(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.