. Individual assessors are prohibited from using any other IT, including IT that is personally owned, to include internal and external cloud services and end-point devices, to process, store, or transmit CMMC assessment reports or any other CMMC assessment-related information. The evaluation of assessment evidence within the OSC environment, using OSC tools, is permitted.

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

(9) Not share any information about an OSC obtained during CMMC pre-assessment and assessment activities with any person not involved with that specific assessment, except as otherwise required by law.

(10) Qualify as a Lead CCA by having at least 5 years of cybersecurity experience, 5 years of management experience, 3 years of assessment or audit experience, and at least one foundational

qualification aligned to Advanced Proficiency Level of the DoD Cyberspace Workforce Framework's Security Control Assessor (612) Work Role, from DoD Manual 8140.03, *Cyberspace Workforce Qualification and Management Program* (*https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf*). Information on the Work Role 612 can be found at *https://public.cyber.mil/dcwf-work-role/security-control-assessor/*.

§ 170.12 CMMC Instructor.

(a) *CMMC Provisional Instructor (PI) roles and responsibilities.* A CMMC Provisional Instructor (PI) teaches CCA and CCP candidates during the transitional period that ends 18 months after December 16, 2024. A PI is trained, tested, and designated to perform CMMC instructional duties by the CAICO to teach CCP and CCA candidates. PIs are designated by the CAICO after successful completion of the PI training and testing requirements set forth by the CAICO. A PI with a valid CCP certification may instruct CCP candidates, while a PI with a valid CCA certification may instruct CCP and CCA candidates. PIs are required to meet requirements in (c) of this section.

(b) *CMMC Certified Instructor (CCI) roles and responsibilities.* A CMMC Certified Instructor (CCI) teaches CCP, CCA, and CCI candidates and performs CMMC instructional duties. Candidate CCIs are certified by the CAICO after successful completion of the CCI training and testing requirements. A CCI is required to obtain and maintain assessor and instructor certifications from the CAICO in accordance with the requirements set forth in §170.10 and in paragraph (c) of this section. A CCI with a valid CCP certification may instruct CCP candidates, while a CCI with a valid CCA certification may instruct CCP, CCA, and CCI candidates. Certifications are valid for 3 years from the date of issuance. CCIs are required to meet requirements in paragraph (c) of this section.

(c) *Requirements.* CMMC Instructors shall:

(1) Obtain and maintain instructor designation or certification, as appropriate, from the CAICO in accordance with the requirements set forth in §170.10.

(2) Obtain and maintain CCP or CCA certification to deliver CCP training.

(3) Obtain and maintain a CCA certification to deliver CCA training.

(4) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in §170.8(b)(17).

(5) Provide all documentation and records in English.

(6) Provide the Accreditation Body and the CAICO annually with accurate information detailing their qualifications, training experience, professional affiliations, and certifications, and, upon reasonable request, submit documentation verifying this information.

(7) Not provide CMMC consulting services while serving as a CMMC instructor; however, subject to the Code of Professional Conduct and Conflict of Interest policies, can serve on an assessment team.

(8) Not participate in the development of exam objectives and/or exam content or act as an exam proctor while at the same time serving as a CCI.

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

(10) Not disclose any CMMC-related data or metrics that is PII, FCI, or CUI to anyone without prior coordination with and approval from DoD.

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

(12) Not share with anyone any CMMC training-related information not previously publicly disclosed.

§ 170.13 CMMC Certified Professional (CCP).

(a) *Roles and responsibilities.* A CMMC Certified Professional (CCP) completes rigorous training on CMMC and the assessment process to provide advice, consulting, and recommendations to their OSA clients. Candidate CCPs are certified by the CAICO after successful completion of the CCP training and testing requirements set forth in paragraph (b) of this section. CCPs are eligible to become CMMC Certified Assessors and can participate as a CCP on

Level 2 certification assessments with CCA oversight where the CCA makes all final determinations.

(b) *Requirements.* CCPs shall:

(1) Obtain and maintain certification from the CAICO in accordance with the requirements set forth in §170.10. Certification is valid for 3 years from the date of issuance.

(2) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics as set forth in §170.8(b)(17).

(3) Complete a Tier 3 background investigation resulting in a determination of national security eligibility. This Tier 3 background investigation will not result in a security clearance and is not being executed for the purpose of government employment. The Tier 3 background investigation is initiated using the Standard Form (SF) 86 (*www.gsa.gov/reference/forms/questionnaire-for-national-security-positions*). These positions are designated as noncritical sensitive with a risk designation of ''Moderate Risk'' in accordance with 5 CFR 1400.201(b) and (d) and the investigative requirements of 5 CFR 731.106(c)(2).

(4) Meet the equivalent of a favorably adjudicated Tier 3 background investigation when not eligible to obtain a Tier 3 background investigation. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only.

(5) Provide all documentation and records in English.

(6) Not share any information about an OSC obtained during CMMC pre-assessment and assessment activities with any person not involved with that specific assessment, except as otherwise required by law.

Subpart D—Key Elements of the CMMC Program

§170.14 CMMC Model.

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

(1) 48 CFR 52.204–21, *Basic Safeguarding of Covered Contractor Information Systems;*

(2) NIST SP 800–171 R2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (incorporated by reference, see §170.2); and

(3) Selected security requirements from NIST SP 800–172 Feb2021, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800–171* (incorporated by reference, see §170.2).

(b) *CMMC domains.* The CMMC Model consists of domains that map to the Security Requirement Families defined in NIST SP 800–171 R2 (incorporated by reference, see §170.2).

(c) *CMMC level requirements.* CMMC Levels 1–3 utilize the safeguarding requirements and security requirements specified in 48 CFR 52.204–21 (for Level 1), NIST SP 800–171 R2 (incorporated by reference, see §170.2) (for Level 2), and selected security requirements from NIST SP 800–172 Feb2021 (incorporated by reference, see §170.2) (for Level 3). This paragraph discusses the numbering scheme and the security requirements for each level.

(1) *Numbering.* Each security requirement has an identification number in the format—DD.L#-REQ—where:

(i) DD is the two-letter domain abbreviation;

(ii) L# is the CMMC level number; and

(iii) REQ is the 48 CFR 52.204–21 paragraph number, NIST SP 800–171 R2 requirement number, or NIST SP 800–172 Feb2021 requirement number.

(2) *CMMC Level 1 security requirements.* The security requirements in CMMC Level 1 are those set forth in 48 CFR 52.204–21(b)(1)(i) through (xv).

(3) *CMMC Level 2 security requirements.* The security requirements in CMMC Level 2 are identical to the requirements in NIST SP 800–171 R2.

(4) *CMMC Level 3 security requirements.* The security requirements in CMMC Level 3 are selected from NIST SP 800–172 Feb2021, and where applicable, Organization-Defined Parameters (ODPs) are assigned. Table 1 to this paragraph identifies the selected requirements and applicable ODPs that represent the CMMC Level 3 security requirements. ODPs for the NIST SP 800–172 Feb2021 requirements are italicized, where applicable:

TABLE 1 TO § 170.14(c)(4)

Security requirement No.*	CMMC Level 3 security requirements (selected NIST SP 800–172 Feb2021 security requirement with DoD ODPs italicized)
(i) AC.L3–3.1.2e	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.
(ii) AC.L3–3.1.3e	Employ *secure information transfer solutions* to control information flows between security domains on connected systems.
(iii) AT.L3–3.2.1e	Provide awareness training *upon initial hire, following a significant cyber event, and at least annually,* focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training *at least annually* or when there are significant changes to the threat.
(iv) AT.L3–3.2.2e	Include practical exercises in awareness training for *all users, tailored by roles, to include general users, users with specialized roles, and privileged users,* that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.
(v) CM.L3–3.4.1e	Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.
(vi) CM.L3–3.4.2e	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, *remove the components or place the components in a quarantine or remediation network* to facilitate patching, re-configuration, or other mitigations.
(vii) CM.L3–3.4.3e	Employ automated discovery and management tools to maintain an 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.

*Roman numerals in parentheses before the Security Requirement are for numbering purposes only. The numerals are not part of the naming convention for the requirement.

(d) *Implementation*. Assessment of security requirements is prescribed by NIST SP 800–171A Jun2018 (incorporated by reference, see §170.2) and NIST SP 800–172A Mar2022 (incorporated by reference, see §170.2). Descriptive text in these documents support OSA implementation of the security requirements and use the terms organization-defined and periodically. Except where referring to Organization-Defined Parameters (ODPs), organization-defined means as determined by the OSA. Periodically means occurring at regular intervals. As used in many requirements within CMMC, the interval length is organization-defined to provided contractor flexibility, with an interval length of no more than one year.

§ 170.15 CMMC Level 1 self-assessment and affirmation requirements.

(a) *Level 1 self-assessment*. To comply with CMMC Level 1 self-assessment requirements, the OSA must meet the requirements detailed in paragraphs (a)(1) and (2) of this section. An OSA conducts a Level 1 self-assessment as detailed in paragraph (c) of this section to achieve a CMMC Status of Final Level 1 (Self).

(1) *Level 1 self-assessment requirements*. The OSA must complete and achieve a MET result for all security requirements specified in §170.14(c)(2) to achieve the CMMC Status of Final Level 1 (Self). No POA&Ms are permitted for CMMC Level 1. The OSA must conduct a self-assessment in accordance with the procedures set forth in §170.15(c)(1) and submit assessment results in SPRS. To maintain compliance with the requirements for the CMMC Status of Final Level 1 (Self), the OSA must conduct a Level 1 self-assessment on an annual basis and submit the results in SPRS, or its successor capability.

(i) *Inputs to SPRS*. The Level 1 self-assessment results in the Supplier Performance Risk System (SPRS) shall include, at minimum, the following items:

(A) CMMC Level.

(B) CMMC Status Date.

(C) CMMC Assessment Scope.

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

(E) Compliance result.

(ii) [Reserved]

(2) *Affirmation*. Affirmation of the Level 1 (Self) CMMC Status is required for all Level 1 self-assessments. Affirmation procedures are set forth in §170.22.

(b) *Contract eligibility*. Prior to award of any contract or subcontract with a requirement for the CMMC Status of Level 1 (Self), OSAs must both achieve a CMMC Status of Level 1 (Self) and have submitted an affirmation of compliance into SPRS for all information systems within the CMMC Assessment Scope.

(c) *Procedures*—(1) *Level 1 self-assessment*. The OSA must conduct a Level 1 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) The Level 1 self-assessment must be performed using the objectives defined in NIST SP 800–171A Jun2018 (incorporated by reference, see §170.2) for the security requirement that maps to the CMMC Level 1 security requirement as specified in table 1 to paragraph (c)(1)(ii) of this section. In any case where an objective addresses CUI, FCI should be substituted for CUI in the objective.

(ii) Mapping table for CMMC Level 1 security requirements to the NIST SP 800–171A Jun2018 objectives.

TABLE 2 TO §170.15(c)(1)(ii)—CMMC LEVEL 1 SECURITY REQUIREMENTS MAPPED TO NIST SP 800–171A JUN2018

CMMC Level 1 security requirements as set forth in §170.14(c)(2)	NIST SP 800–171A Jun2018
AC.L1–b.1.i	3.1.1
AC.L1–b.1.ii	3.1.2
AC.L1–b.1.iii	3.1.20
AC.L1–b.1.iv	3.1.22

TABLE 2 TO § 170.15(c)(1)(ii)—CMMC LEVEL 1 SECURITY REQUIREMENTS MAPPED TO NIST SP 800–171A JUN2018—Continued

CMMC Level 1 security requirements as set forth in § 170.14(c)(2)	NIST SP 800–171A Jun2018
IA.L1–b.1.v	3.5.1
IA.L1–b.1.vi	3.5.2
MP.L1–b.1.vii	3.8.3
PE.L1–b.1.viii	3.10.1
First phrase of PE.L1–b.1.ix (FAR b.1.ix*)	3.10.3
Second phrase of PE.L1–b.1.ix (FAR b.1.ix*)	3.10.4
Third phrase of PE.L1–b.1.ix (FAR b.1.ix*)	3.10.5
SC.L1–b.1.x	3.13.1
SC.L1–b.1.xi	3.13.5
SI.L1–b.1.xii	3.14.1
SI.L1–b.1.xiii	3.14.2
SI.L1–b.1.xiv	3.14.4
SI.L1–b.1.xv	3.14.5

*Three of the 48 CFR 52.204–21 requirements were broken apart by "phrase" when NIST SP 800–171 R2 was developed.

(iii) Additional guidance can be found in the guidance document listed in paragraph (b) of appendix A to this part.

(2) *Artifact retention*. The artifacts used as evidence for the assessment must be retained by the OSA for six (6) years from the CMMC Status Date.

§ 170.16 CMMC Level 2 self-assessment and affirmation requirements.

(a) *Level 2 self-assessment*. To comply with Level 2 self-assessment requirements, the OSA must meet the requirements detailed in paragraphs (a)(1) and (2) of this section. An OSA conducts a Level 2 self-assessment as detailed in paragraph (c) of this section to achieve a CMMC Status of either Conditional or Final Level 2 (Self). Achieving a CMMC Status of Level 2 (Self) also satisfies the requirements for a CMMC Status of Level 1 (Self) detailed in § 170.15 for the same CMMC Assessment Scope.

(1) *Level 2 self-assessment requirements*. The OSA must complete and achieve a MET result for all security requirements specified in § 170.14(c)(3) to achieve the CMMC Status of Level 2 (Self). The OSA must conduct a self-assessment in accordance with the procedures set forth in paragraph (c)(1) of this section and submit assessment results in Supplier Performance Risk System (SPRS). To maintain compliance with the requirements for a CMMC Status of Level 2 (Self), the OSA must conduct a Level 2 self-assessment every three years and submit the results in SPRS, within three years of the CMMC Status Date associated with the Conditional Level 2 (Self).

(i) *Inputs to SPRS*. The Level 2 self-assessment results in the SPRS shall include, at minimum, the following information:

(A) CMMC Level.

(B) CMMC Status Date.

(C) CMMC Assessment Scope.

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

(E) Overall Level 2 self-assessment score (*e.g.*, 105 out of 110).

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

(ii) *Conditional Level 2 (Self)*. The OSA has achieved the CMMC Status of Conditional Level 2 (Self) if the Level 2 self-assessment results in a POA&M and the POA&M meets all the CMMC Level 2 POA&M requirements listed in § 170.21(a)(2).

(A) *Plan of Action and Milestones*. A Level 2 POA&M is allowed only in accordance with the CMMC POA&M requirements listed in § 170.21.

(B) *POA&M closeout*. The OSA must remediate any NOT MET requirements, must perform a POA&M closeout self-assessment, and must post compliance results to SPRS within 180 days of the CMMC Status Date associated with the Conditional Level 2 (Self). If the POA&M is not successfully closed out within the 180-day timeframe, the Conditional Level 2 (Self) CMMC Status for the information system will expire. If

Conditional Level 2 (Self) CMMC Status expires within the period of performance of a contract, standard contractual remedies will apply, and the OSA will be ineligible for additional awards with a requirement for the CMMC Status of Level 2 (Self), or higher requirement, for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(iii) *Final Level 2 (Self).* The OSA has achieved the CMMC Status of Final Level 2 (Self) if the Level 2 self-assessment results in a passing score as defined in §170.24. This score may be achieved upon initial self-assessment or as the result of a POA&M closeout self-assessment, as applicable.

(iv) *CMMC Status investigation.* The DoD reserves the right to conduct a DCMA DIBCAC assessment of the OSA, as provided for under the 48 CFR 252.204–7020. If the investigative results of a subsequent DCMA DIBCAC assessment show that adherence to the provisions of this part have not been achieved or maintained, these DCMA DIBCAC results will take precedence over any pre-existing CMMC Status. At that time, standard contractual remedies will be available and the OSA will be ineligible for additional awards with CMMC Status requirement of Level 2 (Self), or higher requirement, for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(2) *Affirmation.* Affirmation of the Level 2 (Self) CMMC Status is required for all Level 2 self-assessments at the time of each assessment, and annually thereafter. Affirmation procedures are set forth in §170.22.

(b) *Contract eligibility.* Prior to award of any contract or subcontract with requirement for CMMC Status of Level 2 (Self), the following two requirements must be met:

(1) The OSA must achieve, as specified in paragraph (a)(1) of this section, a CMMC Status of either Conditional Level 2 (Self) or Final Level 2 (Self).

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

(c) *Procedures*—(1) *Level 2 self-assessment of the OSA.* The OSA must conduct a Level 2 self-assessment in accordance with NIST SP 800–171A Jun2018 (incorporated by reference, see §170.2) and the CMMC Level 2 scoping requirements set forth in §§170.19(a) and (c) for the information systems within the CMMC Assessment Scope. The Level 2 self-assessment must be scored in accordance with the CMMC Scoring Methodology described in §170.24 and the OSA must upload the results into SPRS. If a POA&M exists, a POA&M closeout self-assessment must be performed by the OSA when all NOT MET requirements have been remediated. The POA&M closeout self-assessment must be performed within 180-days of the Conditional CMMC Status Date. Additional guidance can be found in the guidance document listed in paragraph (c) of appendix A to this part.

(2) *Level 2 self-assessment with the use of Cloud Service Provider (CSP).* An OSA may use a cloud environment to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 2 (Self) under the following circumstances:

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

(ii) The CSP product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline. FedRAMP Moderate or FedRAMP Moderate equivalent is in accordance with DoD Policy.

(iii) In accordance with §170.19(c)(2), the OSA's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the Customer Responsibility Matrix (CRM) must be documented or referred to in the OSA's System Security Plan (SSP).

(3) *Level 2 self-assessment with the use of an External Service Provider (ESP), not a CSP.* An OSA may use an ESP that is not a CSP to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for

the CMMC Status of Level 2 (Self) under the following circumstances:

(i) The use of the ESP, its relationship to the OSA, and the services provided are documented in the OSA's SSP and described in the ESP's service description and CRM.

(ii) The ESP services used to meet OSA requirements are assessed within the scope of the OSA's assessment against all Level 2 security requirements.

(iii) In accordance with §170.19(c)(2), the OSA's on-premises infrastructure connecting to the ESP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSA's SSP.

(4) *Artifact retention.* The artifacts used as evidence for the assessment must be retained by the OSA for six (6) years from the CMMC Status Date.

§ 170.17 CMMC Level 2 certification assessment and affirmation requirements.

(a) *Level 2 certification assessment.* To comply with Level 2 certification assessment requirements, the OSC must meet the requirements set forth in paragraphs (a)(1) and (2) of this section. An OSC undergoes a Level 2 certification assessment as detailed in paragraph (c) of this section to achieve a CMMC Status of either Conditional or Final Level 2 (C3PAO). Achieving a CMMC Status of Level 2 (C3PAO) also satisfies the requirements for a CMMC Statuses of Level 1 (Self) and Level 2 (Self) set forth in §§170.15 and 170.16 respectively for the same CMMC Assessment Scope.

(1) *Level 2 certification assessment requirements.* The OSC must complete and achieve a MET result for all security requirements specified in §170.14(c)(3) to achieve the CMMC Status of Level 2 (C3PAO). The OSC must obtain a Level 2 certification assessment from an authorized or accredited C3PAO following the procedures outlined in paragraph (c) of this section. The C3PAO must submit the Level 2 certification assessment results into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS. To maintain compliance with the requirements for a CMMC Status of Level 2 (C3PAO), the Level 2 certification assessment must be completed within three years of the CMMC Status Date associated with the Conditional Level 2 (C3PAO).

(i) *Inputs into the CMMC instantiation of eMASS.* The Level 2 certification assessment results input into the CMMC instantiation of eMASS shall include, at minimum, the following information:

(A) Date and level of the assessment.

(B) C3PAO name.

(C) Assessment unique identifier.

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

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

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

(G) CMMC Status Date.

(H) Assessment result for each requirement objective.

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

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

(ii) *Conditional Level 2 (C3PAO).* The OSC has achieved the CMMC Status of Conditional Level 2 (C3PAO) if the Level 2 certification assessment results in a POA&M and the POA&M meets all CMMC Level 2 POA&M requirements listed in §170.21(a)(2).

(A) *Plan of Action and Milestones.* A Level 2 POA&M is allowed only in accordance with the CMMC POA&M requirements listed in §170.21.

(B) *POA&M closeout.* The OSC must remediate any NOT MET requirements, must undergo a POA&M closeout certification assessment from a C3PAO, and the C3PAO must post compliance results into the CMMC instantiation of eMASS within 180 days of the CMMC Status Date associated with the Conditional Level 2 (C3PAO). If the POA&M is not successfully closed out within the 180-day timeframe, the Conditional Level 2 (C3PAO) CMMC Status for the information system will expire. If Conditional Level 2 (C3PAO) CMMC Status

expires within the period of performance of a contract, standard contractual remedies will apply, and the OSC will be ineligible for additional awards with a requirement for the CMMC Status of Level 2 (C3PAO), or higher requirement, for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(iii) *Final Level 2 (C3PAO).* The OSC has achieved the CMMC Status of Final Level 2 (C3PAO) if the Level 2 certification assessment results in a passing score as defined in §170.24. This score may be achieved upon initial certification assessment or as the result of a POA&M closeout certification assessment, as applicable.

(iv) *CMMC Status investigation.* The DoD reserves the right to conduct a DCMA DIBCAC assessment of the OSC, as provided for under the 48 CFR 252.204–7020. If the investigative results of a subsequent DCMA DIBCAC assessment show that adherence to the provisions of this part have not been achieved or maintained, these DCMA DIBCAC results will take precedence over any pre-existing CMMC Status. At that time, standard contractual remedies will be available and the OSC will be ineligible for additional awards with CMMC Status requirement of Level 2 (C3PAO), or higher requirement, for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(2) *Affirmation.* Affirmation of the Level 2 (C3PAO) CMMC Status is required for all Level 2 certification assessments at the time of each assessment, and annually thereafter. Affirmation procedures are provided in §170.22.

(b) *Contract eligibility.* Prior to award of any contract or subcontract with a requirement for the CMMC Status of Level 2 (C3PAO), the following two requirements must be met:

(1) The OSC must achieve, as specified in paragraph (a)(1) of this section, a CMMC Status of either Conditional Level 2 (C3PAO) or Final Level 2 (C3PAO).

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

(c) *Procedures*—(1) *Level 2 certification assessment of the OSC.* An authorized or accredited C3PAO must perform a Level 2 certification assessment in accordance with NIST SP 800–171A Jun2018 (incorporated by reference, see §170.2) and the CMMC Level 2 scoping requirements set forth in §170.19(a) and (c) for the information systems within the CMMC Assessment Scope. The Level 2 certification assessment must be scored in accordance with the CMMC Scoring Methodology described in §170.24 and the C3PAO must upload the results into the CMMC instantiation of eMASS. Final results are communicated to the OSC through a CMMC Assessment Findings Report.

(2) *Security requirement re-evaluation.* A security requirement that is NOT MET (as defined in §170.24) may be re-evaluated during the course of the Level 2 certification assessment and for 10 business days following the active assessment period if all of the following conditions exist:

(i) Additional evidence is available to demonstrate the security requirement has been MET;

(ii) Cannot change or limit the effectiveness of other requirements that have been scored MET; and

(iii) The CMMC Assessment Findings Report has not been delivered.

(3) *POA&M.* If a POA&M exists, a POA&M closeout certification assessment must be performed by a C3PAO within 180-days of the Conditional CMMC Status Date. Additional guidance can be found in §170.21 and in the guidance document listed in paragraph (c) of appendix A to this part.

(4) *Artifact retention and integrity.* The hashed artifacts used as evidence for the assessment must be retained by the OSC for six (6) years from the CMMC Status Date. To ensure that the artifacts have not been altered, the OSC must hash the artifact files using a NIST-approved hashing algorithm. The OSC must provide the C3PAO with a list of the artifact names, the return value of the hashing algorithm, and the hashing algorithm for upload into the CMMC instantiation of eMASS. Additional guidance for hashing artifacts can be found in the guidance document listed in paragraph (h) of appendix A to this part.

(5) *Level 2 certification assessment with the use of Cloud Service Provider (CSP).* An OSC may use a cloud environment to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 2 (C3PAO) under the following circumstances:

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

(ii) The CSP product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline. FedRAMP Moderate or FedRAMP Moderate equivalent is in accordance with DoD Policy.

(iii) In accordance with §170.19(c)(2), the OSC's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope. As such, the security requirements from the CRM must be documented or referred to in the OSC's SSP.

(6) *Level 2 certification assessment with the use of an External Service Provider (ESP), not a CSP.* An OSA may use an ESP that is not a CSP to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 2 (C3PAO) under the following circumstances:

(i) The use of the ESP, its relationship to the OSA, and the services provided are documented in the OSA's SSP and described in the ESP's service description and customer responsibility matrix.

(ii) The ESP services used to meet OSA requirements are assessed within the scope of the OSA's assessment against all Level 2 security requirements.

(iii) In accordance with §170.19(c)(2), the OSA's on-premises infrastructure connecting to the ESP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSA's SSP.

§ 170.18 CMMC Level 3 certification assessment and affirmation requirements.

(a) *Level 3 certification assessment.* To comply with Level 3 certification assessment requirements, the OSC must meet the requirements set forth in paragraphs (a)(1) and (2) of this section. An OSC undergoes a Level 3 certification assessment as detailed in paragraph (c) of this section to achieve a CMMC Status of either Conditional or Final Level 3 (DIBCAC). A CMMC Status of Final Level 2 (C3PAO) for information systems within the Level 3 CMMC Assessment Scope is a prerequisite to undergo a Level 3 certification assessment. CMMC Level 3 recertification also has a prerequisite for a new CMMC Level 2 assessment. Achieving a CMMC Status of Level 3 (DIBCAC) also satisfies the requirements for CMMC Statuses of Level 1 (Self), Level 2 (Self), and Level 2 (C3PAO) set forth in §§170.15 through 170.17 respectively for the same CMMC Assessment Scope.

(1) *Level 3 certification assessment requirements.* The OSC must achieve a CMMC Status of Final Level 2 (C3PAO) on the Level 3 CMMC Assessment Scope, as defined in §170.19(d), prior to initiating a Level 3 certification assessment, which will be performed by DCMA DIBCAC (*www.dcma.mil/DIBCAC*) on behalf of the DoD. The OSC must complete and achieve a MET result for all security requirements specified in table 1 to §170.14(c)(4) to achieve the CMMC Status of Level 3 (DIBCAC). DCMA DIBCAC will submit the Level 3 certification assessment results into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS. To maintain compliance with the requirements for a CMMC Status of Level 3 (DIBCAC), the Level 3 certification assessment must be performed every three years for all information systems within the Level 3 CMMC Assessment Scope. In addition, given that compliance with Level 2 requirements is a prerequisite for applying for CMMC Level 3, a Level 2 (C3PAO) certification assessment must also be conducted every three years to maintain CMMC

Level 3 (DIBCAC) status. Level 3 certification assessment must be completed within three years of the CMMC Status Date associated with the Final Level 3 (DIBCAC) or, if there was a POA&M, then within three years of the CMMC Status Date associated with the Conditional Level 3 (DIBCAC).

(i) *Inputs into the CMMC instantiation of eMASS.* The Level 3 certification assessment results input into the CMMC instantiation of eMASS shall include, at minimum, the following items:

(A) Date and level of the assessment.

(B) For each Assessor(s) conducting the assessment, name and government organization information.

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

(D) The name, date, and version of the system security plan(s) (SSP).

(E) CMMC Status Date.

(F) Result for each security requirement objective.

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

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

(ii) *Conditional Level 3 (DIBCAC).* The OSC has achieved the CMMC Status of Conditional Level 3 (DIBCAC) if the Level 3 certification assessment results in a POA&M and the POA&M meets all CMMC Level 3 POA&M requirements listed in §170.21(a)(3).

(A) *Plan of Action and Milestones.* A Level 3 POA&M is allowed only in accordance with the CMMC POA&M requirements listed in §170.21.

(B) *POA&M closeout.* The OSC must remediate any NOT MET requirements, must undergo a POA&M closeout certification assessment from DCMA DIBCAC, and DCMA DIBCAC must post compliance results into the CMMC instantiation of eMASS within 180 days of the CMMC Status Date associated with the Conditional Level 3 (DIBCAC). If the POA&M is not successfully closed out within the 180-day timeframe, the Conditional Level 3 (DIBAC) CMMC Status for the information system will expire. If Conditional Level 3 (DIBCAC) CMMC Status expires within the period of performance of a contract, standard contractual remedies will apply, and the OSC will be ineligible for additional awards with a requirement for the CMMC Status of Level 3 (DIBCAC) for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(iii) *Final Level 3 (DIBCAC).* The OSC has achieved the CMMC Status of Final Level 3 (DIBCAC) if the Level 3 certification assessment results in a passing score as defined in §170.24. This score may be achieved upon initial certification assessment or as the result of a POA&M closeout certification assessment, as applicable.

(iv) *CMMC Status investigation.* The DoD reserves the right to conduct a DCMA DIBCAC assessment of the OSC, as provided for under the 48 CFR 252.204–7020. If the investigative results of a subsequent DCMA DIBCAC assessment show that adherence to the provisions of this part have not been achieved or maintained, these DCMA DIBCAC results will take precedence over any pre-existing CMMC Status. At that time, standard contractual remedies will be available and the OSC will be ineligible for additional awards with CMMC Status requirement of Level 3 (DIBCAC) for the information system within the CMMC Assessment Scope until such time as a new CMMC Status is achieved.

(2) *Affirmation.* Affirmation of the Level 3 (DIBCAC) CMMC Status is required for all Level 3 certification assessments at the time of each assessment, and annually thereafter. Affirmation procedures are provided in §170.22.

(b) *Contract eligibility.* Prior to award of any contract or subcontract with requirement for CMMC Status of Level 3 (DIBCAC), the following two requirements must be met:

(1) The OSC must achieve, as specified in paragraph (a)(1) of this section, a CMMC Status of either Conditional Level 3 (DIBCAC) or Final Level 3 (DIBCAC).

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

(c) *Procedures*—(1) *Level 3 certification assessment of the OSC.* The CMMC Level 3 certification assessment process includes:

(i) *Final Level 2 (C3PAO).* The OSC must achieve a CMMC Status of Final Level 2 (C3PAO) for information systems within the Level 3 CMMC Assessment Scope prior to the CMMC Level 3 certification assessment. The CMMC Assessment Scope for the Level 3 certification assessment must be equal to, or a subset of, the CMMC Assessment Scope associated with the OSC's Final Level 2 (C3PAO). Asset requirements differ for each CMMC Level. Scoping differences are set forth in §170.19.

(ii) *Initiating the Final Level 3 (DIBCAC).* The OSC (including ESPs that voluntarily elect to undergo a Level 3 certification assessment) initiates a Level 3 certification assessment by emailing a request to DCMA DIBCAC point of contact found at *www.dcma.mil/DIBCAC*. The request must include the Level 2 certification assessment unique identifier. DCMA DIBCAC will validate the OSC has achieved a CMMC Status of Level 2 (C3PAO) and will contact the OSC to schedule their Level 3 certification assessment.

(iii) *Conducting the Final Level 3 (DIBCAC).* DCMA DIBCAC will perform a Level 3 certification assessment in accordance with NIST SP 800–171A Jun2018 (incorporated by reference, see §170.2) and NIST SP 800–172A Mar2022 (incorporated by reference, see §170.2) and the CMMC Level 3 scoping requirements set forth in §170.19(d) for the information systems within the CMMC Assessment Scope. The Level 3 certification assessment will be scored in accordance with the CMMC Scoring Methodology set forth in §170.24 and DCMA DIBCAC will upload the results into the CMMC instantiation of eMASS. Final results are communicated to the OSC through a CMMC Assessment Findings Report. For assets that changed asset category (*i.e.*, CRMA to CUI Asset) or assessment requirements (*i.e.*, Specialized Assets) between the Level 2 and Level 3 certification assessments, DCMA DIBCAC will perform limited checks of Level 2 security requirements. If the OSC had these upgraded asset categories included in their Level 2 certification assessment, then DCMA DIBCAC may still perform limited checks for compliance. If DCMA DIBCAC identifies that a Level 2 security requirement is NOT MET, the Level 3 assessment process may be paused to allow for remediation, placed on hold, or immediately terminated.

(2) *Security requirement re-evaluation.* A security requirement that is NOT MET (as defined in §170.24) may be re-evaluated during the course of the Level 3 certification assessment and for 10 business days following the active assessment period if all of the following conditions exist:

(i) Additional evidence is available to demonstrate the security requirement has been MET;

(ii) The additional evidence does not materially impact previously assessed security requirements; and

(iii) The CMMC Assessment Findings Report has not been delivered.

(3) *POA&M.* If a POA&M exists, a POA&M closeout certification assessment will be performed by DCMA DIBCAC within 180-days of the Conditional CMMC Status Date. Additional guidance is located in §170.21 and in the guidance document listed in paragraph (d) of appendix A to this part.

(4) *Artifact retention and integrity.* The hashed artifacts used as evidence for the assessment must be retained by the OSC for six (6) years from the CMMC Status Date. The hashed artifacts used as evidence for the assessment must be retained by the OSC for six (6) years from the CMMC Status Date. To ensure that the artifacts have not been altered, the OSC must hash the artifact files using a NIST-approved hashing algorithm. Assessors will collect the list of the artifact names, the return value of the hashing algorithm, and the hashing algorithm used and upload that data into the CMMC instantiation of eMASS. Additional guidance for hashing artifacts can be found in the guidance document listed in paragraph (h) of appendix A to this part.

(5) *Level 3 certification assessment with the use of Cloud Service Provider (CSP).* An OSC may use a cloud environment to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 3 (DIBCAC) under the following circumstances:

(i) The OSC may utilize a CSP product or service offering that meets the

FedRAMP Moderate (or higher) baseline. If the CSP's product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline, the product or service offering must meet security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline in accordance with DoD Policy.

(ii) Use of a CSP does not relieve an OSC of its obligation to implement the 24 Level 3 security requirements. These 24 requirements apply to every environment where the CUI data is processed, stored, or transmitted, when Level 3 (DIBCAC) is the designated CMMC Status. If any of these 24 requirements are inherited from a CSP, the OSC must demonstrate that protection during a Level 3 certification assessment via a Customer Implementation Summary/Customer Responsibility Matrix (CIS/CRM) and associated Body of Evidence (BOE). The BOE must clearly indicate whether the OSC or the CSP is responsible for meeting each requirement and which requirements are implemented by the OSC versus inherited from the CSP.

(iii) In accordance with §170.19(d)(2), the OSC's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope. As such, the security requirements from the CRM must be documented or referred to in the OSC's SSP.

(6) *Level 3 certification assessment with the use of an ESP, not a CSP.* An OSC may use an ESP that is not a CSP to process, store, or transmit CUI in performance of a contract or subcontract with a requirement for the CMMC Status of Level 3 (DIBCAC) under the following circumstances:

(i) The use of the ESP, its relationship to the OSC, and the services provided are documented in the OSC's SSP and described in the ESP's service description and customer responsibility matrix.

(ii) The ESP services used to meet OSC requirements are assessed within the scope of the OSC's assessment against all Level 2 and Level 3 security requirements.

(iii) In accordance with §170.19(d)(2), the OSC's on-premises infrastructure connecting to the ESP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSC's SSP.

§170.19 CMMC scoping.

(a) *Scoping requirement.* (1) The CMMC Assessment Scope must be specified prior to assessment in accordance with the requirements of this section. The CMMC Assessment Scope is the set of all assets in the OSA's environment that will be assessed against CMMC security requirements.

(2) The requirements for defining the CMMC Assessment Scope for CMMC Levels 1, 2, and 3 are set forth in this section. Additional guidance regarding scoping can be found in the guidance documents listed in paragraphs (e) through (g) of appendix A to this part.

(b) *CMMC Level 1 scoping.* Prior to performing a Level 1 self-assessment, the OSA must specify the CMMC Assessment Scope.

(1) *Assets in scope for Level 1 self-assessment.* OSA information systems which process, store, or transmit FCI are in scope for CMMC Level 1 and must be self-assessed against applicable CMMC security requirements.

(2) *Assets not in scope for Level 1 self-assessment*—(i) *Out-of-Scope Assets.* OSA information systems which do not process, store, or transmit FCI are outside the scope for CMMC Level 1. An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of FCI beyond the Keyboard/Video/Mouse sent to the VDI client is considered out-of-scope. There are no documentation requirements for out-of-scope assets.

(ii) *Specialized Assets.* Specialized Assets are those assets that can process, store, or transmit FCI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment. Specialized Assets are not part of the Level 1 CMMC Assessment Scope and are not assessed against CMMC security requirements.

(3) *Level 1 self-assessment scoping considerations*. To scope a Level 1 self-assessment, OSAs should consider the people, technology, facilities, and External Service Providers (ESP) within its environment that process, store, or transmit FCI.

(c) *CMMC Level 2 Scoping*. Prior to performing a Level 2 self-assessment or Level 2 certification assessment, the OSA must specify the CMMC Assessment Scope.

(1) The CMMC Assessment Scope for CMMC Level 2 is based on the specification of asset categories and their respective requirements as defined in table 3 to this paragraph (c)(1). Additional information is available in the guidance document listed in paragraph (f) of appendix A to this part.

TABLE 3 TO § 170.19(c)(1)—CMMC LEVEL 2 ASSET CATEGORIES AND ASSOCIATED REQUIREMENTS

Asset category	Asset description	OSA requirements	CMMC assessment requirements
Assets that are in the Level 2 CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets.	• Assets that process, store, or transmit CUI.	• Document in the asset inventory. • Document asset treatment in the System Security Plan (SSP). • Document in the network diagram of the CMMC Assessment Scope. • Prepare to be assessed against CMMC Level 2 security requirements.	• Assess against all Level 2 security requirements.
Security Protection Assets	• Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope.	• Document in the asset inventory. • Document asset treatment in SSP. • Document in the network diagram of the CMMC Assessment Scope. • Prepare to be assessed against CMMC Level 2 security requirements.	• Assess against Level 2 security requirements that are relevant to the capabilities provided.

TABLE 3 TO § 170.19(c)(1)—CMMC LEVEL 2 ASSET CATEGORIES AND ASSOCIATED REQUIREMENTS—Continued

Asset category	Asset description	OSA requirements	CMMC assessment 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 asset treatment in the SSP.
		• Document in the network diagram of the CMMC Assessment Scope.
		• Prepare to be assessed against CMMC Level 2 security requirements.
			• Review the SSP:
			  • If sufficiently documented, do not assess against other CMMC security requirements, except as noted.
			  • If OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies.
			  • The limited check(s) shall not materially increase the assessment duration nor the assessment cost.
			  • The limited check(s) will be assessed against CMMC security requirements.

Specialized Assets	• Assets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment.	• Document in the asset inventory. • Document asset treatment in the SSP. • Show these assets are managed using the contractor's risk-based security policies, procedures, and practices. • Document in the network diagram of the CMMC Assessment Scope.	• Review the SSP. • Do not assess against other CMMC security requirements.
Assets that are not in the Level 2 CMMC Assessment Scope			
Out-of-Scope Assets	• Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets.	• Prepare to justify the inability of an Out-of-Scope Asset to process, store, or transmit CUI.	• None.

TABLE 3 TO § 170.19(c)(1)—CMMC LEVEL 2 ASSET CATEGORIES AND ASSOCIATED REQUIREMENTS—Continued

Asset category	Asset description	OSA requirements	CMMC assessment requirements
	• Assets that are physically or logically separated from CUI assets. • Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset. • An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset.		

(2)(i) Table 4 to this paragraph (c)(2)(i) defines the requirements to be met when utilizing an External Service Provider (ESP). The OSA must consider whether the ESP is a Cloud Service Provider (CSP) and whether the ESP processes, stores, or transmits CUI and/or Security Protection Data (SPD).

TABLE 4 TO § 170.19(c)(2)(i)—ESP SCOPING REQUIREMENTS

When the ESP processes, stores, or transmits:	When utilizing an ESP that is:	
	A CSP	Not a CSP
CUI (with or without SPD)	The CSP shall meet the FedRAMP requirements in 48 CFR 252.204–7012.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as part of the OSA's assessment.
SPD (without CUI)	The services provided by the CSP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.
Neither CUI nor SPD	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.

(ii) The use of an ESP, its relationship to the OSA, and the services provided need to be documented in the OSA's SSP and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSA and ESP with respect to the services provided. Note that the ESP may voluntarily undergo a CMMC certification assessment to reduce the ESP's effort required during the OSA's assessment. The minimum assessment type for the ESP is dictated by the OSA's DoD contract requirement.

(d) *CMMC Level 3 scoping*. Prior to performing a Level 3 certification assessment, the CMMC Assessment Scope must be specified.

(1) The CMMC Assessment Scope for Level 3 is based on the specification of asset categories and their respective requirements as set forth in table 5 to this paragraph (d)(1). Additional information is available in the guidance

document listed in paragraph (g) of appendix A to this part.

TABLE 5 TO § 170.19(d)(1)—CMMC LEVEL 3 ASSET CATEGORIES AND ASSOCIATED REQUIREMENTS

Asset category	Asset description	OSC requirements	CMMC assessment requirements
Assets that are in the Level 3 CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets.	• Assets that process, store, or transmit CUI. • Assets that can, but are not intended to, process, store, or transmit CUI (defined as Contractor Risk Managed Assets in table 1 to paragraph (c)(1) of this section CMMC Scoping).	• Document in the asset inventory. • Document asset treatment in the System Security Plan (SSP). • Document in the network diagram of the CMMC Assessment Scope. • Prepare to be assessed against CMMC Level 2 and Level 3 security requirements.	• Limited check against Level 2 and assess against all Level 3 CMMC security requirements.
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 asset treatment in the SSP. • Document in the network diagram of the CMMC Assessment Scope. • Prepare to be assessed against CMMC Level 2 and Level 3 security requirements.	• Limited check against Level 2 and assess against all Level 3 CMMC security requirements that are relevant to the capabilities provided.
Specialized Assets	• Assets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment.	• Document in the asset inventory. • Document asset treatment in the SSP. • Document in the network diagram of the CMMC Assessment Scope. • Prepare to be assessed against CMMC Level 2 and Level 3 security requirements.	• Limited check against Level 2 and assess against all Level 3 CMMC security requirements. • Intermediary devices are permitted to provide the capability for the specialized asset to meet one or more CMMC security requirements.
Assets that are not in the Level 3 CMMC Assessment Scope			
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 process, store, or transmit CUI.	• None.

TABLE 5 TO § 170.19(d)(1)—CMMC LEVEL 3 ASSET CATEGORIES AND ASSOCIATED REQUIREMENTS—Continued

Asset category	Asset description	OSC requirements	CMMC assessment requirements
	• Assets that are physically or logically separated from CUI assets. • Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset. • An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset.		

(2)(i) Table 6 to this paragraph (d)(2)(i) defines the requirements to be met when utilizing an External Service Provider (ESP). The OSA must consider whether the ESP is a Cloud Service Provider (CSP) and whether the ESP processes, stores, or transmits CUI and/or Security Protection Data (SPD).

TABLE 6 TO § 170.19(d)(2)(i)—ESP SCOPING REQUIREMENTS

When the ESP processes, stores, or transmits:	When utilizing an ESP that is:	
	A CSP	Not a CSP
CUI (with or without SPD)	The CSP shall meet the FedRAMP requirements in 48 CFR 252.204–7012.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as part of the OSA's assessment.
SPD (without CUI)	The services provided by the CSP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.
Neither CUI nor SPD	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.

(ii) The use of an ESP, its relationship to the OSC, and the services provided need to be documented in the OSC's SSP and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSC and ESP with respect to the services provided. Note that the ESP may voluntarily undergo a CMMC certification assessment to reduce the ESP's effort required during the OSA's assessment. The minimum. The minimum assessment type for the ESP is dictated by the OSC's DoD contract requirement.

(e) *Relationship between Level 2 and Level 3 CMMC Assessment Scope.* The Level 3 CMMC Assessment Scope must be equal to or a subset of the Level 2 CMMC Assessment Scope in accordance with § 170.18(a) (*e.g.*, a Level 3 data enclave with greater restrictions and protections within a Level 2 data enclave). Any Level 2 POA&M items must be closed prior to the initiation of the Level 3 certification assessment.

DCMA DIBCAC may check any Level 2 security requirement of any in-scope asset. If DCMA DIBCAC identifies that a Level 2 security requirement is NOT MET, the Level 3 assessment process may be paused to allow for remediation, placed on hold, or immediately terminated. For further information regarding scoping of CMMC Level 3 assessments please contact DCMA DIBCAC at *www.dcma.mil/DIBCAC/*.

§ 170.20 Standards acceptance.

(a) *NIST SP 800–171 R2 DoD assessments*. In order to avoid duplication of efforts, thereby reducing the aggregate cost to industry and the Department, OSCs that have completed a DCMA DIBCAC High Assessment aligned with CMMC Level 2 Scoping will be given the CMMC Status of Final Level 2 (C3PAO) under the following conditions:

(1) *DCMA DIBCAC High Assessment*. An OSC that achieved a perfect score with no open POA&M from a DCMA DIBCAC High Assessment conducted prior to the effective date of this rule, will be given a CMMC Status of Level 2 Final (C3PAO) with a validity period of three (3) years from the date of the original DCMA DIBCAC High Assessment. DCMA DIBCAC will identify assessments that meet these criteria and verify that SPRS accurately reflects the CMMC Status. Eligible DCMA DIBCAC High Assessments include ones conducted with Joint Surveillance in accordance with the DCMA Manual 2302–01 Surveillance. The scope of the Level 2 certification assessment is identical to the scope of the DCMA DIBCAC High Assessment. In accordance with §170.17(a)(2), the OSC must also submit an affirmation in SPRS and annually thereafter to achieve contractual eligibility.

(2) [Reserved].

(b) [Reserved].

§ 170.21 Plan of Action and Milestones requirements.

(a) *POA&M*. For purposes of achieving a Conditional CMMC Status, an OSA is only permitted to have a POA&M for select requirements scored as NOT MET during the CMMC assessment and only under the following conditions:

(1) *Level 1 self-assessment*. A POA&M is not permitted at any time for Level 1 self-assessments.

(2) *Level 2 self-assessment and Level 2 certification assessment*. An OSA is only permitted to achieve the CMMC Status of Conditional Level 2 (Self) or Conditional Level 2 (C3PAO), as appropriate, if all the following conditions are met:

(i) The assessment score divided by the total number of CMMC Level 2 security requirements is greater than or equal to 0.8;

(ii) None of the security requirements included in the POA&M have a point value of greater than 1 as specified in the CMMC Scoring Methodology set forth in §170.24, except SC.L2–3.13.11 CUI Encryption may be included on a POA&M if encryption is employed but it is not FIPS-validated, which would result in a point value of 3; and

(iii) None of the following security requirements are included in the POA&M:

(A) AC.L2–3.1.20 External Connections (CUI Data).

(B) AC.L2–3.1.22 Control Public Information (CUI Data).

(C) CA.L2–3.12.4 System Security Plan.

(D) PE.L2–3.10.3 Escort Visitors (CUI Data).

(E) PE.L2–3.10.4 Physical Access Logs (CUI Data).

(F) PE.L2–3.10.5 Manage Physical Access (CUI Data).

(3) *Level 3 certification assessment*. An OSC is only permitted to achieve the CMMC Status of Conditional Level 3 (DIBCAC) if all the following conditions are met:

(i) The assessment score divided by the total number of CMMC Level 3 security requirements is greater than or equal to 0.8; and

(ii) The POA&M does not include any of following security requirements:

(A) IR.L3–3.6.1e Security Operations Center.

(B) IR.L3–3.6.2e Cyber Incident Response Team.

(C) RA.L3–3.11.1e Threat-Informed Risk Assessment.

(D) RA.L3–3.11.6e Supply Chain Risk Response.

(E) RA.L3–3.11.7e Supply Chain Risk Plan.

(F) RA.L3–3.11.4e Security Solution Rationale.

(G) SI.L3–3.14.3e Specialized Asset Security.

(b) *POA&M closeout assessment.* A POA&M closeout assessment is a CMMC assessment that assesses only the NOT MET requirements that were identified with POA&M in the initial assessment. The closing of a POA&M must be confirmed by a POA&M closeout assessment within 180-days of the Conditional CMMC Status Date. If the POA&M is not successfully closed out within the 180-day timeframe, the Conditional CMMC Status for the information system will expire.

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

(2) *Level 2 certification assessment.* For Level 2 certification assessment, the POA&M closeout certification assessment must be performed by an authorized or accredited C3PAO.

(3) *Level 3 certification assessment.* For Level 3 certification assessment, DCMA DIBCAC will perform the POA&M closeout certification assessment.

§ 170.22 Affirmation.

(a) *General.* The OSA must affirm continuing compliance with the appropriate level self-assessment or certification assessment. An Affirming Official from each OSA, whether a prime or subcontractor, must affirm the continuing compliance of their respective organizations with the specified security requirement after every assessment, including POA&M closeout, and annually thereafter. Affirmations are entered electronically in SPRS. The affirmation shall be submitted in accordance with the following requirements:

(1) *Affirming Official.* The Affirming Official is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations.

(2) *Affirmation content.* Each CMMC affirmation shall include the following information:

(i) Name, title, and contact information for the Affirming Official; and

(ii) Affirmation statement attesting that the OSA has implemented and will maintain implementation of all applicable CMMC security requirements to their CMMC Status for all information systems within the relevant CMMC Assessment Scope.

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

(i) Upon achievement of a Conditional CMMC Status, as applicable;

(ii) Upon achievement of a Final CMMC Status;

(iii) Annually following a Final CMMC Status Date; and

(iv) Following a POA&M closeout assessment, as applicable.

(b) *Submission procedures.* All affirmations shall be completed in SPRS. The Department will verify submission of the affirmation in SPRS to ensure compliance with CMMC solicitation or contract requirements.

(1) *Level 1 self-assessment.* At the completion of a Level 1 self-assessment and annually thereafter, the Affirming Official shall submit a CMMC affirmation attesting to continuing compliance with all requirements of the CMMC Status Level 1 (Self).

(2) *Level 2 self-assessment.* At the completion of a Level 2 self-assessment and annually following a Final CMMC Status Date, the Affirming Official shall submit a CMMC affirmation attesting to continuing compliance with all requirements of the CMMC Status Level 2 (Self). An affirmation shall also be submitted at the completion of a POA&M closeout self-assessment.

(3) *Level 2 certification assessment.* At the completion of a Level 2 certification assessment and annually following a Final CMMC Status Date, the Affirming Official shall submit a CMMC affirmation attesting to continuing compliance with all requirements of the CMMC Status Level 2 (C3PAO). An affirmation shall also be submitted at the completion of a POA&M closeout certification assessment.

(4) *Level 3 certification assessment.* At the completion of a Level 3 certification assessment and annually following a Final CMMC Status Date, the Affirming Official shall submit a CMMC affirmation attesting to continuing compliance with all requirements of the CMMC Status Level 3 (DIBCAC). Because C3PAOs and DCMA DIBCAC check for compliance with different requirements in their respective assessments, OSCs must annually affirm their CMMC Status of Level 2 (C3PAO) in addition to their CMMC Status of Level 3 (DIBCAC) to maintain eligibility for contracts requiring compliance with Level 3. An affirmation shall also be submitted at the completion of a POA&M closeout certification assessment.

§ 170.23 Application to subcontractors.

(a) CMMC requirements apply to prime contractors and subcontractors throughout the supply chain at all tiers that will process, store, or transmit any FCI or CUI on contractor information systems in the performance of the DoD contract or subcontract. Prime contractors shall comply and shall require subcontractors to comply with and to flow down CMMC requirements, such that compliance will be required throughout the supply chain at all tiers with the applicable CMMC level and assessment type for each subcontract as follows:

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

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

(3) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contract has a requirement for a CMMC Status of Level 2 (C3PAO), then the CMMC Status of Level 2 (C3PAO) is the minimum requirement for the subcontractor.

(4) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contract has a requirement for the CMMC Status of Level 3 (DIBCAC), then the CMMC Status of Level 2 (C3PAO) is the minimum requirement for the subcontractor.

(b) As with any solicitation or contract, the DoD may provide specific guidance pertaining to flow-down.

§ 170.24 CMMC Scoring Methodology.

(a) *General.* This scoring methodology is designed to provide a measurement of an OSA's implementation status of the NIST SP 800–171 R2 security requirements (incorporated by reference elsewhere in this part, see §170.2) and the selected NIST SP 800–172 Feb2021 security requirements (incorporated by reference elsewhere in this part, see §170.2). The CMMC Scoring Methodology is designed to credit partial implementation only in limited cases (*e.g.*, multi-factor authentication IA.L2–3.5.3).

(b) *Assessment findings.* Each security requirement assessed under the CMMC Scoring Methodology must result in one of three possible assessment findings, as follows:

(1) *Met.* All applicable objectives for the security requirement are satisfied based on evidence. All evidence must be in final form and not draft. Unacceptable forms of evidence include but are not limited to working papers, drafts, and unofficial or unapproved policies.

(i) Enduring exceptions when described, along with any mitigations, in the system security plan shall be assessed as MET.

(ii) Temporary deficiencies that are appropriately addressed in operational plans of action (*i.e.*, include deficiency reviews and show progress towards the implementation of corrections to reduce or eliminate identified vulnerabilities) shall be assessed as MET.

(2) *Not Met.* One or more applicable objectives for the security requirement is not satisfied. During an assessment, for each security requirement objective marked NOT MET, the assessor will document why the evidence does not conform.

(3) *Not Applicable (N/A).* A security requirement and/or objective does not

apply at the time of the CMMC assessment. For example, Public-Access System Separation (SC.L2–3.13.5) might be N/A if there are no publicly accessible systems within the CMMC Assessment Scope. During an assessment, an assessment objective assessed as N/A is equivalent to the same assessment objective being assessed as MET.

(c) *Scoring*. At each CMMC Level, security requirements are scored as follows:

(1) *CMMC Level 1*. All CMMC Level 1 security requirements must be fully implemented to be considered MET. No POA&M is permitted for CMMC Level 1, and self-assessment results are scored as MET or NOT MET in their entirety.

(2) *CMMC Level 2 Scoring Methodology*. The maximum score achievable for a Level 2 self-assessment or Level 2 certification assessment is equal to the total number of CMMC Level 2 security requirements. If all CMMC Level 2 security requirements are MET, OSAs are awarded the maximum score. For each requirement NOT MET, the associated value of the security requirement is subtracted from the maximum score, which may result in a negative score.

(i) *Procedures*. (A) Scoring methodology for Level 2 self-assessment and Level 2 certification assessment is based on all CMMC Level 2 security requirement objectives, including those NOT MET.

(B) In the CMMC Level 2 Scoring Methodology, each security requirement has a value (*e.g.*, 1, 3 or 5), which is related to the designation by NIST as basic or derived security requirements. Per NIST SP 800–171 R2, the basic security requirements are obtained from FIPS PUB 200 Mar2006, which provides the high-level and fundamental security requirements for Federal information and systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST SP 800–53 R5.

(*1*) For NIST SP 800–171 R2 basic and derived security requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration of CUI, five (5) points are subtracted from the maximum score. The basic and derived security requirements with a value of five (5) points include:

(*i*) *Basic security requirements*. AC.L2–3.1.1, AC.L2–3.1.2, AT.L2–3.2.1, AT.L2–3.2.2, AU.L2–3.3.1, CM.L2–3.4.1, CM.L2–3.4.2, IA–L2–3.5.1, IA–L2–3.5.2, IR.L2–3.6.1, IR.L2–3.6.2, MA.L2–3.7.2, MP.L2–3.8.3, PS.L2–3.9.2, PE.L2–3.10.1, PE.L2–3.10.2, CA.L2–3.12.1, CA.L2–3.12.3, SC.L2–3.13.1, SC.L2–3.13.2, SI.L2–3.14.1, SI.L2–3.14.2, and SI.L2–3.14.3.

(*ii*) *Derived security requirements*. AC.L2–3.1.12, AC.L2–3.1.13, AC.L2–3.1.16, AC.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, three (3) points are subtracted from the maximum score. The basic and derived security requirements with a value of three (3) points include:

(*i*) *Basic security requirements*. AU.L2–3.3.2, MA.L2–3.7.1, MP.L2–3.8.1, MP.L2–3.8.2, PS.L2–3.9.1, RA.L2–3.11.1, and CA.L2–3.12.2.

(*ii*) *Derived security requirements*. AC.L2–3.1.5, AC.L2- 3.1.19, MA.L2–3.7.4, MP.L2–3.8.8, SC.L2–3.13.8, SI.L2–3.14.5, and SI.L2–3.14.7.

(*3*) All remaining derived security requirements, other than the exceptions noted, if not implemented, have a limited or indirect effect on the security of the network and its data. For these, 1 point is subtracted from the maximum score.

(*4*) Two derived security requirements, IA.L2–3.5.3 and SC.L2–3.13.11, can be partially effective even if not completely or properly implemented, and the points deducted may be adjusted depending on how the security requirement is implemented.

(*i*) Multi-factor authentication (MFA) (CMMC Level 2 security requirement IA.L2–3.5.3) is typically implemented first for remote and privileged users (since these users are both limited in number and more critical) and then for the general user, so three (3) points are subtracted from the maximum score if MFA is implemented

only for remote and privileged users. Five (5) points are subtracted from the maximum score if MFA is not implemented for any users.

(*ii*) FIPS-validated encryption (CMMC Level 2 security requirement SC.L2–3.13.11) is required to protect the confidentiality of CUI. If encryption is employed, but is not 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*) OSAs must have a System Security Plan (SSP) (CMMC security requirement CA.L2–3.12.4) in place at the time of assessment to describe each information system within the CMMC Assessment Scope. The absence of an up to date SSP at the time of the assessment would result in a finding that '*an assessment could not be completed due to incomplete information and noncompliance with 48 CFR 252.204–7012*.'

(*6*) For each NOT MET security requirement the OSA must have a POA&M in place. A POA&M addressing NOT MET security requirements is not a substitute for a completed requirement. Security requirements not implemented, whether described in a POA&M or not, is assessed as 'NOT MET.'

(*7*) Specialized Assets must be evaluated for their asset category per the CMMC scoping guidance for the level in question and handled accordingly as set forth in § 170.19.

(*8*) If an OSC previously received a favorable adjudication from the DoD CIO indicating that a security requirement is not applicable or that an alternative security measure is equally effective (in accordance with 48 CFR 252.204–7008 or 48 CFR 252.204–7012), the DoD CIO adjudication must be included in the system security plan to receive consideration during an assessment. A security requirement for which implemented security measures have been adjudicated by the DoD CIO as equally effective is assessed as MET if there have been no changes in the environment.

(ii) *CMMC Level 2 Scoring Table.* CMMC Level 2 scoring has been assigned based on the methodology set forth in table 1 to this paragraph (c)(2)(ii).

TABLE 7 TO § 170.24(c)(2)(ii)—CMMC LEVEL 2 SCORING TABLE

CMMC Level 2 requirement categories	Point value subtracted from maximum score
Basic Security Requirements:	
If not implemented, could lead to significant exploitation of the network, or exfiltration of CUI	5
If not implemented, has specific and confined effect on the security of the network and its data	3
Derived Security Requirements:	
If not implemented, could lead to significant exploitation of the network, or exfiltration of CUI	5
If not completely or properly implemented, could be partially effective and points adjusted depending on how the security requirement is implemented: —Partially effective implementation—3 points. —Non-effective (not implemented at all)—5 points.	3 or 5
If not implemented, has specific and confined effect on the security of the network and its data	3
If not implemented, has a limited or indirect effect on the security of the network and its data	1

(3) *CMMC Level 3 assessment scoring methodology.* CMMC Level 3 scoring does not utilize varying values like the scoring for CMMC Level 2. All CMMC Level 3 security requirements use a value of one (1) point for each security requirement. As a result, the maximum score achievable for a Level 3 certification assessment is equivalent to the total number of the selected subset of NIST SP 800–172 Feb2021 security requirements for CMMC Level 3, see § 170.14(c)(4). The maximum score is reduced by one (1) point for each security requirement NOT MET. The CMMC Level 3 scoring methodology reflects the fact that all CMMC Level 2 security requirements must already be MET (for the Level 3 CMMC Assessment Scope). A maximum score on the Level 2 certification assessment is required to be eligible to initiate a Level 3 certification assessment. The Level 3 certification assessment score is equal to the number of CMMC Level 3 security requirements that are assessed as MET.

APPENDIX A TO PART 170—GUIDANCE

Guidance documents include:

(a) ''CMMC Model Overview'' available at *https://DoDcio.defense.gov/CMMC/*.

(b) ''CMMC Assessment Guide—Level 1'' available at *https://DoDcio.defense.gov/CMMC/*.

(c) ''CMMC Assessment Guide—Level 2'' available at *https://DoDcio.defense.gov/CMMC/*.

(d) ''CMMC Assessment Guide—Level 3'' available at *https://DoDcio.defense.gov/CMMC/*.

(e) ''CMMC Scoping Guide—Level 1'' available at *https://DoDcio.defense.gov/CMMC/*.

(f) ''CMMC Scoping Guide—Level 2'' available at *https://DoDcio.defense.gov/CMMC/*.

(g) ''CMMC Scoping Guide—Level 3'' available at *https://DoDcio.defense.gov/CMMC/*.

(h) ''CMMC Hashing Guide'' available at *https://DoDcio.defense.gov/CMMC/*.

PART 173—COMPETITIVE INFORMATION CERTIFICATE AND PROFIT REDUCTION CLAUSE

Sec.

AUTHORITY: 10 U.S.C. 2202.

SOURCE: 53 FR 42948, Oct. 25, 1988, unless otherwise noted.

§ 173.1 Scope.

(a) The purpose of the Competitive Information Certificate is to provide the Contracting Officer sufficient information and assurance to support award of a contract in those circumstances where certification is required.

(b) Although a Competitive Information Certificate provides reasonable assurance to the Government, the possibility remains that even a diligent internal review by the contractor may fail to identify illegal or improper actions. The purpose of the Profit Reduction Clause is to ensure effective protection of the Government's interest in making contract awards when a Competitive Information Certification is required. The Profit Reduction Clause is required in all competitively awarded new contracts over $100,000 when a Competitive Information Certificate is required prior to award.

§ 173.2 Competitive Information Certification.

(a) The Competitive Information Certificate is required prior to award of all competitively awarded new contracts of a value exceeding $100,000 to contractors subject to the requirement.

(1) Corporate activities required to provide the Certificate are corporations or corporate divisions which have been the subject of search warrants, or as to which other official information indicates such certification should be required, and their subsidiaries and affiliates. A list of contractors from whom certification is required is maintained and published as required under authority of the Department of Defense Procurement Task Force.

(2) The requirement to provide the Certificate may be further limited to certain divisions or subsidiaries, contracts or programs upon the basis of official information, furnished by the contractor or otherwise, sufficient to establish to the satisfaction of the Department of Defense that the investigation is so limited. Such information may include copies of search warrants, subpoenas and affidavits from corporate officials concerning the scope and conduct of the investigation. The sufficiency of such information is solely within the discretion of the Department of Defense.

(3) Contractors from whom certification in certain instances is required will be relieved of the certification requirement when the Department of Defense determines that information developed in the ''Ill Wind'' investigation has been resolved in such a manner that certification is no longer required to protect the interests of the Government.

(4) A Certificate will not be required prior to the exercise of options or noncompetitive award of contracts. This does not limit in any manner the Government's ability to inquire into, or require information concerning, the circumstances surrounding an underlying competitive award.

(b) With respect to information disclosed under paragraph (1) of the Certificate, the offeror must attach to the Certificate a written statement detailing what information was obtained, and how, when, and from whom it was