Cybersecurity Maturity Model Certification

CMMC ASSESSMENT PROCESS

Version 2.0

December 2024

DISCLAIMER

The views, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official U.S. Government position, policy, or decision, unless designated by other documentation.

Nothing contained in this document supersedes any standard, policy, direction, or official CMMC program information that has been promulgated by the United States Department of Defense (DoD) or the National Institute of Standards and Technology (NIST). In the event of a contradiction, real or perceived, the reader should adhere to the DoD and/or NIST documentation.

NO WARRANTIES ARE MADE HEREIN. THIS MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. THE CMMC ACCREDITATION BODY, INC. MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY OR RESULTS OBTAINED FROM USE OF THE MATERIAL, NOR ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, or COPYRIGHT INFRINGEMENT.

Document Revision History

Date	Version	Page(s)	Description	Author
23 AUG 2022	v1.0[1]	All	Pre-Decisional Draft	The Cyber AB
16 DEC 2024	v2.0	All	CMMC 2.0 Effective and In Force	The Cyber AB

Comments on this DRAFT CAP v2.0 are welcomed from all members of the CMMC Ecosystem, the DIB, and the public. This feedback will be used to improve the document and may help inform the publication of future editions of the CAP. Feedback can be submitted via the email address CAPComments@cyberab.org.

[1] A DRAFT CAP with an internal developmental version number 5.6.1 was provided for training purposes only during the summer of 2022.

Table of Contents

INTRODUCTION TO THE CMMC ASSESSMENT PROCESS (CAP)

The Cybersecurity Maturity Model Certification (CMMC) Program is the U.S. Department of Defense's (DoD) initiative for the assessment and certification of conformance to established security requirements by companies and organizations within the Defense Industrial Base (DIB).[2] Specifically, CMMC is designed to safeguard Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) that is processed, stored, and/or transmitted during the performance of DoD contracts.

The CMMC Program is overseen by the Office of the DoD Chief Information Officer (ODCIO) and administered by the CMMC Program Management Office (CMMC PMO). The Cyber AB is the designated sole Accreditation Body for the CMMC Program. The Cyber AB supports the CMMC Program through a no-cost contract with DoD's Washington Headquarters Services (WHS).[3]

Most of the official CMMC doctrine and documentation is provided within the Code of Federal Regulations (CFR) or by DoD and the National Institute of Standards and Technology (NIST) within the Department of Commerce. For example, the actual CMMC Level 2 security requirements themselves are codified within the NIST Special Publication 800-171, Revision 2 (NIST SP 800-171 R2), "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". The CMMC Scoping Guides and Assessment Guides that are developed, maintained, and published by DoD provide supplemental guidance and insight consistent with authoritative references for establishing the assessment boundaries as well as for evaluating the implementation of CMMC security requirements, respectively.

The *CMMC Assessment Process* (CAP), by comparison, **is the official procedural guide for CMMC Third-Party Assessment Organizations (C3PAOs)** conducting a CMMC Level 2 certification assessment (herein also referred to as an "assessment") of an Organization Seeking Certification (OSC). The CAP is published and maintained by The Cyber AB and reviewed and approved by the CMMC PMO. It is intended as a resource for the entire CMMC Ecosystem, as well as for companies and organizations within the DIB.

The purpose of the CAP is to ensure the consistency and integrity of CMMC Level 2 certification assessments. Adherence to the CAP is required by C3PAOs and their CMMC Certified Assessors (CCAs) and is an element of the C3PAO Accreditation Scheme. The CAP is not to be confused with references to a generalized CMMC "assessment process" that appear in the Code of Federal Regulations (CFR), Title 32, part 170.

---

[2] Specifically, CMMC assesses conformance to the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252-204-7021, "Assessing Contractor Implementation of Cybersecurity Requirements".

[3] The Cyber AB is the "doing business as (d/b/a)" name for the Cybersecurity Maturity Model Certification Accreditation Body, Inc., an independent, tax-exempt 501(c)(3) charitable organization that supports the Department of Defense's CMMC Program via a no-cost contract (Department of Defense contract #HQ003420H0003).

How to Use the CAP

The CAP applies only to the conduct of CMMC Level 2 certification assessments.

The CAP must be used in concert with the authoritative CMMC source material—32 CFR part 170 and those documents included by reference therein—as well as the supplemental CMMC guidance published by DoD. It neither replaces nor supersedes any requirements or directions contained in those documents. Moreover, the CAP does not reproduce nor reinterpret any of the rules, provisions, or procedures from either authoritative references or DoD supplemental guidance. Rather, it cites and references those documents throughout. Accordingly, C3PAOs and their CMMC Assessment Teams will need active access to the authoritative documents, along with the CAP, when conducting a CMMC Level 2 certification assessment.

The CAP addresses pre-assessment "preliminary proceedings" that are then followed by the actual assessment process, which is organized across four (4) phases and describes the required activities, roles, and responsibilities of CMMC assessment participants in each.

The four phases are:

- Phase 1: "Conduct the Pre-Assessment";
- Phase 2: "Assess Conformity to Security Requirements";
- Phase 3: "Complete and Report Assessment Results"; and
- Phase 4: "Issue Certificate and Closeout POA&M".

These four phases have been designed to support each CMMC Level 2 certification assessment meeting the following objectives:

- Achieve the highest possible accuracy, fidelity, and quality of CMMC Level 2 certification assessments conducted by C3PAOs;
- Maximize consistency to ensure that CMMC Level 2 certification assessments conducted by C3PAOs and their CMMC Certified Assessors follow the same procedures, sequencing of activities, and production of verifiable results; and
- Instill trust and confidence in the CMMC Program by providing effective, transparent, and efficient CMMC Level 2 certification assessments that are well-planned, executed in consistent fashion, and accurately reported.

The CAP provides a logical and practical sequencing of activities and actions throughout the four phases of the assessment process to ensure procedural coherence for the parties. In certain sections of the process, a precise sequence of specific actions may be explicitly mandated in the document. In these instances, the text will make clear the necessity of following certain procedures in a manner of specific order. In all other aspects of the CAP, the C3PAO and the OSC have the latitude and flexibility to conduct the CMMC assessment with a reasonable approach of their own *when applied to the general sequencing* of actions throughout the preliminary proceedings and four phases.

ROLES AND RESPONSIBILITIES

A CMMC Level 2 certification assessment requires the active engagement, communication, and attention of several key individuals or organizations, which may include:

As defined in 32 CRF §170.4:

- Organization Seeking Certification (OSC)
- Affirming Official
- CMMC Third-Party Assessment Organization (C3PAO)
  - Assessment Team members
- Accreditation Body (The Cyber AB)
- CMMC Assessor and Instruction Certification Organization (The CAICO)

Other relevant individuals not directly defined in 32 CRF §170.4:

- **Authorized Certifying Official**: A designated official employed by the C3PAO and registered with The Cyber AB who is eligible to serve as the issuing authority and signatory for the CMMC Level 2 Certificate of CMMC Status provided to the OSC. C3PAOs may designate more than one Authorized Certifying Official.
- **Lead CCA:** The CMMC Certified Assessor (CCA) who satisfies the requirements of 32 CFR §170.4(b)(11) and who oversees and manages a dedicated Assessment Team on behalf of the C3PAO for the conduct of a CMMC Level 2 certification assessment. The Lead CCA serves as the counterpart to the Affirming Official. Lead CCA is a formal qualified designation issued by the CAICO. A Lead CCA may oversee multiple Assessment Teams across concurrent CMMC Level 2 certification assessments.
- **OSC Point of Contact (OSC POC):** The individual within or on behalf of the OSC who provides daily coordination and liaison support between the OSC and the Assessment Team. The OSC POC does not necessarily have to be an employee of the organization that is being assessed, but rather could be a contractor, consultant, or advisor, such as a CMMC Registered Practitioner (RP).
- **quality assurance (QA) individual:** An individual who manages the C3PAO's quality assurance reviews for a CMMC Level 2 certification assessment, which includes observing the Assessment Team's conduct and management of the assessment. A QA individual also manages a CMMC appeals process that might be initiated by an OSC.[4] A QA individual must be a CCA and cannot be a member of an Assessment Team for which they are performing a quality assurance role. A QA individual is also responsible for the uploading of assessment information into the CMMC instantiation of eMASS.

[4] 32 CFR §170.9(b)(13)

PRELIMINARY PROCEEDINGS

A CMMC Level 2 certification assessment compels a few preliminary administrative, framing, and contractual activities that should be addressed prior to the formal commencement of Phase 1 of the assessment. These interactions between the C3PAO and the OSC concern important aspects of the prospective assessment, and their successful and mutually agreeable resolution will help enable a proper, viable, and transparent CMMC Level 2 certification assessment.

Receive CMMC Assessment Request from OSC

P.1 An OSC generally initiates the engagement concerning a prospective CMMC Level 2 certification assessment by contacting an authorized or accredited C3PAO.

P.2 The updated registry of authorized or accredited C3PAOs in good standing is maintained on the CMMC Marketplace website administered by The Cyber AB. Unless otherwise notified by The Cyber AB, any C3PAO listed as "authorized" or "accredited" within the Marketplace may be considered a C3PAO in good standing and eligible to conduct a CMMC Level 2 certification assessment.[5]

Confirm the Entity/Entities to be Assessed

P.3 The C3PAO shall confirm the specific corporate legal entity that will be assessed, *i.e.*, the precise identity of the actual "Organization Seeking Certification."

P.4 The C3PAO shall solicit from the OSC the Commercial and Government Entity (CAGE) code, or multiple CAGE codes, that are affiliated with the CMMC Level 2 certification assessment. Technically, a Level 2 CMMC Certificate of Status is issued upon a discrete and identified information system, as defined within a System Security Plan (SSP), that is owned and operated by an OSC. The identity of the OSC is determined by the CAGE code(s), which are issued by DoD.

P.5 The C3PAO should also request the OSC's assessment unique identifier (UID) if a previous self-assessment had generated one. The DoD Supplier Performance Risk System (SPRS) generates a UID for a Level 1 and Level 2 self-assessment. The Pre-Assessment Form should include this SPRS UID if it exists, but it is *not required* for a Level 2 certification assessment, as the CMMC instantiation of eMASS will generate a new UID upon successful attainment of a Level 2

[5] In no circumstances will individuals from The Cyber AB, the CAICO, or DoD provide recommendations or facilitate introductions to any C3PAO.

Certificate of CMMC Status. The CMMC eMASS UID and the SPRS UID share the same format, serve the same purpose, and are unique for each Level 2 certification assessment and self-assessment, respectively.

P.6 All OSCs must possess a valid CAGE code and the CMMC Level 2 certification assessment cannot proceed without at least one CAGE code of record.[6] A single CMMC assessment may cover multiple entities in the event more than one CAGE code is associated with a singular CMMC Level 2 Assessment Scope.[7]

P.7 The C3PAO should ask the OSC whether any in-scope External Service Providers (ESPs), as defined by **32 CFR § 170.4(b**), exist and whether the OSC considers the ESP a Cloud Service Provider (CSP) or a "non-CSP" ESP under **32 CFR § 170.19(c)(2)**.

Frame the Assessment

P.8 The C3PAO shall work with the Affirming Official and/or the OSC POC to determine the purview and planning details of the assessment. This shall include discussing schedule, the size of the organization and information system to be assessed, personnel, logistics, relevant contractual requirements, and the prospective CMMC Assessment Scope.

P.9 The CMMC Assessment Scope is the set of all assets in the OSC's environment that will be assessed against CMMC security requirements. It must be specified prior to the commencement of the Assessment.[8] **The determination of proper CMMC Assessment Scope is established in in 32 CFR §170.19(c), "CMMC Level 2 Scoping".** Supplemental information on CMMC Assessment Scope is contained the DoD manual, *CMMC Assessment Scope – Level 2*.

P.10 In framing the CMMC Level 2 certification assessment, the C3PAO and OSC should discuss and agree upon, at a minimum, the following aspects:

- Availability of personnel in support of the assessment;
- Availability of evidence in support of the assessment;
- OSC's relevant documentation, including the System Security Plan (SSP); and
- An estimate for the approximate duration and timing for the assessment.

P.11 Another consideration of framing the assessment involves determining assessment location(s), including what security requirement objectives of the assessment might be assessed virtually or in-person on the OSC premises. The Lead CCA and/or the C3PAO should consider the optimal logistical approach for implementation validation of the following 18 CMMC security requirement objectives to ensure adequate assessment scope and depth:

- CM.L2-3.4.5[d]: Physical access restrictions associated with changes to the system are enforced.
- MA.L2-3.7.2[d]: Personnel used to conduct system maintenance are controlled.
- MP.L2-3.8.1[c]: Paper media containing CUI is securely stored.

[6] For access to SPRS, the OSC will also need to obtain a Unique Entity ID that is generated from registration in SAM.gov.

[7] In addition, the HQ organization or the Host Unit, depending on the corporate structure, must also have registered with the General Services Administration's (GSA) SAM.gov system and have been issued a Unique Entity Identifier (UEI).

[8] 32 CFR §170.19(a)

- MP.L2-3.8.1[d]: Digital media containing CUI is securely stored.
- MP.L2-3.8.4[a]: Media containing CUI is marked with applicable CUI markings.
- MP.L2-3.8.4[b]: Media containing CUI is marked with distribution limitations.
- PE.L1-3.10.1[b]: Physical access to organization systems is limited to authorized individuals.
- PE.L1-3-10.1[c]: Physical access to equipment is limited to authorized individuals.
- PE.L1-3-10.1[d]: Physical access to operating environments is limited to authorized individuals.
- PE.L2-3.10.2[a]: The physical facility where organizational systems reside is protected.
- PE.L2-3.10.2[b]: The support infrastructure for organizational systems is protected.
- PE.L2-3.10.2[c]: The physical facility where organizational systems reside is monitored.
- PE.L2-3.10.2[d]: The support infrastructure for organizational systems is monitored.
- PE.L1-3.10.3[a]: Visitors are escorted.
- PE.L1-3.10.3[b]: Visitor activity is monitored.
- PE.L1-3.10.5[b]: Physical access devices are controlled.
- PE.L1-3.10.5[c]: Physical access devices are managed.
- SC.L2-3.13.12[b]: Collaborative computing devices provide indication to users of devices in use.

NOTE: For OSC CMMC-scoped environments that DO NOT have physical and/or environmental controls due to a cloud environment or other factors that negate conducting an "on-site" portion of the assessment, the applicability of these requirements should be addressed between the OSC and the C3PAO in Phase 1.

Identify and Manage Initial Conflicts of Interest (COI)

P.12 C3PAOs are ultimately responsible for managing impartiality and identifying conflicts of interest relating to a CMMC Level 2 certification assessment. This responsibility cannot be delegated to their CMMC Assessment Team or the OSC.

P.13 C3PAOs shall adhere to the impartiality requirements of ISO/IEC 17020:2012 and the conflict-of-interest disclosure provisions and COI prohibitions within the CMMC Code of Professional Conduct (CoPC). The CoPC contains additional details on impartiality requirements, including CMMC-specific examples of potential COIs that are to be mitigated or avoided.

P.14 The C3PAO shall propose to the OSC the name of the Lead CCA that it intends to assign to the OSC's CMMC Level 2 certification assessment. The C3PAO shall coordinate with the OSC to ascertain if any conflicts of interest exist between the proposed Lead CCA and the OSC.

P.15 If a conflict of interest is disclosed or identified, by either party, the C3PAO shall work with the OSC to develop a mitigation plan for the identified conflict in question.

P.13.1 Any mitigation measures to which the parties agree shall be documented.

P.13.2 In the event the conflict cannot be sufficiently mitigated due to the circumstances, the C3PAO shall not proceed with the assessment.

P.16 The C3PAO should obtain concurrence of the OSC on the assignment of the Lead CCA prior to commencing with the CMMC Level 2 certification assessment.

Execute Contractual Agreement

P. 17 The C3PAO shall execute a written contractual agreement for the CMMC Level 2 certification assessment with the OSC. Neither The Cyber AB nor DoD are parties to the CMMC Level 2 certification assessment contract between the C3PAO and the OSC.

P.18 The format and structure of the contract is at the discretion and mutual agreement of the C3PAO and OSC.

P.19 A mutual non-disclosure agreement (NDA) between the parties shall be incorporated into the contractual agreement or negotiated and executed in a separate document (*e.g.*, stand-alone NDA, master services agreement, etc.).

P.20 All contractual agreements for CMMC assessments must comport to the CMMC Code of Professional Conduct. Specifically, the C3PAO is prohibited from offering any "guarantees" or "promises" relating to the results of the CMMC Level 2 certification assessment, nor may the C3PAO include any incentives or bonus payments contingent on the issuance of a Certificate of CMMC Status to the OSC.

PHASE 1 – CONDUCT THE PRE-ASSESSMENT

In Phase 1, the C3PAO will evaluate if the OSC has adequately prepared for the assessment of its implementation of CMMC Level 2 security requirements.

At the conclusion of Phase 1, the C3PAO will submit the Pre-Assessment Information Form into the CMMC instantiation of eMASS.

1.1. The Lead CCA shall supervise Phase 1 activities.

Review the System Security Plan (SSP)

1.2. C3PAO personnel shall review the OSC's System Security Plan (SSP) and examine the document for completeness, accuracy, and consistency. By conducting this cursory review of the SSP in Phase 1, the C3PAO should be able to arrive at a reasonable expectation that the OSC has addressed the security requirements of NIST SP 800-171 R2, without regard to evaluating the adequacy or sufficiency of implementation.

Validate CMMC Assessment Scope

1.3. **The Lead CCA shall validate the OSC's CMMC Level 2 Assessment Scope in accordance with 32 CFR §170.19(c), "CMMC Level 2 Scoping".** The DoD publication, *CMMC Assessment Scope – Level 2*, contains additional CMMC scoping guidance.

1.4. Any disagreements or differences of opinion concerning the CMMC Assessment Scope must be resolved between the C3PAO and the OSC before the CMMC Level 2 certification assessment may proceed to Phase 2.

1.5. As part of the defined Assessment Scope requirements addressed in 32 CFR §170.19(c), the Lead CCA, Assessment Team members, and the OSC shall establish evaluation methods for CMMC Level 2 security requirement objectives, based on the OSC's CUI Level 2 assets, and the degree of rigor to be applied to the assessment, which may include, but is not necessarily limited to, the assessment methods addressed in activity 1.10.

1.6. If the OSC has identified an ESP as being within their CMMC Assessment Scope, the Assessment Team shall confirm that a Customer Responsibility Matrix (CRM) will be available and that ESP personnel will be present and actively participating in the assessment.

1.7. If the ESP that has been identified as being within the OSC's CMMC Assessment Scope stores, processes, or transmits CUI, the Assessment Team shall confirm that the OSC will be prepared to provide evidence of the ESP's FedRAMP Moderate Authorization, FedRAMP Moderate equivalency, or a Level 2 Certificate of CMMC Status, as appropriate.

1.8. If the Lead CCA cannot confirm proper incorporation, documentation, and/or participation, as appropriate, of an ESP in the OSC's CMMC Level 2 Assessment Scope, the C3PAO should confer with the OSC Affirming Official and discuss the merits of not proceeding with the CMMC Level 2 certification assessment.

Confirm Availability of Evidence

1.9. The Assessment Team will need access to various evidence and artifacts—as well as OSC personnel and ESP personnel (if applicable)—to conduct the evaluative activities in Phase 2 of the CMMC Level 2 certification assessment. The Lead CCA, in preparing for the assessment, should be confident that there will be ample evidence made accessible to the Assessment Team to render an accurate evaluation of the security requirements of NIST SP 800-171 R2 and determine if they have been properly implemented by the OSC.

Determine Readiness for Assessment

1.10. The Lead CCA shall make the determination as to the readiness of the OSC to proceed with the conduct of the CMMC Level 2 certification assessment. The determination should be based on the reviews and confirmations conducted in this Phase as well as a general confidence that the OSC is overall prepared for the conduct of the assessment. The Lead CCA should convey to the OSC that various assessment methods (*e.g.*, reviewing, inspecting, observing, studying, analyzing, discussing, and exercising assessment objects) will be employed and may include assessment methods and associate attributes of depth and coverage as outlined in:

- NIST SP 800-171A, Appendix D, "Assessment Methods";
- NIST SP 800-53A, 3.2.3.2 - "Depth- and Coverage-Related Considerations";
- NIST SP 800-53A, Appendix C, "Assessment Method Descriptions"; and
- Any in-person observations of security requirement objectives as discussed in activity P.11.

1.11. The Assessment Team shall not speculate, intimate, nor make any preliminary determination of the OSC's likelihood of a successful assessment outcome and subsequent issuance of a Certificate of CMMC Status. The sole purpose of this activity is to confirm that the OSC is sufficiently prepared to begin the evaluative portion of the assessment in Phase 2.

Compose the Assessment Team

1.12. **The C3PAO shall compose the CMMC Assessment Team as established and defined in 32 CFR §170.11(b)(10).** The C3PAO should propose to the OSC the names of the CMMC Certified Assessors (CCAs) and CMMC Certified Professionals (CCPs) that it intends to assign to the Assessment Team.

1.13. The C3PAO shall have implemented the personnel procedures established in Section 6.15 and 6.16 of ISO/IEC 17020:2012 in composing its Assessment Team.

1.14. The C3PAO is responsible for managing impartiality and identifying any conflicts of interest of the members of the Assessment Team prior to the commencement of Phase 2 activities. This responsibility cannot be delegated to the Lead CCA or the OSC. Any COI between a member of the Assessment Team and the OSC must be sufficiently mitigated or avoided.

Complete the Pre-Assessment Form

1.15. **The C3PAO shall generate, collect, and document required pre-assessment and planning information and material via the Pre-Assessment Form pursuant to 32 CFR §170.9(b)(8)**. Examples of this material include the OSC CAGE code, SSP title, OSC contact information, Assessment Team information, dates of the assessment, the readiness determination for assessment, and other data. This pre-assessment information is required to be collected and uploaded into CMMC eMASS for DoD program management and oversight purposes.[9]

1.16. The C3PAO may utilize the official CMMC Level 2 Pre-Assessment Form (CMMC_PreAssessment_Template.xlsx) that is available on the CMMC eMASS website. Alternatively, C3PAOs may develop or purchase any tool that is compliant with the CMMC eMASS data standard that can generate pre-assessment data in the required JSON file format.

1.17. The C3PAO shall follow the instructions and guidance for the pre-assessment and planning information and material as contained in "The DoD CMMC eMASS Concept of Operations for CMMC Third-Party Assessment Organizations".

1.18. The C3PAO shall not share any OSC pre-assessment information with any person or organization not involved with that specific CMMC Level 2 certification assessment, except as otherwise required by law.[10]

Conduct Quality Assurance Review of Pre-Assessment and Planning Information

1.19. A C3PAO quality assurance individual shall conduct a quality assurance review of the Pre-Assessment Form upon completion by the CMMC Assessment Team. **For this quality assurance function, the C3PAO shall meet the requirements as outlined in 32 CFR §170.9(b)(13).**

Upload Pre-Assessment Form into CMMC eMASS

1.20. Upon completion of a satisfactory quality assurance review, a quality assurance individual shall upload the pre-assessment form into the CMMC instantiation of eMASS. **The C3PAO shall follow the CMMC eMASS data standard and upload procedures as set forth in "The Department of Defense CMMC eMASS Concept of Operations for CMMC Third-Party Assessment Organizations".**

1.21. Phase 1 of the CMMC Level 2 certification assessment concludes upon the successful upload of the Pre-Assessment Form into CMMC eMASS.

---

[9] 32 CFR § 170.9(b)(8)

[10] 32 CFR § 170.11(b)(9)

Adverse Determination of Assessment Readiness

1.22. In the event the Lead CCA determined that the OSC was not sufficiently prepared to undergo the CMMC Level 2 certification assessment, they should directly inform the Affirming Official of their decision and provide a full explanation in writing to the OSC as to why the recommendation to suspend the Assessment was made, without providing any remedial advice as to how the OSC could improve its documentation and preparation for the assessment.

1.23. **Under no circumstances shall the C3PAO, its Assessment Team, or any other affiliated personnel offer any advice, implementation assistance, or recommendations as to how the OSC can improve or enhance their preparedness for a replanned or rescheduled CMMC Level 2 certification assessment and, pursuant to the CMMC Code of Professional Conduct (CoPC), doing so would conflict the C3PAO from eventually resuming the suspended CMMC certification assessment with that specific OSC.**

1.24. In the event the OSC decides to cancel or postpone the assessment, both parties should settle all affairs, as appropriate to the terms of their agreement, including the return of any OSC proprietary information. The C3PAO and the OSC should discuss, in general terms, the option of revisiting the CMMC Level 2 certification assessment when the OSC is fully prepared, as well as the anticipated timelines for resuming the suspended assessment and returning to complete the Phase 1 pre-assessment.

1.25. In the event of an assessment postponement or cancellation, the C3PAO shall still complete, review, and upload the Pre-Assessment Form into the CMMC instantiation of eMASS as described in previous activities 1.13 through 1.19.

PHASE 2 – ASSESS CONFORMITY TO SECURITY REQUIREMENTS

The purpose of Phase 2 is to assess the implementation of CMMC Level 2 security requirements—both in depth and coverage — by the OSC and determine if it has met the assessment objectives of NIST SP 800-171A.

The C3PAO shall conduct the CMMC Level 2 certification assessment in accordance with 32 CFR § 170.17, NIST SP 800-171A, this document (the "CAP"), and ISO/IEC 17020:2012, "Conformity Assessment—Requirements for the operation of various types of bodies performing inspection."

Conduct In-Brief Meeting

2.1. The Lead CCA shall convene an In-Brief Meeting prior to the commencement of assessing the implementation of CMMC security requirements of the OSC. This In-Brief Meeting may be conducted in-person, virtually, or in a hybrid manner. The purpose of the In-Brief Meeting is to establish a common understanding of the assessment objectives, procedures, roles and responsibilities, and schedule.

2.2. The Lead CCA shall ensure that official minutes or a detailed meeting summary of the kickoff, including all questions and answers, shall be documented and retained by the C3PAO.

2.3. Attendees for the in-brief meeting shall include, but are not limited to, the Lead CCA, the Affirming Official, the OSC POC, and the Assessment Team members. If a member of the CMMC Assessment Team is unable to attend the In-Brief Meeting, the Lead CCA shall still inform the OSC of the identity of the absent member(s) and facilitate an introduction to the OSC at a subsequent juncture of the assessment.

2.4. The OSC may elect to have additional employees, consultants, ESP personnel, and any observers present at the In-Brief Meeting. If the C3PAO desires additional individuals external to the CMMC Assessment Team to be present or to observe the actual assessment, it must receive permission from the Affirming Official or OSC POC to do so.

2.5. The Lead CCA shall, at a minimum, address the following issues with the OSC during the In-Brief Meeting:

- Introduce the Assessment Team members and invite the introduction of key OSC personnel and support staff;
- Confirm the CMMC Assessment Scope;
- Explain CMMC Level 2 assessment procedures as established in 32 CFR §170.17(c);
- Review the assessment schedule;

- Reconfirm the absence of, or disclose, any organizational or individual conflicts of interest;
- Inform the OSC of its rights to appeal the assessment results and describe the C3PAO's appeals process; and
- Invite any questions or issues for clarification from the OSC.

Assess Implementation of Security Requirements

2.6. The Assessment Team shall evaluate the OSC's implementation of security requirements in accordance with NIST SP 800-171A (current applicable version) and 32 CFR §170.17(c). The three (3) assessment methods of examine, interview, and test, as outlined in NIST SP 800-171A, shall be adhered to by all Assessment Team CCAs assessing security requirements.

2.7. Upon mutual agreement, the parties may conduct much of the evidence collection and evaluation process virtually, using a stable and commercially secure video conference system or web-based collaboration platform. The C3PAO should make the final decision on whether to conduct some eligible evidence collection activities virtually or in person, based on internal procedures and risk evaluation. In a virtual assessment arrangement, the C3PAO and OSC shall ensure that CUI is not shared electronically as part of the evidence collection and evaluation process, unless the assessment is conducted within CMMC Level 2-conforming environments on both sides.

Apply Sampling Values for Depth and Coverage

2.8. The Assessment Team's optimal sampling aims to balance ensuring sufficient evaluation of assets, people, policies, and procedures to achieve an accurate and proper determination of conformity with the need to conduct an efficient, manageable, and cost-effective assessment. Achieving that balance involves selecting representative samples of evidence to be tested or inspected, while minimizing the risk of overlooking non-conforming items.

2.9. **For CMMC Level 2 certification assessments, the Assessment Team shall use a nonstatistical sampling approach in accordance with NIST SP 800-171 R2, Appendix D, "Assessment Method Descriptions". The Assessment Teams shall employ the FOCUSED value for both depth and coverage in evaluating all Level 2 security requirements, as applicable.**

2.10. The Assessment Team should increase the sample for evaluation once it encounters questionable, insufficient, or inadequate evidence for a CMMC security requirement.

2.11. When encountering multiple CAGE codes in a given assessment, the Assessment Team shall ensure that all CAGE codes have been accounted for in the sampling approach.

2.12. When encountering multiple physical locations, the Assessment Team should consider in its sampling approach whether different locations use different physical control methods, whether scan results cover systems at all locations, and whether defined system boundaries account for all physical locations.

Conduct Assessment Scoring

2.13. **The Assessment Team shall employ the CMMC Level 2 Scoring Methodology as established in 32 CFR §170.24 that provides a measurement of the OSC's implementation of the NIST SP 800-171 R2 security requirements.**

2.14. The DoD CMMC Scoring Methodology should be referenced for the following:

2.14.1. Assessment Findings: **32 CFR §170.24(b)**

- Assessment requirements *for* ***Met*** findings, including enduring exceptions and temporary deficiencies;
- Assessment requirements for ***Not Met*** findings; and
- Assessment requirements for ***Not Applicable*** findings.

2.14.2. Scoring: **32 CFR §170.24(c)**

- Assessment requirements for ***Basic Security Requirements*** scoring; and
- Assessment requirements for ***Derived Security Requirements*** scoring.

2.15. Assessors may re-evaluate NOT MET security requirements during the assessment and for ten (10) business days following the active assessment period (*i.e.*, the conclusion of Phase 2 activities) **in accordance with the requirements established in 32 CFR §170.17(c)(2).**

Address External Service Providers

2.16. **The Assessment Team shall determine the OSC's utilization and disposition of an in-scope ESP as established in 32 CFR §170.16(a)(3) and 32 CFR §170.16(a)(2), respectively.** In addition, the CMMC PMO has published Frequently Asked Questions (FAQ) on this issue that should be consulted for additional clarification on the use of ESPs.

2.17. The Assessment Team shall evaluate that the Customer Responsibility Matrix (CRM) of an ESP is up-to date, includes all relevant parties with security responsibilities, and addresses all in-scope CMMC security requirements performed wholly, partially, or jointly by the ESP.

2.18. When an Assessor employs the interview method to validate a security requirement on the CRM that is assigned to the ESP, the ESP respondent must demonstrate sufficient knowledge and credible "ownership" of that requirement—no different than that which is required for an OSC representing a security requirement under its own responsibility. The Assessment Team should also employ the examine and test methods when evaluating the inheritance claims made in the CRM by the OSC.

2.19. In the event the OSC is utilizing a "non-CSP" ESP that voluntarily attained a Level 2 or Level 3 Certificate of CMMC Status, the Assessment Team should anticipate and accept a lower level of effort on behalf of the ESP during the OSC's assessment.[11] Specifically, if the Assessment Team confirms the ESP is in possession of a valid Certificate of CMMC Status, it may consider those

[11] 32 CFR §179.19(c)(2)(ii)

security requirements under the responsibility of the ESP to be in a validated state. The Assessment Team shall still ensure that each inherited security requirement from the ESP is still implemented and currently being maintained in the state under which it was originally assessed and/or have the ESP attest to same. ESP personnel still need to participate during Phase 2 of the OSC's assessment to answer questions of the Assessment Team.

Address Cloud Service Providers

2.20. If the OSC represents that the CSP cloud environment supporting them is currently Authorized at the Moderate baseline within FedRAMP, the Assessment Team shall verify said Authorization by referring to the FedRAMP Marketplace at https://marketplace.fedramp.gov/products and identifying the name of the CSP under the column heading "Provider". The Assessment Team shall then ascertain if **the specific cloud service offering that is documented in the OSC's SSP** is listed under the column heading "Service Offering". The Assessment Team can then determine the current Authorization baseline and status of the cloud offering by checking both the "Impact Level" and "Status" column headings. If the above condition is satisfied, the FedRAMP Moderate (or higher) baseline of the CSP's cloud service offering shall be accepted and noted as such in the assessment results.

2.21. If the OSC represents that the CSP cloud environment supporting them within their CMMC Assessment Scope *is not* FedRAMP Authorized **but meets the security requirements of FedRAMP Moderate (or higher) *equivalency*,** the Assessment Team shall determine if equivalency has been attained in accordance with **current DoD CIO policy on equivalency at the time of the OSC's Level 2 certification assessment.**[12]

2.21.1. During the OSC's CMMC Level 2 certification assessment, the Assessment Team shall verify that the CSP's FedRAMP Moderate Equivalency body of evidence (BOE), as presented by the OSC, is complete, intact, and within the established periodicity, as required. The Assessment Team shall employ the following definitions when reviewing the BoE:

- **Complete:** all required elements of the BoE have been compiled and presented to the C3PAO for review;
- **Intact:** each element of the BoE is presented in full and is not missing any critical sections, pages, or material information; and
- **Established Periodicity:** any element that has a temporal requirement (*e.g.*, must be completed annually) has been completed within the specified timeframe.

If the Assessment Team determines that all elements of the cloud service offering's BoE are complete, intact, and within the established periodicity, then FedRAMP Moderate Equivalency of that cloud service offering has been verified for the CMMC Level 2 certification assessment and shall be denoted as such in the assessment results.

2.21.2. In reviewing the BoE, the Assessment Team is *not* evaluating the CSP's cloud service offering for conformance to the FedRAMP Moderate standard. Nor is the CMMC

[12] 32 CFR §179.17(c)(5)(ii)

Assessment Team conducing a qualitative examination of any element of the BoE, including testing results. Rather, the CMMC Assessment Team is conducting a review of the BoE to verify that it is complete, intact, and within established periodicity.

Conduct Quality Assurance Reviews

2.22. **The C3PAO shall conduct quality assurance reviews during the assessment pursuant to 32 CFR §170.19(b)(14).** These reviews are in addition to the quality assurance requirements pertaining to the Pre-Assessment Form and the Final Assessment Report as discussed in Phases 1 and 3, respectively, and include conducting observations of the Assessment Team's conduct and management of the CMMC assessment process. These reviews shall be performed by a quality assurance individual who is not a member of the Assessment Team.

Convene Daily Checkpoint Meetings

2.23. The Assessment Team shall host a Daily Checkpoint Meeting with the OSC POC and other OSC personnel at the end of each assessment day to summarize progress, identify any challenges, and discuss additional items for coordination.

PHASE 3 – COMPLETE AND REPORT ASSESSMENT RESULTS

The purpose of Phase 3 is to complete, review, report, and submit the assessment results of the CMMC Level 2 certification assessment. By the time the assessment reaches Phase 3, all evaluative activity of the OSC's implemented security requirements and examination of evidence shall have been completed by the Assessment Team.

Compile and Compose Assessment Results

3.1. Upon conclusion of the evaluative activity in Phase 2, the Assessment Team shall compile the assessment results and begin composing the results in the required format for eventual upload into the CMMC instantiation of eMASS.

3.2. **The C3PAO shall follow the CMMC eMASS data standard as set forth in "The Department of Defense CMMC eMASS Concept of Operations for CMMC Third-Party Assessment Organizations".**

3.3. C3PAOs may utilize the CMMC Level 2 Assessment Results Template that is available on the CMMC eMASS website. Alternatively, C3PAOs may develop or purchase any tool that is compliance with the CMMC eMASS data standard that can generate assessment results data in the required JSON file format.

3.4. If the Lead CCA determines that all security requirements have been implemented and thus MET, the certification assessment results will reflect a recommendation for a CMMC Level 2 **Final** Certificate of CMMC Status for the OSC's in-scope data environment.

3.5. If the Lead CCA determines that all security requirements have been implemented and thus MET, with the exception of those security requirements that are documented on an existing and valid POA&M **that is in accordance with 32 CFR §170.21, "Plan of Action and Milestone requirements,"** the certification assessment results will reflect a recommendation for a CMMC Level 2 **Conditional** Certificate of CMMC Status for the OSC's in-scope data environment.

3.6. If the Lead CCA determines that all security requirements have not been implemented and thus NOT MET and/or a valid POA&M is not attainable, the certification assessment results will reflect a recommendation for no issuance of a Level 2 Certificate of CMMC Status.

Conduct Quality Assurance Review

3.7. The C3PAO shall conduct a formal quality assurance review of the certification assessment results. The C3PAO shall conduct the quality assurance review of the certification assessment results ***prior to*** the conduct of the Out-Brief Meeting with the OSC.

3.8. The C3PAO shall ensure that any individual(s) fulfilling this quality assurance function **must be a CCA and cannot be a member of the CMMC Assessment Team conducting the CMMC Level 2 certification assessment for which they are performing the quality assurance function**. The CCA conducting the quality assurance review shall also not have any interaction with the CMMC Assessment Team relating to the conduct of the CMMC Level 2 certification assessment while it is in progress prior to conduct of the quality assurance review itself.

3.9. The C3PAO quality assurance review of the CMMC Level 2 certification assessment results shall, at a minimum, incorporate quality checks on the accuracy and completeness of the evaluation of all security requirements as well as the conformance to the required reporting formats and incorporated data fields for each.

Convene Out-Brief Meeting

3.10. The Lead CCA will convene the Out-Brief Meeting upon the compilation, composition, and quality review of the assessment results. If the OSC has elected to request a re-evaluation of a security requirement pursuant to 32 CFR §170.17(c)(2), "Security requirement re-evaluation," the Lead CCA will convene the Out-Brief Meeting no sooner than ten (10) business days upon conclusion of all evaluative activity in Phase 3. The Out-Brief Meeting may be conducted in-person, virtually, or in a hybrid manner. The purpose of the Out-Brief Meeting is to convey the results of the assessment to the OSC.

3.11. Attendees for the out-brief meeting shall include, but are not limited to, the Lead CCA, the OSC Official, the OSC POC, and all Assessment Team Members. If a member of the CMMC Assessment Team is unable to attend the Out-Brief Meeting, the Lead CCA shall inform the OSC of the identity of the absent member(s). The OSC retains the right to insist upon the presence of all CMMC Assessment Team members at the Out-Brief Meeting and, should they do so, the Out-Brief Meeting shall not be conducted until all CMMC Assessment Team members are available to participate or until which time the OSC agrees to proceed with the Out-Brief Meeting without full attendance by the CMMC Assessment Team.

3.12. The OSC may elect to have additional employees, consultants, ESP personnel, and any observers present at the Out-Brief Meeting. If the C3PAO desires additional individuals external to the Assessment Team to be present at the Out-Brief Meeting, it must receive permission from the Affirming Official or OSC POC to do so.

3.13. The Lead CCA shall ensure that official minutes or a detailed meeting summary of the Out-Brief Meeting, including all questions and answers, are documented and retained by the C3PAO.

3.14. The Assessment Team shall prepare and deliver an Assessment Results Briefing documenting the certification assessment results for presentation to the OSC during the Out-Brief Meeting.

The Assessment Results Briefing shall be developed within a common presentation application (*e.g.* Microsoft PowerPoint, Google Slides, Apple Pages) and can be provided in PDF file format as well.

The following information should be included in the Assessment Results Briefing and addressed during the Out-Brief Meeting:

- Cover page with C3PAO logo, name of Lead CCA, and date of Out-Brief Meeting;
- Dates during which the CMMC Level 2 certification assessment was conducted;
- Name of the OSC;
- CAGE code(s) of the entity/entities associated with the data environment that was assessed;
- Unique Identifier (UID) from SPRS of the system previously self-assessed (if one exists);
- Short name and/or description of the assessment enclave or network that was assessed; the environment that was assessed;
- Final MET / NOT MET / NA determination for each security requirement;
- Status of POA&Ms *(if applicable)*;
- Determination of CMMC Level 2 Certificate of CMMC Status to be issued or denied;
- Artifact retention and integrity procedures (*i.e.,* hashing requirements*)*;
- Proprietary information return and/or destruction per NDA or contract; and
- Summary of OSC Assessment Appeal rights and C3PAO appeals process.

3.15. **Under no circumstances shall the Assessment Results Briefing contain any information that communicates, references, or insinuates any recommended or suggested remedial actions that the OSC could or should consider based on the results of the assessment.**

3.16. The Assessment Team shall inform the OSC that the hashed artifacts used as evidence for the assessment must be retained by the OSC for six (6) years from the CMMC Status Date that will appear on their Certificate of CMMC Status.[13] The Assessment Team shall inform the OSC that it must hash the artifact files using a NIST-approved hashing algorithm. The OSC must provide the Assessment Team with a list of the following for upload into CMMC eMASS.:

- Names of all artifacts;
- Return values of the hashing algorithm; and
- Hashing algorithm.

Additional guidance for hashing artifacts can be found in the supplemental guidance document, "CMMC Hashing Guide" available at https://DoDcio.defense.gov/CMMC/.

Upload Certification Assessment Results into CMMC eMASS

3.17. A C3PAO quality assurance individual shall upload the certification assessment results into CMMC eMASS. **The C3PAO shall follow the CMMC eMASS data standard and upload**

[13] 32 CFR §170.17(c)(4)

procedures as set forth in current version of "The Department of Defense CMMC eMASS Concept of Operations for CMMC Third-Party Assessment Organizations".

3.18. C3PAOs may utilize the certification assessment results template provided by DoD (CMMC_AssessmentResults_Template.xlsx) that is available on the CMMC eMASS website.

3.19. Although CMMC Level 2 certification assessment results at the point of creation may not necessarily meet the formal definition of Controlled Unclassified Information (CUI), **C3PAOs and their CMMC Assessment Teams shall process, store, and transmit CMMC Level 2 certification assessment results as if those assessment results, were, in fact, CUI.**

3.20. **Accordingly, the C3PAO shall utilize their IT environment that is resident within their CMMC Level 2 Assessment Scope as assessed by the Defense Industrial Security Cybersecurity Assessment Center (DIBCAC)—as a qualifying condition of their C3PAO authorization or accreditation—for the purposes of accessing and uploading CMMC Level 2 certification assessment results into CMMC eMASS.** Specifically, the user workspace that is used to upload CMMC Level 2 certification assessment results to CMMC eMASS shall be one that exists within the scope of the C3PAO's DIBCAC-assessed environment. There will be no "system-to-system" connections from C3PAOs to CMMC eMASS, so a valid user workspace or end point is required.

3.21. The C3PAO quality assurance individual shall ensure that the OSC's hashing data is incorporated into the certification assessment results prior to uploading into CMMC eMASS.

3.22. Once the certification assessment results are uploaded into CMMC eMASS, if the results warrant a determination of either FINAL or CONDITIONAL CMMC Status of Level 2 (C3PAO) for the OSC, the quality assurance individual will receive from CMMC eMASS the following information: 1) a confirmation of the FINAL or CONDITIONAL CMMC Level 2 Status; 2) an assessment unique Identifier (UID); and 3) the CMMC Status Date of record for the determination.

Administer Assessment Appeals (if required)

3.23. The C3PAO shall address any appeals of the Assessment Team's findings, results, and/or Certificate of CMMC Status determination that is received by the OSC **in accordance with 32 CFR §170.9(b)(19)** and its own internal assessment appeals process. The OSC must file an initial appeal with the same C3PAO that conducted its CMMC Level 2 certification assessment.

3.24. The C3PAO shall have an assessment appeals process, in accordance with ISO/IEC 17020 (2012), on file with The Cyber AB. The C3PAO's assessment appeals process shall have a time-bound, internal appeals process clearly identified to address all appeals received. The C3PAO shall follow its own published assessment appeals process and shall not deviate from the version that is on file with The Cyber AB.

3.25. A quality assurance individual who is a CCA shall manage within the C3PAO's assessment appeals process the OSC's Level 2 certification Assessment Appeal. The quality assurance individual assigned to manage the OSC's Assessment Appeal **cannot be a member of the CMMC Assessment Team that conducted the CMMC Level 2 certification assessment.** In addition**,** if the quality assurance individual managing the OSC Assessment Appeal performed

any quality assurance reviews of the assessment in question, that individual shall not be involved in determining the final decision on the Appeal.

3.26. The C3PAO shall complete its assessment appeals process and render a decision on the OSC's assessment appeal. The adjudication decision of the assessment appeal must be conveyed to the OSC in writing with its supporting rationale.

3.27. The C3PAO shall enter the required Assessment Appeal information into the assessment appeals template required for CMMC eMASS. The quality assurance individual managing the OSC's Assessment Appeal shall perform a quality review of the assessment appeals template prior to it being uploaded to CMMC eMASS.

3.28. Should the OSC refute or oppose the adjudication decision of their Assessment Appeal by the C3PAO, they may elevate their appeal to The Cyber AB. The OSC must elevate its appeal to The Cyber AB within fifteen (15) business days of receiving the adjudication decision of their Assessment Appeal by the C3PAO in writing. **All Assessment Appeals decisions rendered by The Cyber AB are final**. The Assessment Appeals Process of The Cyber AB may be found on www.cyberab.org.

PHASE 4 – ISSUE CERTIFICATE AND CLOSE OUT POA&M

The final phase of the CMMC Level 2 certification assessment centers on the C3PAO issuing a CMMC Level 2 Certificate of CMMC Status to the OSC, as well as closing out any Plan of Action and Milestones (POA&Ms) that might exist.

The completion of Phase 4 brings the CMMC Level 2 certification assessment to its formal conclusion.

Generate Certificate of Status

4.1. Upon receipt from CMMC eMASS of the confirmation of CMMC Level 2 Status (FINAL or CONDITIONAL), the UID, and CMMC Status Date following the submission of the certification assessment results, a quality assurance individual shall generate the Certificate of Status for approval and issuance to the C3PAO.

4.2. The C3PAO shall only use the standardized CMMC Level 2 Certificate of CMMC Status templates (FINAL and CONDITIONAL) that are approved and provided by The Cyber AB.

4.3. All C3PAO-generated Certificates of CMMC Status must be approved and signed only by an Authorized Certifying Official that is on file with The Cyber AB.

4.4. When generating the Certificate of CMMC Status, a quality assurance individual shall enter, affix, or retain the following required information to the document prior to approval and signature by the Authorized Certifying Official:

4.4.1. OSC full legal name;

4.4.2. All industry CAGE codes associated with the information systems addressed by the CMMC Assessment Scope;

4.4.3. Short description of the information system assessed;

4.4.4. Unique identifier (UID) received from CMMC eMASS;

4.4.5. Dates of assessment (beginning of Phase 1 to date of Out-Brief Meeting);

4.4.6. CMMC Status Date;

4.4.7. CMMC Level;

4.4.8. Statement of conformity to NIST SP 800-171 R2;

4.4.9. Name and Logo of C3PAO;

4.4.10. Logo of the CMMC Program;

4.4.11. C3PAO authorization or accreditation badge with ID number; and

4.4.12. Signature block for Authorized Certifying Official.

Issue Certificate of CMMC Status

4.5. Upon generation of the Certificate of CMMC Status, an Authorized Certifying Official shall review and sign the Certificate to convey formal issuance on behalf of the C3PAO.

4.6. The C3PAO shall produce the approved Certificate of CMMC Status in PDF file format.

4.7. A C3PAO quality assurance individual shall upload the Certificate of CMMC Status into CMMC eMASS **in accordance with the current version of the "Department of Defense CMMC eMASS Concept of Operations for CMMC Third-Party Assessment Organizations".**

4.8. The C3PAO shall deliver, either in electronic or physical form, a copy of the CMMC Level 2 Certificate of CMMC Status to the Affirming Official, and the OSC POC. The CMMC Level 2 Certificate of CMMC Status is not considered CUI and is not required to be stored, processed, or transmitted as such.

4.9. The C3PAO shall deliver an electronic copy of the Certificate of CMMC Status to The Cyber AB via the certificates@cyberab.org account.

Close-Out POA&M

4.10. An OSC that has been issued a CONDITIONAL Level 2 Certificate of CMMC Status may retain the services of an authorized or accredited C3PAO to close out a Plan of Action & Milestones (POA&M). The OSC may engage a C3PAO *different* from the C3PAO that conducted Phases 1 through 3 of the applicable CMMC Level 2 certification assessment and issued the CONDITIONAL Level 2 Certificate of CMMC Status. In this situation, the POA&M Closeout C3PAO assumes the responsibility for FINAL CMMC Status determination and, if the POA&M satisfies the closeout requirements, issues the Level 2 FINAL Certificate of CMMC Status to the OSC.

4.11. The C3PAO shall conduct and document a conflict-of interest disclosure and mitigation review prior to commencing a POA&M closeout for the OSC.

4.12. **The C3PAO shall follow the procedures and meet the requirements for closing out a POA&M as established in 32 CFR part 170.17(a)(1)(ii)(B).**

4.13. A quality assurance individual shall conduct a quality assurance review of the POA&M close-out upon completion by the Assessment Team. The C3PAO shall ensure that any individual(s) fulfilling this quality assurance function **must be a CCA and cannot be a member of the CMMC**

Assessment Team conducting the POA&M closeout assessment for which they are performing the quality assurance function.[14]

4.14. The C3PAO quality assurance review of the POA&M closeout shall, at a minimum, incorporate quality checks on the accuracy and completeness of the evaluation of all POA&M security requirements as well as the conformance to the required reporting formats and incorporated data fields for each. The C3PAO shall conduct the quality assurance review of the CMMC POA&M closeout ***prior to*** its upload into CMMC eMASS.

4.15. The Assessment Team may choose to offer the OSC a POA&M Out-Brief Meeting, but one is not required. The Assessment Team is required to convey the results of the POA&M closeout in writing and convey the remaining administrative next steps to the OSC.

4.16. In the event the C3PAO refutes the findings of the CMMC Assessment Team during the POA&M closeout, they retain the right to appeal the findings, results, and/or CMMC Level 2 Status decision. The process and timelines for administering and adjudicating a POA&M closeout appeal are identical to those of established in Phase 3, with the exception that the assessment appeals process of the Phase 4 C3PAO that closed out the POA&M is controlling and shall be followed.

4.17. Upon conclusion of the POA&M closeout and quality assurance review, the C3PAO shall submit the POA&M closeout results to CMMC eMASS. If the POA&M was satisfactorily closed out, the C3PAO shall then issue a FINAL Level 2 Certificate of CMMC Status, utilizing the same procedures and following the same requirements as established above in activities 4.1 through 4.9.

[14] 32 CFR §170.9(14)