PRE-DECISIONAL **DRAFT**

Cybersecurity Maturity Model Certification (CMMC)

CMMC ASSESSMENT PROCESS (CAP)

Version 1.0

July 2022

THIS DOCUMENT HAS NOT YET BEEN ENDORSED BY THE DEPARTMENT OF DEFENSE AND IS NOT YET AUTHORIZDD FOR USE IN CMMC CERTIFICATION ASSESSMENTS

PRE-DECISIONAL **DRAFT**

This page intentionally left blank.

DISCLAIMER

The view, 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.

NO WARRANTY. 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.

TABLE OF CONTENTS

This page intentionally left blank.

INTRODUCTION TO THE CMMC ASSESSMENT PROCESS (CAP)

The Cybersecurity Maturity Model Certification (CMMC) framework is the Department of Defense's (DoD) unifying standard for the implementation of cybersecurity measures within the Defense Industrial Base (DIB).

The CMMC Assessment Guides that are developed, maintained, and published by DoD provide the objectives, specific criteria, and technical guidelines for assessing the conformance of DIB organizations seeking CMMC Certification to the applicable cybersecurity practices of the CMMC standard, which is grounded in the National Institute of Standards and Technology (NIST) Special Publication 800-171. These guides serve as the controlling technical authority for the purposes of assessing the implementation of CMMC practices.

The *CMMC Assessment Process* (CAP), by comparison, **is the CMMC doctrine providing the overarching procedures and guidance** for CMMC Third-Party Assessment Organizations (C3PAOs) conducting official CMMC Assessments of organizations seeking CMMC Certification.

This version of the CAP applies to Level Two (L2) of the CMMC Model only.

The CAP, developed and maintained by the CMMC Accreditation Body and reviewed and endorsed by DoD, is an element of official CMMC canon and adherence to its procedures is required by C3PAOs and their Assessors. While tailored for specific use by C3PAOs, Certified CMMC Assessors (CCAs), and Certified CMMC Professionals (CCPs), it is intended as a resource for the entire CMMC Ecosystem.

The CAP is organized across four (4) phases and describes the required activities to ensure that CMMC Assessments are conducted consistently across the DIB. The four phases are:

- Phase 1: "Plan and Prepare the Assessment";
- Phase 2: "Conduct the Assessment";
- Phase 3: "Report Assessment Results"; and
- Phase 4: "Close-Out POA&Ms and Assessment" *(if necessary)*.

These four (4) phases have been designed to ensure that every CMMC Assessment meets the following objectives:

- Achieve the highest possible accuracy, fidelity, and quality for CMMC Assessments conducted by C3PAOs;
- Maximize consistency to ensure that different Assessments conducted by different C3PAOs and Assessors yield the same verifiable results and outcomes each time;
- Improve the cybersecurity defensive posture and the cyber resiliency of the DIB by providing effective and efficient Assessments that are well-planned, executed in consistent fashion, and accurately reported.

The CAP is designed to be used in conjunction with other official doctrine and publications within the CMMC Ecosystem, including the *CMMC Model Overview*, *CMMC Assessment Guide—Level* 2, *CMMC Scoping Guidance—Level 2*, the "CMMC eMASS Concept of Operations for CMMC Third Party Assessment Organizations," and the "CMMC Artifact Hashing Tool User Guide". Many of these documents are available on the official DoD CMMC website at www.acq.osd.mil/cmmc.

Comments on this document, as well as on the overall CMMC framework, are welcomed from all members of the CMMC Ecosystem and the public. This feedback will be used to improve the CAP and may help inform future adjustments to the CMMC Model itself. Feedback can be submitted via the DoD CMMC website www.acq.osd.mil/cmmc/contact-us.html or also via the CMMC Accreditation Body address at cmmcsupport@cyberab.org.

This page intentionally left blank.

Document Conventions

Various syntax, naming, and terminology specifications are employed throughout this document.

Category	Convention
Body Typeface	Arial
Body Font	10 Regular
Phase Heading Font	14 CAPS
Section Heading Font	12 CAPS
Table Headings Font	9 Bold
Auxiliary Verb of Compulsion	“Shall”, connoting a requirement
Capitalized Terms	Assessment
	Assessment Team Member
	Assessor
	C3PAO Assessment Team
	Certification
	CMMC Quality Assurance Professional
	Defense Industrial Base
	Evidence
	External Cloud Service Provider
	Final Findings Briefing
	Headquarters Unit
	Host Unit
	Lead Assessor
	Limited Practice Deficiency Correction
	Organization Seeking Certification
	OSC Assessment Official
	OSC Point of Contact
	Registered Practitioner
	Registered Practitioner Organization
	Supporting Organization

This page intentionally left blank.

PHASE 1 – PLAN AND PREPARE THE ASSESSMENT

A strong and effective CMMC Certification Assessment begins with a well-organized planning and preparation effort. The critical foundation for a successful Assessment engagement between CMMC Third-Party Assessment Organizations (C3PAOs) and Organizations Seeking Certification (OSCs) is established in Phase I.

All activities in Phase I are necessary to ensure the conduct of a proper and consistent CMMC Assessment. Phase I Assessment planning could range from one (1) to several days, depending on C3PAO-OSC communication effectiveness and the OSC's readiness and ability to provide the required information, including Evidence of CMMC practice implementation. An OSC's understanding of the CMMC practices and its preparation for the Assessment—including the fidelity and accuracy of its proposed CMMC Assessment Scope—is the primary driver on how efficiently Phase I might be completed.

1.1 Receive CMMC Assessment Request from OSC

An OSC generally initiates the engagement concerning a prospective CMMC Assessment by contacting an authorized C3PAO. The updated registry of authorized C3PAOs in good standing is maintained in the CMMC Marketplace website administered by the CMMC Accreditation Body (The Cyber AB). Unless otherwise notified by The Cyber AB, any C3PAO listed as "Authorized" within the Marketplace may be considered a C3PAO in good standing and eligible to conduct a CMMC Assessment. The initial contact from the OSC can be made via the CMMC Marketplace's online intake form or by direct email or phone call to the C3PAO. C3PAO-OSC contact and communications may be initiated by either party, but in no circumstances will individuals from The Cyber AB nor the Department of Defense serve in an introductory or facilitation role.

Once the request for a CMMC Assessment is received, the C3PAO should respond to the OSC within five (5) business days, acknowledging the request and proposing the scheduling of an initial coordination call or virtual meeting. During this initial exchange, the C3PAO should confirm the requested timeframes and geographic location(s) for the Assessment and attempt to ascertain the general preparedness of the OSC for a CMMC Level 2 Assessment. This could include asking any outstanding questions or requesting missing information from the initial request submission.

The OSC shall communicate the general parameters of its Assessment requirements, including the projected timeframe of when it would be ready for an Assessment and the physical location of its corporate assets that would be included in its CMMC Assessment Scope.

Note: the OSC's initial request may also include the identification or preference for a specific Lead Assessor or CMMC Assessment Team Member, but the authority and decision for selecting and assigning the CMMC Assessment Team rests solely with the C3PAO.

1.2 Establish Roles and Responsibilities

A consistent, accurate, fair, and efficient CMMC Assessment requires the active engagement, communication, and attention of several key figures and entities, upon each of whom rests specific responsibilities:

- **Organization Seeking Certification (OSC):** The OSC is the Defense Industrial Base (DIB) company, organization, university or college, legal entity, or discrete business division or practice area that is pursuing CMMC Certification by contracting with a C3PAO and proceeding with a CMMC Assessment. The OSC is responsible for implementing CMMC practices for the target CMMC Level to which they aspire and providing a cooperative environment for the C3PAO to conduct the Assessment.
- **OSC Assessment Official:** The most senior representative of an Organization Seeking Certification who is directly and actively responsible for leading and managing the OSC's engagement in the Assessment and who possesses decision-making authority for the OSC with

regard to the CMMC Assessment. The OSC Assessment Official must be an employee of the organization that is being assessed. Whereas the OSC Assessment Official, as described herein, may not necessarily reside in a single individual in some organizations (*i.e.*, multiple company officials who have the authority to make decisions on behalf of the OSC may be involved in the Assessment), it is important for the C3PAO to identify and designate a single OSC Assessment Official who will be making Assessment-related decisions and agreements.

- **OSC Point of Contact (OSC POC):** The individual within 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 like a CMMC Registered Practitioner (RP).
- **CMMC Third-Party Assessment Organization (C3PAO):** An authorized and independent conformity-Assessment body that contracts with the Organization Seeking Certification to conduct CMMC Assessments and issues the CMMC Certification. Authorized C3PAOs are listed on the CMMC Marketplace.
- **C3PAO Assessment Team:** The representative body of a C3PAO composed of certified personnel who conduct a CMMC Assessment and any additional, non-certified individuals who may provide administrative or logistical support to the Assessment. Also referred to as the "Assessment Team".
- **Lead Assessor:** The CMMC Certified Assessor (CCA) who oversees and manages a dedicated CMMC Assessment Team for the Assessment of an OSC. Lead Assessors hold the formal designation as such from the CMMC Accreditation Body.
- **Assessment Team Members:** Individuals who comprise the C3PAO Assessment Team.
- **CMMC Quality Assurance Professional (CQAP)**: The formally trained individual who is responsible for ensuring Assessment documentation completeness and accuracy. Each C3PAO is required to have at least one (1) CQAP on staff for ensuring all Assessment packages are reviewed and validated for procedural integrity prior to upload into eMASS or any other official CMMC repository system or application.

1.3 Discuss Contractual Arrangements

OSCs retain the services of an authorized C3PAO to conduct a CMMC Assessment. For all CMMC Assessments, the privity of contract exists between the OSC and the C3PAO; neither the CMMC Accreditation Body, Inc. nor the Department of Defense are parties to this agreement. As such, OSCs and C3PAOs are given latitude as to how and when an Assessment engagement is structured and executed, as well as to the specific terms and conditions of the contractual agreement, including pricing and payment considerations. However, all contractual agreements for CMMC Assessments must comport to the CMMC Code of Professional Conduct (*e.g.*, certification "guarantees" are prohibited).

The C3PAO works with the OSC Assessment Official to determine an anticipated level-of-effort and associated cost estimate to conduct the CMMC Assessment. By the completion of Phase 1, all pertinent Assessment planning details will have been gathered, discussed, and reviewed to create the Assessment plan that will be carried out as part of the contract between the C3PAO and OSC. Prior to beginning the Assessment, the contractual agreement between these two parties shall be signed by authorized representatives of the C3PAO and the OSC Assessment Official and executed accordingly in good faith.

1.4 Organize and Prepare Assessment Documents and Templates

The C3PAO Assessment Team shall maintain regular familiarity and currency with the full body of CMMC Assessment doctrine. C3PAOs should have these documents "at the ready" when communicating with OSCs prior to, and during, a CMMC Assessment engagement. In addition to this CAP, the compendium of CMMC doctrine includes the following:

- *Cybersecurity Maturity Model Certification (CMMC) Model Overview*, Version 2.0
- *CMMC Assessment Guide*, Level 2, Version 2.0

- *CMMC Assessment Scope*, Level 2, Version 2.0
- *CMMC eMASS Concept of Operations (CONOPS) for CMMC Third Party Assessment Organizations*; and
- *CMMC Artifact Hashing Tool User Guide*, Version 2.0

Many of the above documents are available for download at the Department of Defense's CMMC Program Management Office website: https://www.acq.osd.mil/cmmc/documentation.html.

In addition, C3PAOs will need to utilize a range of templates throughout a CMMC Assessment engagement in order to properly document Assessment activities and findings. The Cyber AB has prepared the following templates as appendices to this CAP for use by C3PAOs and their Assessment Team Members:

- **CMMC Pre-Assessment Form:** provides the central record and information for the Assessment, to include the documentation of assets and CMMC Assessment Scope, Evidence, and other OSC data. **Use of this template is mandatory.**
- **Virtual Assessment Evidence Preparation Template:** Excel file to support the organization and presentation of Evidence that will be validated virtually during an Assessment. **Use of this template is mandatory.**
- **C3PAO and Assessor Conflict of Interest Attestation:** Short statement in which both the C3PAO and its Assessment Team Members confirm that they have not provided consulting, advisory, or CMMC implementation support to the OSC that they will be assessing and that no conflicts of interest (COI) exist with that OSC. **The use of this template is mandatory.**
- **CMMC Assessment In-Brief:** PowerPoint file that can be used to construct the formal kickoff briefing for the commencement of the actual conduct of the CMMC Assessment (Phase 2). The use of this template is not mandatory.
- **CMMC Assessments Results:** serves as the official file documenting the final results of the CMMC Assessment. **Use of this template is mandatory.**
- **Daily Checkpoint:** PowerPoint file that supports the coordination and tracking of daily Assessment activities. Use of this template is not mandatory.
- **Conditional Practice Deficiency Correction Worksheet:** Documentation of record for any OSC implemented CMMC practices that were assessed with discrepancies that require resolution for a "MET" score. Use of this template is not mandatory.
- **CMMC Assessment Results:** spreadsheet that contains the official record of the Assessment results. **Use of this template is mandatory.**
- **CMMC Assessment Findings Briefing:** PowerPoint file that can be used to construct the reporting of the Assessment results to the OSC. While use of this particular template is not mandatory, the formal brief-out of Assessment results from the C3PAO to the OSC is required.
- **CMMC Assessment Quality Review Checklist:** Checklist of items to be verified during the CMMC Quality Assurance Professional's review of documentation. **Use of this template is mandatory.**
- **Confirmation of Destruction of OSC Data:** MS Word template to be used by the C3PAO to document their surrender and/or destruction of any OSC proprietary information at the conclusion of the Assessment. While use of the particular template is not mandatory, the formal notification that proprietary information is no longer being retained by the C3PAO (in the absence of expressed written consent by the OSC) is required.

Tables 1.1 and 1.2 summarize the CMMC templates and other forms and documents, respectively, that are used or referenced in the CMMC Assessment Process.

Table 1.1 CMMC Assessment Templates

Template Name	Format	Appendix	Phase(s)	Mandatory
CMMC Pre-Assessment Form Template	Excel	D	1	Y
Virtual Assessment Evidence Preparation Template	Excel	E	1	Y
C3PAO and Assessor COI Attestation	MS Word	F	2	N
CMMC Assessment In-Brief	PowerPoint	G	2	N
Daily Checkpoint	PowerPoint	H	2	N
Conditional Practice Deficiency Correction Program Worksheet	PDF	I	2	Y
CMMC Assessment Results	Excel	J	2/3/4	Y
CMMC Assessment Findings Briefing	PowerPoint	K	2	N
CMMC Assessment Quality Review Checklist	PDF	L	3	Y
Confirmation of Destruction of OSC Data	MS Word	M	4	N

Table 1.2 Select CMMC Forms and Documents

Form/Document Name	Format	Appendix	Phase(s)
OSC Self-Assessment Practice Deficiency Tracker	Excel	N	1
CMMC Scoring with DoD Assessment Scoring Methodology	PDF	O	2/4
CMMC Assessor Waiver Process	PDF	P	1
CMMC Assessment Appeals Process	PDF	Q	2
CMMC Assessment Evidence Collection Approaches	PDF	R	2

Note: C3PAOs and their Assessment Team Members shall be familiar with all applicable templates and have them available for use as an engagement with an OSC commences.

1.5 Ascertain Assessment Conditions and Requirements

Upon agreement between the parties (*i.e.*, C3PAO and OSC) to proceed with planning a CMMC Assessment, the C3PAO works with the OSC Assessment Official and the OSC POC to determine the purview and planning details of the Assessment. This will include discussing schedule, size of the organization, personnel, logistics, relevant contractual requirements, and the prospective CMMC Assessment Scope.

It is very important to make a distinction here between the two types of "scoping" activity that a C3PAO will encounter in Phase 1 of a CMMC Assessment: 1) Assessment framing, which is the high-level contract scoping discussed and agreed to at the onset of C3PAO-OSC engagement; and 2) CMMC Assessment Scope, which is an official and technical CMMC term. Both C3PAOs and OSCs must understand the respective definitions of both terms and, to avoid confusion and miscommunication, take measures to use both words in their proper context, and always differentiate between the two:

- **Assessment framing:** the practice of identifying the size, scale, date, time, place, manner, resources, and level-of-effort associated with the prospective conduct of a CMMC Assessment. High-level contract framing is performed jointly by the C3PAO and the OSC and is conducted at the beginning of their engagement.

- **CMMC Assessment Scope:** the boundaries within an organization's networked environment that contain all the assets that will be assessed. CMMC Assessment Scope is initially determined by the OSC and then validated by the C3PAO. More information on how to consider and determine an OSC's proper CMMC Assessment Scope can be found in the DoD manual, *CMMC Assessment Scope - Level 2*.

1.5.1 Frame the Assessment

The C3PAO works with the OSC to frame the Assessment. The initial discussion may be conducted between a C3PAO corporate representative and any OSC representative, including the OSC POC, but follow-on substantive conversations should be between the C3PAO and the OSC Assessment Official.

Note: It is recommended that the C3PAO and OSC sign a non-disclosure agreement (NDA) as part of the initial contractual arrangement in order to protect and give legal grounds to the OSC in the event of disclosure or loss of proprietary information by the C3PAO and/or Assessment Team members.

While it is not recommended, the OSC POC may serve as the OSC Assessment Official if that individual has decision-making authority within the company and is able to bound the OSC in agreements with the C3PAO. The OSC Assessment Official is responsible for ensuring all OSC-required actions during the Assessment are carried out, including the funding and payment for the Assessment. If needed, the OSC Assessment Official can delegate a separate individual within the OSC, in addition to the OSC POC, to serve as an additional OSC representative, who will also work with the Lead Assessor on a regular and operational basis for planning, preparing, and executing the Assessment.

For Assessment framing, the C3PAO and OSC shall discuss and agree upon the following elements of the prospective Assessment:

- Assessment location(s), including what aspects and activities of the Assessment will be conducted virtually;
- Identification of OSC staff that will provide Evidence and support for the Assessment;
- OSC's CMMC Assessment Scope;
- OSC's relevant documentation, including roles and responsibilities of its information and technology and information security staff(s),
- Evidence;
- A rough order-of-magnitude (ROM) estimate for the approximate duration and timing for the Assessment; and
- The Assessment outputs that will be provided to the OSC Assessment Official upon completion of the Assessment; and

Note: only the OSC Assessment Official can agree to and sign and approve the framing and terms of the Assessment, codified in a valid legal contract, once determined through coordination with the Lead Assessor and C3PAO.

1.5.2 Identify Lead Assessor

The C3PAO reviews the CMMC Pre-Assessment Data Form or other initially submitted information and then considers prospective Certified CMMC Assessors to assign as Lead Assessor for the engagement. The C3PAO should consider the experience of the Lead Assessor and how that relates to the size and complexity of the prospective Assessment, the geographical location(s) of the Assessment, the Lead Assessor's familiarity with the OSC's lines of business, and any potential conflicts of interest with the OSC. Once the C3PAO selects and assigns a Lead Assessor, the C3PAO replies to the OSC in writing and introduces the Lead Assessor to begin the engagement with the OSC.

1.5.3 Confirm the Corporate Identity to be Assessed

The Lead Assessor works with the OSC Assessment Official and/or the OSC POC to confirm the specific corporate legal entity that will be assessed, *i.e.*, the precise identity of the actual "Organization Seeking Certification." The actual OSC could be the entirety of the company itself, referred to as the Headquarters Organization (HQ Organization). Alternatively, the actual OSC could be a discrete subsidiary, division, or operating component—referred to as the "Host Unit"—of the larger corporation. It is also important for the C3PAO to understand the existence of any Supporting Organizations affiliated with the OSC that might factor into the CMMC Assessment Scope. The following definitions are used to designate the various elements of an assessed organization:

- **HQ Organization:** The legal entity that will be delivering services or products under the terms of a DoD contract. The HQ Organization itself could be the OSC, or it could designate a Host Unit as the OSC.
- **Host Unit:** The specific people, procedures, and technology within an HQ Organization that would be applied to the DoD contract and that are to be considered the OSC for CMMC Assessment purposes.
  - **Enclave:** A set of system resources that operate within the same security domain and that share the protection of a single, common, and continuous security perimeter. A segmentation of an organization's network or data that is intended to "wall off" that network or database from all other networks or systems. A CMMC Assessment scope can be within the Assessment scope of an enclave.
- **Supporting Organizations:** The people, procedures, and technology external to the HQ Organization that support the Host Unit. The assets affiliated with Supporting Organizations may need to be included as part of the CMMC Assessment Scope, but the Supporting Organizations themselves would NOT receive a CMMC Certification during the OSCs' Assessment.

Table 1.3 Examples of CMMC Organizational Definitions

Name	Unit	Description
Acme Heavy Industries, Inc.	HQ Organization	Parent Company
Acme Defense Mission Systems, Ltd.	Host Unit	OSC
All-American Cloud Services, Inc.	Supporting Organization	Business entity that supports the OSC but may or may not necessarily be part of the CMMC Assessment

The HQ Organization or the Host Unit, depending on the corporate structure, must possess a Commercial and Government Entity (CAGE) code issued by the Department of Defense. The Assessment cannot proceed if the OSC does not have a valid CAGE code. 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).

Note: Small and medium-sized businesses may not have a multi-level corporate architecture that necessitates the delineation of a Host Unit, whereas larger corporations may not necessarily outsource certain functions to Supporting Organizations.

1.5.4 Validate CMMC Assessment Scope

Determining the proper and accurate CMMC Assessment Scope is essential for conducting a valid Assessment. The OSC has the initial responsibility to establish the CMMC Assessment Scope of their networked environment, to include identifying and taking inventory of the various categories of assets contained therein that will be the subject of the CMMC Assessment. For guidance on how to conduct this scoping, refer to the Department of Defense's *CMMC Assessment Scope - Level 2*, December 2021.

The OSC presents the CMMC Assessment Scope to the Lead Assessor, who then proceeds to verify its accuracy and integrity. In support of understanding and interpreting the CMMC Assessment Scope, the OSC must also provide to the Lead Assessor with supporting documentation, such as network schematic diagrams, the System Security Plan (SSP), policies, and organizational charts.

In doing so, the OSC should ensure that any proprietary information is clearly marked as such. If possession of these materials is granted to the Lead Assessor or other Assessment Team Members, a non-disclosure agreement between the OSC and the C3PAO should be considered since a formal Assessment contract may not necessarily exist yet between the parties. Regardless, OSC documentation does not necessarily have to leave OSC control at this point of the process.

Note: Throughout the Assessment engagement, it is neither prohibited nor improper for a C3PAO to receive company proprietary information from the OSC and maintain access and/or possession of such information during the Assessment process. To be clear, however, upon completion of the Assessment or Assessment engagement (in the event the parties do not actually proceed with the Assessment itself) the C3PAO must return and/or destroy any and all OSC proprietary information. It is a violation of the CMMC Code of Professional Conduct (and of the *CMMC Assessment Process*) for a C3PAO to retain OSC proprietary information past the conclusion of the C3PAO-OSC engagement. As previously stated, a non-disclosure agreement should be in place between the parties prior to any proprietary information being shared.

The Lead Assessor is required to validate the OSC's CMMC Assessment Scope. Any disagreements or differences of opinion concerning the CMMC Assessment Scope must be resolved before the actual Assessment may commence.

1.5.4.1 Ascertain the Use of External Cloud Service Providers

During the validation of the CMMC Assessment Scope, the C3PAO may likely encounter the OSC's relationship to Supporting Organizations that are providing "external cloud services" through an external connection under CMMC practice AC.L1-3.1.20, "External connections: Verify and control limit connections to and use of external information systems." Most OSCs with an external connection to cloud services will be expected to meet the requirements described under DFARS 252.201-7012(b)(2)(ii)(D) when they store, process, or transmit CUI (or when they do not store, process, or transmit CUI, but are still in the scope of applicability for inheritance as described in NIST SP 800-171.)

The services of External Cloud Service Providers are at the core of "cloud computing." DFARS 252.239-7010 defines "cloud computing" as:

> *"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 includes other commercial terms, such as on-demand self-service, broach network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-service."*

For CMMC purposes, these Supporting Organizations providing "cloud computing" services to OSCs are considered **External Cloud Service Providers**, which is the term used in DFARS 252.204-7012(b)(2)(ii)(D). External Cloud Service Providers may be characterized informally by the OSC as "cloud service providers" (CSPs), "managed service providers" (MSPs), or other names depending on the services provided. Regardless as to what or how the cloud vendor themselves or the OSC refers to them, the C3PAO must obtain a basic understanding of the relationship between the OSC and its External Cloud Service Providers, which is fundamental to identifying the accurate CMMC Assessment Scope and related shared security requirements.

For additional information on the definition of External Cloud Service Providers, see NIST SP 500-292, "NIST Cloud Computing Reference Architecture," section 2.3.

Ultimately, the OSC is solely responsible for their relationship with any External Cloud Service Provider and how those cloud services that they are receiving are meeting the requirements for CMMC Certification.

Note: OSCs that are **operating an IT service or system on behalf of the Government**, must meet unique

requirements under DFARS 252.204-7012(b)(1)(i). When an OSC meets this description of operating IT services or systems on behalf of the Government, the controlling security standards are established by DFARS 252.239-7010, "Cloud Computing Services."[1] In these instances, CMMC Certification requirements are not applicable, the C3PAO shall refer the OSC to the *DoD Cloud Computing Security Requirements Guide,* and the CMMC Assessment does not proceed.

The vast majority of OSCs, however, will likely not be operating IT services or systems on behalf of the Government. For these OSCs and their External Cloud Service Providers, the cloud security requirements established in DFARS 252.204-7012(b)(2)(ii)(D) are controlling for CMMC Assessments. The OSC is responsible for identifying all External Cloud Service Providers, the external connections to them, the types of external services received under their agreement, and whether or not the external connections are used to store, process, or transmit CUI and FCI. If the External Cloud Service Provider supporting the OSC processes, transmits, or stores CUI, then the External Cloud Service Provider must meet the requirements under DFARS 252.204-7012(b)(2)(ii)(D), comply with the reporting requirements of DFARS 252.204-7012(c-g), and meet CUI-related requirements per the DoD Instruction 5200.48, "Controlled Unclassified Information".

Note: External Cloud Service Providers who **only** store, process, and transmit *FCI* must implement the safeguarding requirements for CMMC Level 1. However, those with an external connection to the CUI/FCI environment under AC.L1-3.1.20 must also meet all the practices for CMMC Level 2.[2]

As a first principle, the C3PAO must obtain a basic understanding of the nature of the specifications, definitions, services, and information flow between the OSC and the External Cloud Service Provider with an external connection to the OSC under CMMC practice AC.L1-3.1.20, "External Connections: Verify and control/limit connections to and use of external information systems." The OSC's External Cloud Service Provider may or may not have an external connection to the OSC's environment under this practice. Moreover, if the OSC's External Cloud Service Provider does have an external connection, it may not necessarily store, process, or transmit CUI through their cloud services.

If an external connection exists between the OSC and their External Cloud Service Provider, the elements that determine the security requirements for the External Cloud Service Provider are based on:

- Whether or not the external connection is functioning for the delivery of products and services through cloud services;
- The flow of CUI (and FCI), or the restriction of the flow of CUI (and FCI), between the OSC and the External Cloud Service Provider; and
- Any Specified CUI requirements impacting either the OSC or their Eternal Cloud Service Provider.

The OSC is responsible for identifying the External Cloud Service Providers with external connections to the OSC that store, process, or transmit CUI. If the External Cloud Service Provider processes, transmits, or stores CUI, **then the External Cloud Service Provider is subject to the requirements of DFARS 252.204-7012(b)(2)(ii)(D) and applicable DoD policies related to the requirements:**

> *"If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the FedRAMP Moderate baseline and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this cause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment."*

[1] DFARS 252.204-7012(b)(1)(i), "For covered contractor information systems that are part of an **Information Technology (IT) service or system operated on behalf of the Government,** the following security requirements apply: (i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010 , Cloud Computing Services, of this contract."

[2] Safeguards for FCI are required under CMMC by FAR 52.204-21, but the definitions, restrictions, and requirements for CUI are distinct and most often do not directly correlate to FCI.

"FedRAMP" is the short title for the Federal Risk and Authorization Management Program, and the "Moderate baseline" is an official certification within the FedRAMP program. If the OSC's External Cloud Service Provider does not possess a valid FedRAMP Moderate certification, then the C3PAO Assessment Team will need to determine if the External Cloud Services Provider's security practices are equivalent to those of the FedRAMP Moderate baseline.

Procedures for determining if FedRAMP Moderate baseline equivalency has been established by the OSC's External Cloud Service Provider are addressed in Phase 2.

Some External Cloud Service Provides with external connections to the OSC **may not** store, process, or transmit CUI and FCI. If the External Cloud Service Provider does not store, process, or transmit CUI, but contributes to the OSC in meeting CMMC requirements (*i.e.*, providing protection) for the OSC's environment containing CUI and FCI, **then the External Cloud Service Provider must only meet NIST SP 800-171 requirements and attain CMMC certification for CUI/FCI** (or only meet CMMC Level 1 requirements when only FCI is present and the flow of CUI is restricted from the access through the external connection). The phrases "provides protection" or "provides security protection" mean the External Cloud Service Provider contributes to the OSC meeting at least one or more of CMMC practice requirements or other specified CUI security requirements.[3]

1.5.5 Evaluate Model Non-Duplication

Some OSCs may possess alternative cybersecurity certifications or findings, such as those of ISO 27001, FedRAMP, or other conformance regimes. Conformance to these standards is determined by external assessors not affiliated with CMMC in this capacity. Accordingly, absent subsequent official non-duplication policies published by the Department of Defense, other cybersecurity conformance regimes that may have been implemented by an OSC do not bestow any status or credit toward an OSC's CMMC Assessment or Certification.

1.5.6 Inventory OSC Cybersecurity Practices Against CMMC Model

Working under the guidance of, and in coordination with, their assigned Lead Assessor, the OSC shall provide to the C3PAO Assessment Team the following information:

- Results of most recent OSC self-Assessment or any pre-Assessment conducted by an RP or Registered Practitioner Organization (RPO);
- A preliminary list of anticipated Evidence;
- The System Security Plan and other relevant documentation; and
- A list of all OSC personnel who play a role in the procedures that are in scope.

The Assessment Team then collaborates and coordinates with the OSC to correlate all of the above information to each of the CMMC practices. The purpose of this procedure is to do a preliminary "triage" of all of the available evidentiary materials and "map" or "cross-walk" each item to their respective CMMC practices in order to establish the mutual understanding that the OSC has, at a minimum, addressed each of the CMMC practices with some evidentiary basis. This inventory does not establish that any or all CMMC practices have been implemented adequately sufficiently in accordance with the CMMC standard, but rather that no "gaps" exist with regard to a particular CMMC practice to ensure that the practice was neither neglected, ignored, or dismissed.

1.5.7 Verify and Record Evidence Against Adequacy and Sufficiency Criteria

The Lead Assessor determines and confirms the estimate of needed interviews, observations, reviews, and related Evidence that is needed for each practice or process that corresponds to the organizational functional areas and process roles. This is based on the requirements for Evidence:

[3] Under Scope and Applicability, "The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components." NIST SP 800-171 (pg. 3) "Protection" is defined under 32 CFR 2002.4(kk), "Protection includes all controls an agency applies or must apply when handling information that qualifies as CUI."

- **Adequacy**: criteria needed to determine if a given artifact, interview response (affirmation), demo, or test demonstrates performance of a CMMC practice. Adequacy answers the question, "Does the Assessment Team have the right Evidence?"
- **Sufficiency**: criteria needed to verify, based on CMMC Assessment Scope, that CMMC domain and practice coverage by the OSC is enough (sufficient) to rate against each practice. Sufficiency answers the question: "Does the Assessment Team have enough of the right Evidence?" All Evidence must:
  - Cover the sampled Host Units and/or Supporting Organizations;
  - Cover the model scope of the Assessment (CMMC L2 Scoping Guide); and
  - Correspond to the Host Unit and/or Supporting Organizations in the Evidence collection approach.

Adequate and sufficient Evidence will be required to determine if the OSC is ready for the Assessment, which is outlined in Section 1.6.3.

1.5.8 Review OSC Self-Assessment and DoD Assessment Findings Criteria

The Lead Assessor and the OSC POC shall jointly review the OSC's most recent CMMC self-assessment (either conducted by themselves or by a trusted third party, such as their RP or RPO) against the context of the DoD's criteria for the assessment of CMMC practices. This joint review is conducted to ensure that the C3PAO Assessment Team and the OSC are aligned in terms of expectations and requirements as they relate to the OSC's CMMC Assessment Scope and the framing of the Assessment engagement contract. The DoD Assessment findings criteria can be found in the *CMMC Assessment Guide* – Level 2, Version 2.0, pages 9-10:

> *The assessment of a CMMC practice results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE. To achieve a specific CMMC level, the contractor will need a finding of MET or NOT APPLICABLE finding on all CMMC practices required for the desired level as well as for all lower levels. For example, a contractor will need a MET or NOT APPLICABLE finding on all CMMC practices at Levels 2 and to achieve a CMMC Level 2 certification.*
>
> *• **MET:** The contractor successfully meets the practice. For each practice marked MET, the Certified Assessor includes statements that indicate the response conforms to all objectives and documents the appropriate evidence to support the response. Assessment Criteria and Methodology CMMC Assessment Guide – Level 2 | Version 2.0 10*
>
> *• **NOT MET:** The contractor has not met the practice. For each practice marked NOT MET, the Certified Assessor includes statements that explain why and documents the appropriate evidence that the contractor does not conform fully to all of the objectives.*
>
> *• **NOT APPLICABLE (N/A):** The practice does not apply for the assessment. For each practice marked N/A, the Certified Assessor includes a statement that explains why the practice does not apply to the contractor. For example, SC.L1-3.13.5 might be N/A if there are no publicly accessible systems.*
>
> *A contractor can inherit practice objectives. A practice objective that is inherited is MET if adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice objective. An ESP may be external people, technology, or facilities that the contractor uses, including cloud service providers, managed service providers, managed security service providers, cybersecurity-as-a-service providers.*
>
> *Evidence from the enterprise or the entity from which the objectives are inherited should show they are applicable to in-scope assets and that the assessment objectives are met. For each practice objective that is inherited, the Certified Assessor includes statements that indicate how they were evaluated and from whom they are inherited. If the contractor*

cannot demonstrate adequate evidence for all assessment objectives, through either contractor evidence or evidence of inheritance, the OSC will receive a NOT MET for the practice.

1.6 Complete Pre-Assessment Planning

The Pre-Assessment Data Form is essentially the holistic planning document for the Assessment itself. The template's purpose is to record the requirements, agreements, risks, conflicts-of-interest mitigation, and logistics for the CMMC Assessment. The Pre-Assessment Data Form must be maintained up-to-date throughout Phase 1 as the CMMC Assessment Scope and other conditions may evolve. The Pre-Assessment Data Form must be updated whenever any significant change occurs, including, but not limited to:

- If/when any significant changes to the framing of the Assessment and the OSC-C3PAO contract occur;
- Any change to the OSC's CMMC Assessment Scope (*e.g.,* added or removed assets or removed process roles) is declared;
- Changes to dates/times or scheduled Assessment events, including the scheduled dates for the Assessment itself are agreed upon;
- C3PAO effects changes to the makeup of its Assessment Team; and
- Any unplanned disruptions (*e.g.,* COVID-19 travel restrictions or protocols, natural disasters, etc.) emerge.

The Lead Assessor and the OSC Assessment Official must ultimately reach agreement on the content and submission of the final Pre-Assessment Plan for the Assessment to commence. The final version of the Pre-Assessment Data Form is submitted via upload into CMMC eMASS at the completion of Phase 1. It must be uploaded by a CMMC eMASS-authorized C3PAO representative. If changes occur after the Pre-Assessment Plan, a new data upload is required. Previous data uploads are retained in CMMC eMASS to allow for audit tracking.

Any official CMMC Certification Assessment must have a documented and current Assessment Plan, using the required CMMC Assessment plan template, or a C3PAO equivalent document with the same data.

1.6.1 Develop Evidence Collection Approach

The Lead Assessor shall identify methods, techniques, and responsibilities for collecting, managing, and reviewing Evidence, including:

- Artifact gathering and availability;
- Interview approach;
- Test or demonstration observation approach; and
- Requests for information (email or surveys).

The Evidence collection approach has implications for the following aspects of the Assessment:

- The amount of time and effort expended by the OSC in preparing for the Assessment;
- Ability of the Assessment Team to make accurate judgments;
- Usefulness and accuracy of the Assessment results; and
- Overall cost of the Assessment.

During Phase 1, the Evidence collection approach must record the use of any virtual data collection techniques, including any risks and mitigations, and how any Controlled Unclassified Information (CUI), Federal Contract Information (FCI), and/or OSC proprietary information will be managed and protected.

During Phase 2, the C3PAO Assessment Team will conduct affirmation sessions (interviews or demonstrations) either in person (face-to-face) or virtually (using video teleconference technology) with participants (interviewees) from the OSC.

Upon mutual agreement, much of the Evidence collection process may be conducted virtually, utilizing a stable and commercially secure video conference system of a web-based collaboration platform. The ultimate decision as to whether or not some of the Evidence collection activities will be conducted virtually or "on premises, in-person" rests with the OSC.

That notwithstanding, **implementation validation of the following 15 CMMC practice objectives must be observed by the C3PAO Assessment Team in-person and on the premises of the OSC** and the Evidence collection thereof is precluded from being conducted virtually:

- 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.
- 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.L2-3.10.2[a]: 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: the above CMMC practices may be exempted from mandatory on-site assessment if the OSC employs a cloud services provider to manage them and the cloud services provider holds FedRAMP Moderate certification or a valid determination of its equivalency.

If the OSC has security barriers, *e.g.,* a firewall that prevents access to artifacts by the Assessment Team, ensure at least one (1) Assessment Team Member for each C3PAO team has access to the artifacts (*i.e.*, physically onsite, OSC-provided hard copy, or electronic files). Please see Appendix T – "CMMC Assessment Evidence Collection Approaches" on various techniques, methods, and responsibilities for Evidence collection.

1.6.2 Select Assessment Team Members

The identification and assignment of C3PAO Assessment Team Members should be conducted with deliberate consideration and thought. This important activity should be viewed as a shared responsibility of both the C3PAO and the Lead Assessor that the C3PAO has selected for a specific OSC's CMMC Assessment. These personnel decisions entail much more than just selecting names off a CCA or CCP roster. The composition of a C3PAO Assessment Team should incorporate several factors. First and foremost, the C3PAO is responsible for verifying that all CMMC Certified Assessors and CMMC Certified Professionals on the team possess an active status in good standing with the CMMC Accreditation Body, which can be confirmed on the CMMC Marketplace. Other considerations for assigning Assessment Team Members should include, but are not necessarily limited to, the following:

- Absence of any conflicts of interest with the OSC;

- Availability for the targeted date range of Assessment;
- Cost, especially the hourly rate of independent (*i.e.*, "1099") Assessors;
- Years of experience;
- Geographic location of the Assessor;
- Specialization with a particular DIB sub-sector that aligns with the OSC's lines of business; and
- Professional reputation within the CMMC Ecosystem.

C3PAOs and Lead Assessors may, at times, receive requests from OSCs for a specific Assessor. For example, an OSC might have received a referral or recommendation from another OSC that acknowledged a certain Assessor's professionalism and thoroughness during a prior Assessment. OSCs have no authority or standing to insist on any particular individual as an Assessment Team Member. C3PAOs should view any by-name requests critically but may take into account such requests in composing their team as long as no conflict of interest exists between the Assessor and the OSC.

1.6.3 Identify Resources and Schedule

Through iterative dialogue, the Lead Assessor and the OSC Assessment Official determine the resources and schedule within which the Assessment is to be conducted. The statutory requirements of a CMMC Assessment and the preferences of the OSC Assessment Official, along with the consequent costs, logistics, size of the C3PAO Assessment Team, and schedule factors are balanced to arrive at an efficient and effective resource plan for the Assessment. The C3PAO has the primary responsibility for verifying that all planning requirements have been met, including:

- Providing and recording detailed resource needs beyond general boilerplate estimates;
- Identifying and documenting all Assessment participants, including:
  - The names and titles of individuals who are candidates for affirmation, *i.e.*, interviewees;
  - The names and functions of Assessment support personnel within the OSC (if any);
  - The organizational or project affiliation of all participants; and
  - Assessment Team Members, roles, and verified qualifications.
- Identifying and records any facilities to be used, including the location, seating capacity, required support equipment, and room configuration;
- Determining and recording schedule aspirations and constraints, including the estimated duration of key activities;
- Identifying any travel requirements;
- Identifying and recording any potential triggers for when replanning and/or updating of the Assessment plan will be required (*e.g.*, schedule overruns, unavailability of resources, etc.)

The C3PAO should also develop a proposed schedule for each day of the Assessment and show how the team effort estimates are applied over the scheduled Assessment duration. The Lead Assessor and the OSC should also determine if there will be any anticipated constraints or limitations in accessing necessary data for the Assessment.

1.6.4 Identify and Manage Conflicts of Interest (COI)

A basic conflict of interest is a situation or set of circumstances in which an individual or an organization involved in multiple interests—financial, organizational, or otherwise—and acting in the best interest of one, could simultaneously serve as working against the best interests of another. Conflicts of interest—or the perception of them—can undermine objectivity, including that of the Assessment Team, and must be avoided or mitigated within the CMMC Ecosystem. The International Standards Organization (ISO) regime to which C3PAOs will ultimately be held accountable, ISO/IEC 17020, "Conformity Assessment—Requirements for the operation of various types of bodies performing inspection," includes specific

measures for ensuring impartiality of conformity Assessments. For CMMC Assessments, the C3PAO is responsible for identifying both organizational and individual conflicts of interests, to include ensuring that the Lead Assessor and all Assessment Team Members have disclosed any COIs with the specific OSC to be assessed. The Lead Assessor will document any COIs in the Pre-Assessment Plan and take decisive action to either avoid them or develop and implement verifiable measures to mitigate them.

All parties should be familiar with—and refer to regularly—the conflict-of-interest provisions and prohibitions within the CMMC Code of Professional Conduct.

If a conflict of interest is disclosed or identified, by either party, the Lead Assessor should work with the OSC Assessment Official to develop a mitigation plan for the identified conflict in question. Any mitigation measures to which the parties agree should be documented and signed accordingly. In the event the conflict cannot be sufficiently mitigated due to the circumstances, the C3PAO must not proceed with the Assessment.

In addition, prior to commencing the Assessment, the Lead Assessor and all Assessment Team Members must attest (by signature) and submit to the CMMC Accreditation Body the "Absence of Conflict-of-Interest Confirmation Statement," as outlined in Phase 2.

1.7 Verify Readiness to Conduct the Assessment

The final step of Phase 1–for which the Lead Assessor is responsible—is to confirm that all parties are ready and positioned to conduct the CMMC Assessment. This includes ensuring that the OSC is adequately prepared, the C3PAO Assessment Team is established and ready, that Evidence is available and accessible, and that risks have been identified—all of which contribute to the overall feasibility of conducting the Assessment as planned. The Lead Assessor must also verify that all necessary logistics have been planned and that the C3PAO and the OSC have agreed to contract terms.

The readiness review is not intended to be a comprehensive determination of whether an OSC will necessarily meet any targeted CMMC Level and be successful in attaining Certification. Rather, the readiness review is the process of confirming that both parties are sufficiently prepared to conduct the Assessment.

Upon analyzing all of the information collected and discussions conducted during Phase 1, the Lead Assessor shall arrive at one of the following four (4) possible determinations:

1) **Proceed with the Assessment as planned:** all preparedness requirements have been met and all planning conditions are satisfactory to conduct a CMMC Assessment;
2) **Replan the Assessment**: not all preparedness requirements have been met, compelling the OSC and/or C3PAO to resolve certain discrepancies before the Assessment may commence;
3) **Reschedule**: all preparedness requirements have been met but planning conditions have been compromised due to external factors such as personnel health issues, natural disasters, current events, etc., and the Assessment must be rescheduled for a different date range; or
4) **Cancel the Assessment**; the Assessment cannot proceed due to insurmountable factors such as a conflict of interest that cannot be mitigated, a failure to arrive contract terms between the C3PAO and OSC, etc.

In all four determinations, the Lead Assessor makes the recommendation, but the C3PAO retains ultimate decision and approval authority.

1.7.1 Access and Verify Evidence

With the list of Evidence that was inventoried and "mapped" against the CMMC practices in Phase 1.4.6, the Lead Assessor and/or Assessment Team Members shall now perform a cursory review of the actual Evidence to verify that it exists and is ready for the formal scrutiny that will be applied by the C3PAO Assessment Team during the conduct of the Assessment in Phase 2. While previously, in Phase 1.4.6, the Lead Assessor was only reviewing an unverified list of the Evidence the OSC *intended to present*, in this step the Lead Assessor and/or Assessment Team Members are obtaining said Evidence and confirming

that it is present, accessible, and available to satisfy the requirement to assess the Evidence for CMMC Certification purposes in Phase 2.

Note: To reiterate, Evidence is only being *verified* at this stage; it is *not* being examined by the C3PAO Assessment Team.

If aspects of the CMMC Assessment will be conducted virtually, the Lead Assessor should ensure that the Virtual Assessment Evidence Preparation Template (Appendix O) has been utilized, that all practices have been annotated, and that the necessary Evidence and the manner in which it will be presented is accounted for on the form.

Note: The CMMC Accreditation Body **does not permit** a C3PAO to perform a readiness review with the intent of identifying weakness in the Evidence so the OSC can take corrective action prior to the conduct of the actual Assessment in Phase 2. At no time during this preliminary review of the Evidence shall the Assessment Team provide any advice or recommendation on how the OSC could improve or enhance the sufficiency or adequacy of their presented Evidence.

Additionally, the Lead Assessor is responsible for verifying any in-scope CMMC practices that the OSC proposes to claim as "Not Applicable" or "N/A" for that Host Unit or Supporting Organization. The Lead Assessor must also ensure that no proprietary data is to leave the OSC's environment without the express written consent of the OSC Assessment Official.

1.7.2 Make Assessment Feasibility Determination

Based on the verified existence of Evidence, along with the aforementioned resource estimates, Assessment objectives, plans, and schedule, the Lead Assessor shall determine if conducting the Assessment, as framed, is feasible.

The Lead Assessor makes his or her Assessment feasibility determination known to the OSC and the C3PAO and documents the recommendation in writing.

The C3PAO retains the ultimate decision authority on whether or not to proceed with the conduct of the Assessment, obviously dependent upon the willingness of the OSC to proceed as well.

If the C3PAO makes the decision to proceed with the Assessment as planned, the Lead Assessor and Assessment Team Members shall prepare the Pre-Assessment Form to be uploaded into CMMC eMASS.

In the event that the C3PAO elects to either **replan** or **reschedule** the Assessment, the C3PAO and the OSC should agree upon the specific way forward and make arrangements accordingly to resume the engagement at a future date. **Under no circumstances shall the C3PAO offer any advice, implementation assistance, or recommendations as to how the OSC can improve or enhance their preparedness for a replanned or rescheduled CMMC Assessment and doing so is an explicit violation of the CMMC Code of Professional Conduct.**

If the C3PAO or the OSC decides to cancel the Assessment, both parties should settle all affairs—including the return of any OSC proprietary information—and formally close out the engagement.

1.7.3 Conduct Quality Review on Pre-Assessment Form Data

C3PAOs shall have at least one CMMC Quality Assurance Professional (CQAP) supporting its CMMC Assessment Teams. One of the primary roles of the CQAP is to verify, prior to uploading into CMMC eMASS, the Pre-Assessment Form data as captured throughout Phase I to ensure the accuracy and completeness of the information. In addition to the quality of the data, the CQAP also ensures that the Pre-Assessment information is properly structured in the JavaScript Object Notation (JSON) format to facilitate successful exporting into CMMC eMASS. For guidance on the proscribed JSON schema, please refer to the "CMMC eMASS Concept of Operations (CONOPS) for C3POs." Formatting assistance is also available on the CMMC eMASS tool/website at https://cmmc.emass.apps.mil.

1.7.4 Upload Pre-Assessment Form into CMMC eMASS

Upon completion of the quality assurance review, the Lead Assessor shall direct one of the C3PAO's approved CMMC eMASS account holders to upload the Pre-Assessment Form into CMMC eMASS. The Pre-Assessment Form Template provided in Appendix A may be used for this purpose.

C3PAOs may elect to develop an in-house spreadsheet or purchase a third-party tool to facilitate the upload of the Pre-Assessment Form data into CMMC eMASS. Any such application must be incorporate all required Pre-Assessment Form data fields, meet DoD security requirements, and generate Pre-Assessment Form data in the required CMMC eMASS JSON file format.

Note: C3PAOd are required to send representatives to attend a free CMMC eMASS training session provided by the Department of Defense before they can be granted access to the system. Scheduling facilitation assistance for these training sessions is provided by the CMMC Accreditation Body. Prior to uploading the Pre-Assessment Form data to CMMC eMASS, the C3PAO CMMC eMASS account holder must contact the CMMC Program Management Office (PMO) administrator in order to have a record created for the OSC being assessed. This important step configures access controls to assure the data uploaded by the C3PAO is protected from access by other C3PAOs.

1.7.5 Prepare the Assessment Team

Prior to commencing Phase 2, the Lead Assessor shall verify that all Assessment Team Members are sufficiently prepared for performing the planned Assessment activities. This preparation includes ensuring Assessment Team Members are familiar with the CMMC Assessment Scope of the OSC and its System Security Plan. The Lead Assessor shall assign and communicate specific roles and responsibilities for each Assessment Team Member before conduct of the Assessment commences.

PHASE 2 – CONDUCT THE ASSESSMENT

The purpose of Phase 2 is to assess the implementation of CMMC practices by the OSC in conformance with the CMMC Model. The C3PAO Assessment Team will verify the adequacy and sufficiency of Evidence to determine whether the practices have met the required standard. The Assessment Team identifies, describes, and records any gaps in procedures related to model practices or procedures and presents the results of each day to the OSC during a daily checkpoint described in Phase 2.2.

Most of the activities throughout this entire Phase, from subphases 2.1.1 through 2.1.6 are iterative in nature during an Assessment.

2.1 Convene Assessment Kickoff Meeting

The Lead Assessor will convene an Assessment kickoff meeting prior to the commencement of Assessment conduct, using the CMMC Appendix D – CMMC Assessment In-Brief or equivalent presentation. This meeting may be conducted in-person, virtually, or in a hybrid manner.

Attendees for this meeting shall include, but are not limited to, the OSC Assessment Official, the OSC POC, the Assessment Team Members, and members of the OSC who will be participating in the Assessment. The OSC may elect to have their RP or RPO present as well. The Lead Assessor and/or Assessment Team Members shall brief the Assessment process, purpose, schedule, and objectives. The Lead Assessor also communicates specific information about scheduled events and the locations where they will occur.

The OSC should also deliver a briefing providing a high-level overview of their company/organization being and their cybersecurity program. During this meeting, the OSC Assessment Official or the OSC POC should inform all relevant OSC personnel of their role in supporting the Assessment, including those being interviewed and providing Evidence.

Any questions, issues, or concerns by either party should be identified, discussed, and resolved as part of this kickoff session. The Lead Assessor 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.

2.2 Collect and Examine Evidence

The CMMC Assessment Guide – Level 2 incorporates the Assessment procedures described in NIST SP 800-171A[1] Section 2.11:

> *An Assessment procedure consists of an Assessment objective and a set of potential Assessment methods and Assessment objects that can be used to conduct the Assessment. Each Assessment objective includes a determination statement related to the [CMMC practice] that is the subject of the Assessment. The determination statements are linked to the content of the [CMMC practice] to ensure traceability of the Assessment results to the requirements. The application of an Assessment procedures to a [CMMC practice] produces Assessment findings. These findings reflect, or are subsequently used, to help determine if the [CMMC practice] has been satisfied. Assessment objects identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals.*
>
> - *Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, architectural designs) associated with a system.*
> - *Mechanisms are the specific hardware, software, or firmware safeguards employed within a system.*

- *Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic).*
- *Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.*
- *For additional information on "Terms for Referring to Assessment Objects" see NISTIR 8011 Vol. 1, Paragraph 2.2.1.*

*The Assessment methods define the nature and the extent of the Assessor's actions. These methods include **examine**, **interview**, and **test**.*

- *The **examine method** is the process of reviewing, inspecting, observing, studying, or analyzing Assessment objects (i.e., specifications, mechanisms, activities). The purpose of the examine method is to facilitate understanding, achieve clarification, or obtain Evidence. The examination must link directly to the Assessment objectives of the relevant CMMC practice, and the results of the examination are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time. For an artifact to be accepted as Evidence in an Assessment, it must demonstrate the extent of implementing, performing, or supporting the organizational or project procedures that can be mapped to one or more CMMC practices and those artifacts must be produced by people who understand the practice and are in the chain of command that implements the practice.*
- The **interview method** is the process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain Evidence. The interview must link directly to the Assessment objectives of the relevant CMMC practice, and the interview results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time. For an interview statement to be accepted as Evidence in an Assessment, it must demonstrate the extent of implementing, performing, or supporting function, or enclave procedures that can be mapped to one or more CMMC model practices. Interview affirmations must be provided by people who implement, perform, or support the practices.
- Finally, the **test method** is the process of exercising Assessment objects (*i.e.*, activities, mechanisms) under specified conditions to compare actual with expected behavior[1]. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time and institutionalization. For a test/demonstration to be accepted as Evidence in an Assessment, it must pass its requirements and criteria while being observed by the Lead Assessor and Assessment Team. Any failed test results in a "NOT MET" CMMC practice.

In all three Assessment methods, the results are used to make specific determinations called for in the determination statements and thereby achieving the objectives for the Assessment procedures.

Assessors shall follow the guidance in NIST SP 800-171A when determining which Assessment methods to use:

> *Organizations [Certified Assessors] are not expected to employ all Assessment methods and objects contained within the Assessment procedures identified in this publication. Rather, organizations [Certified Assessors] have the flexibility to determine the level of effort needed and the assurance required for an Assessment (e.g., which Assessment methods and Assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the organization [contractor] can accomplish the Assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the CUI requirements have been satisfied.*

The primary deliverable of an Assessment is a report that contains the findings associated with each practice. For more detailed information on Assessment methods, see Appendix D of NIST SP 800-171A.

Any Evidence collection method that results in a CMMC practice being scored "NOT MET" must be evaluated using the current DoD Assessment methodology against the CMMC 2.0 Plan of Action and Milestones (POA&M) scoring criteria. The failed practice must also be recorded on the OSC's Level 2 CA.3.12.1 "Security Control Assessment" practice documentation, under the corresponding practice as "NOT MET".

During a CMMC Assessment, the Lead Assessor makes the final decision on preliminary recommended determination on all practices. For any practices where there is still a dispute between the Assessment Team and the OSC, the C3PAO holds the final interpretation authority for practice scorings and their related findings.

2.2.1 Examine and Analyze Evidence

Examining Evidence is an effective means to gain detailed insight about the practices implemented by the OSC and how those practices are performed. The OSC should provide a current and organized list of their Evidence and process mappings from any internal or third-party gap analysis as well as from the readiness review results. For each relevant practice in the CMMC Model, the C3PAO Assessment Team will review and collect the Evidence to demonstrate that the practice that is being performed is effectively implemented and conforms to the CMMC standard. The C3PAO Assessment Team shall be mindful of the following principles:

- The list of Evidence to be examined was provided to the Lead Assessor during Phase I, and that same list should be used to coordinate the collection of the Evidence for examination.
- Evidence artifacts might not necessarily have a one-to-one relationship with CMMC practices, resulting in a possible requirement for multiple artifacts.
- The OSC's Evidence should be evaluated based on the Assessment objectives defined in the *CMMC Level 2 Assessment Guide*.
- For recently implemented practices, the implementation should demonstrate that the practices and/or procedures will show sufficient confidence to support the determination that the CUI protection requirements have been MET.
- It is incumbent upon the Assessment Team to ensure that the artifact being examined is current and that it was produced by the same individuals who are performing, implementing, or supporting the work.
- Assessment artifacts that represent policies and procedures must also demonstrate deployment and adoption by the affected OSC personnel.

2.2.2 Conduct Interviews and Assess Responses

Interviews are another effective means by which to glean insight into the CMMC conformance of an OSC, including an understanding of how those practices or procedures are performed employees, contract staff, and Supporting Organizations. The Lead Assessor works with the OSC POC to identify staff within the OSC or third parties who perform procedures or have a role in supporting relevant cybersecurity activities. The Lead Assessor schedules affirmation or interview sessions with identified staff as part of the Assessment planning activities. These may be single or group interviews, as determined by the Lead Assessor's understanding of the OSC's stated roles and responsibilities of its staff and any Customer Responsibility Matrix (CRM) that might be in place with any of its Supporting Organizations.

During the interview session, the Lead Assessor and, if applicable, the Assessment Team:

- Takes steps to ensure and verify that confidentiality and non-attribution is addressed for interviewees so that they can speak openly without fear or concern about retribution from any member of the OSC;

- Asks questions of OSC staff to get clarity and understanding of practice or process implementation, and then review or verify any corresponding artifacts to determine CMMC practice implementation and records their answers in the form of notes; and
- Maps responses from interviewees to CMMC model practices to aide in determining and supporting the rating of that practice.

Conducting interviews may be an iterative activity, requiring some follow-up interview sessions or requests for information. Interviews resulting from daily checkpoint sessions should also be recorded and verified by the Lead Assessor and Assessment Team.

2.2.3 Observe Tests and Analyze Results

Observing live tests or demonstrations provides the Lead Assessor and Assessment Team with detailed operational insight into the effectiveness of the CMMC practices implemented in the OSC, including an understanding of how those practices are executed or supported through the use of a given technology application, system, test, or other similar approach.

The Lead Assessor works with the OSC POC to identify staff in the OSC who perform procedures or have a role in supporting the practice under review. The Lead Assessor schedules test or demonstration observations with identified staff as part of the Assessment planning activities. These may be single or group tests or demonstrations, as determined by the OSC's stated roles and responsibilities of its staff and any Customer Responsibility Matrix (CRM) that might be in place with any of its Supporting Organizations.

During the test or demonstration observation session, the Lead Assessor and, if applicable, Assessment Team:

- Takes steps to ensure and verify that confidentiality and non-attribution is addressed for anyone conducting a test or demonstration so that they can speak openly without fear or concern about retribution from any member of the OSC.
- Asks questions of OSC staff to get clarity of the test approach and results, and to verify any corresponding artifacts or procedures to verify and determine CMMC practice implementation and records their answers in the form of notes; and
- Maps responses from tests and demonstrations to CMMC practices to aide in determining and supporting the rating of that practice.

Any test or demonstration that successfully demonstrates how the CMMC practice is implemented will be noted as "MET". Conversely, any test or demonstration that fails to demonstrate how a CMMC practice is implemented results in a "NOT MET" for that CMMC practice.

2.2.4 Determine FedRAMP Moderate Equivalency for Cloud Computing Providers

If the OSC is utilizing a Supporting Organization that is an External Cloud Service Provider, the C3PAO Assessment Team will be responsible for ascertaining and determining if the External Cloud Service Provider meets the security requirements "equivalent" to the FedRAMP Moderate baseline as per the DFARS 252-204-7012(b)(2)(ii)(D) requirement.

The OSC can ensure that the External Cloud Service Provider meets security requirements equivalent to FedRAMP Moderate in the same way the OSC would normally ensure any services or product being contracted for will meet its requirements. For example, an External Cloud Service Provider may choose to provide evidence that it meets the security requirements equivalent to FedRAMP Moderate by providing a body of evidence (BOE) that attests to and describes how the External Cloud Service Provider meets the FedRAMP Moderate baseline security requirements.

Examples of items that could be included in such a BOE are an SSP that describes the system environment, system responsibilities, and the current status of the FedRAMP Moderate baseline controls required for the system, as well as a Customer Implementation Summary/Customer Responsibility Matrix that summarizes how each control is met and which party is responsible for maintaining that control.

In determining whether the External Cloud Service Provider meets the FedRAMP moderate "equivalency" requirement, the C3PAO Assessment Team shall examine whether the OSC has met the following two criteria:

1) The OSC or the External Cloud Service Provider has provided a body of evidence documenting how the External Cloud Service Provider's security controls are equivalent to those provided by the FedRAMP Moderate baseline standard; and

2) Said body of evidence has been attested to by an independent, credible, professional source.

If the C3PAO Assessment Team's examination concludes that both criteria have been met, the OSC's External Cloud Service Provider can be considered to have met the FedRAMP Moderate equivalency requirement and the C3PAO should consider the DFARS 252-204-7012(b)(2)(ii)(D) requirement satisfied.

If the C3PAO Assessment Team's examination concludes that both criteria have not been met, then the Assessment findings shall reflect the in-scope CMMC practices for which the External Cloud Service Provider is responsible be scored as NOT MET.

To be clear, the C3PAO Assessment Team **is not** conducting a quasi-FedRAMP certification audit of the External Cloud Service Provider, for which it is neither authorized nor certified. Rather, the C3PAO is applying the two criteria established by DoD to determine if FedRAMP Moderate "equivalency" has been attained and can be recognized.

Note: With regard to criterion #2, a CMMC RP or RPO employed, contracted, or under a paid engagement with the OSC **may not** serve as the independent, credible, professional source for attesting to the FedRAMP Moderate body of evidence. A FedRAMP Third-Party Assessment Organization (3PAO), however, retained by the OSC, ***may* serve** in this role to attest to the credibility of the body of evidence.

2.2.5 Identify and Document Evidence Gaps

The primary intent of this activity is to derive whether, from the Evidence gathered and reviewed, that an Evidence gap exists between that which the OSC's Evidence shows and what the C3PAO Assessment Team requires to support a claim that conformance to the CMMC practice has been attained. During this phase, the Lead Assessor and Assessment Team verify both Evidence adequacy and sufficiency. All Evidence examined by the C3PAO Assessment Team must address the full CMMC Assessment Scope of the OSC. As a reminder from Phase I:

- **Adequacy** criteria will determine if a given artifact, interview response (affirmation), demonstration, or test meets the CMMC practice. Adequacy answers the question: "Does the Assessment Team have the right Evidence?"
- **Sufficiency** criteria is needed to verify, based on Assessment and organizational scope, that coverage by domain, practice and Host Units, Supporting Units, and enclaves is enough (sufficient) to rate against each practice by the process role performing the work. Sufficiency answers the question: "Does the Assessment Team have enough of the right Evidence?"

If the examined artifact does sufficiently answer both the adequacy and sufficiency questions, an Evidence gap exists. Evidence gaps may point to a deficiency or weakness in the OSC's implementation of its cybersecurity measures, which exposes them to greater security risk. Examples of Evidence deficiencies could include:

- Documents that are incomplete (*e.g.*, authorized access control list missing new personnel)
- Affirmations that are illegitimate (*e.g.*, attestation from an employee who is not the proper owner/operator/supervisor of the system or information being examined)
- Policies that lack endorsement by senior management (*e.g.,* policies that are not signed, or signed by individuals not in a position of authority within the OSC)

The Assessment Team methodically works its way through the Evidence and records any gaps against CMMC model practices. For any in-scope practices that are determined to be "NOT MET," the Assessor making that determination should ensure that the Lead Assessor is informed and has visibility on the "NOT MET" practice.

(Similarly, the Assessment Team also records all practices determined to be MET during the Evidence examination).

2.2.6 Update Evidence Review Approach and Status

The Evidence collection and review approach provides a means for the Assessment Team to continuously monitor progress toward sufficient and adequate coverage of the CMMC practices being assessed. The Assessment Team regularly reviews any additional time or duration impacts resulting from additional Evidence collection efforts and records the status on a minimum of a daily basis throughout the Assessment. The Evidence collection status summarizes the differences between the Evidence reviewed thus far, and the Evidence needed to support the completion of the Assessment results, including the recommended findings and findings. If significant changes are incurred to the manner or nature of how the OSC's Evidence is being collected and examined, those changes should be reflected in the Pre-Assessment Data Form and updated file should be exported to CMMC eMASS.

2.3 Score OSC Practices and Validate Preliminary Results

The Assessment Team shall score each in-scope CMMC practice based on the examination of the presented Evidence. The Assessment Team shall then review and validate these scores with representatives of the OSC during the daily review. The OSC, as appropriate, may then present additional Evidence, as agreed upon and accepted by the Lead Assessor, which the Assessment Team may then use to update or verify practice scores.

These activities in this Assessment phase will be iterative based on the daily review results.

2.3.1 Determine and Record Initial Scores

When the initial Evidence for each CMMC in-scope practice has been reviewed, verified, and scored, the Assessment Team records the initial MET/NOT MET/NA scores and prepares to review them with the Assessment participants during the daily checkpoint.

CMMC Assessments will be scored at the objective level using the "CMMC Scoring with DoD Assessment Scoring Methodology" as featured in Appendix K. Assessors will score the objectives as MET/NOT MET/NA for each practice. Each practice with an objective(s) that is scored as NOT MET will inherently be scored as "NOT MET" for the entire practice and, accordingly, the Assess will ascribe a deduction for the practice.

For example, if the Assessor for CMMC practice AC.L1-3.1.20 has found that the OSC has not effectively achieved objective [a], "connections to external systems are identified," because the Assessor discovered a multiple-level protection scheme (MLPS) connection that is not annotated in any OSC documentation, this makes the entire practice, "NOT MET" due to this external connection having not been identified.

Note: If a practice is assessed to have an implementation discrepancy or deficiency that is eligible for remediation in a Plan of Action and Milestones (POA&M), that practice will be individually tracked using the CMMC Assessment Results Template.

2.3.2 Correct Limited Practice Deficiencies

On occasion, certain OSC practices may have been effectively implemented, but not necessarily documented correctly. In consonance with the implicit nature of a maturity model program and associated standards conformance regime (as opposed to a regulatory inspection or compliance audit), a Limited Practice Deficiency Correction accommodation exists for OSCs, to be implemented and cleared within a restricted timeframe.

2.3.2.1 Ineligible Practices for Deficiency Corrections

It is important for the C3PAO Assessment Team to understand first what OSC practices are not eligible for consideration under the Limited Practice Deficiency Correction provision. The following criteria below render any applicable CMMC practices as ineligible for said treatment and Assessors shall not track them under the Limited Practice Deficiency Correction Program:

- Practices that could lead to significant exploitation of the network or exfiltration of CUI, as listed in Appendix K, paragraphs (e) and (f);
- Any practice(s) listed on the OSC's Self-Assessment Practice Deficiency Tracker (validated in paragraph 1.4.2);
- Practices that were not implemented by the OSC prior to the current CMMC Assessment; and
- Any practice that changes and/or limits the effectiveness of another practice that has been scored as "MET".

2.3.2.2 Eligible Practices for Limited Deficiency Correction Consideration

The following are the only practices authorized for Limited Practice Deficiency correction as they have a limited or indirect effect on the security of the network and its data:

AC.L1-3.1.20	AC.L2-3.1.14	CM.L2-3.4.3	IR.L2-3.6.3	PE.L2-3.10.6	SC.L2-3.13.14
AC.L1-3.1.22	AC.L2-3.1.15	CM.L2-3.4.4	MA.L2-3.7	RA.L2-3.11.3	SC.L2-3.13.16
AC.L2-3.1.3	AC.L2-3.1.21	CM.L2-3.4.9	MA.L2-3.7.6	CA.L2-3.12.4	
AC.L2-3.1.4	AT.L2-3.2.3	IA.L2-3.5.4	MP.L2-3.8.4	SC.L2-3.13.3	
AC.L2-3.1.6	AU.L2-3.3.3	IA.L2-3.5.5	MP.L2-3.8.5	SC.L2-3.13.4	
AC.L2-3.1.7	AU.L2-3.3.4	IA.L2-3.5.6	MP.L2-3.8.6	SC.L2-3.13.7	
AC.L2-3.1.8	AU.L2-3.3.6	IA.L2-3.5.7	MP.L2-3.8.9	SC.L2-3.13.9	
AC.L2-3.1.9	AU.L2-3.3.7	IA.L2-3.5.8	PE.L1-3.10.3	SC.L2-3.13.10	
AC.L2-3.1.10	AU.L2-3.3.8	IA.L2-3.5.9	PE.L1-3.10.4	SC.L2-3.13.12	
AC.L2-3.1.11	AU.L2-3.3.9	IA.L2-3.5.11	PE.L1-3.10.5	SC.L2-3.13.13	

For any of the practices listed above, if the OSC's implementation of the individual practice meets the criteria below, that practice may be placed on the Limited Practice Deficiency Correction program:

1) A practice that was implemented, but missing minor updates (*e.g*. updates to policy signatures, procedural documentation that exists but is outdated, etc.), **but where** the practice Evidence demonstrates the implementation has been in place for a period of time; *and*
2) Consensus among the C3PAO Assessment Team that the practice in question does not change and/or limit the effectiveness of another practice that has been scored as "MET."

Both criteria must be in play for a particular practice to be tracked under the Limited Practice Deficiency Correction program.

Any CMMC practice that meets the above criteria can be placed on the Limited Practice Deficiency Correction program by the Lead Assessor. All practices placed on the Limited Practice Deficiency Correction program will be scored as "NOT MET" and recorded on the CMMC L2 Limited Practice Deficiency Correction Program Worksheet.

2.4 Generate and Validate Preliminary Recommended Findings

Based on the examination of Evidence, the C3PAO Assessment Team shall begin generating and validating the preliminary recommended findings. To begin, the Lead Assessor generates preliminary recommended findings to summarize all practice MET/NOT MET scores and indicate the extent to which the in-scope practices conform to the CMMC standard. Preliminary recommended findings should start being entered by the Assessment Team Members into the draft CMMC Assessment Findings Brief Template found in Appendix I.

Preliminary Findings must be presented to the OSC prior to the Final Findings presentation. The Lead Assessor shall keep the OSC updated as the draft findings are being developed, which can be accomplished during the daily checkpoint meeting. During this session, Assessment participants should be instructed that all additional Evidence will be verified by the Assessment Team as adequate, sufficient, and then rated accordingly during the next day's activities.

The daily checkpoint meeting may provide the OSC an opportunity to locate and present additional Evidence and may result in modifications to the Assessment Team's recorded practice scores and findings (as well as the inventory of Evidence if additional artifacts are presented.)

2.4.1 Determine Final Practice MET/NOT MET/NA Results

After all Evidence for each CMMC in-scope practice has been reviewed, verified, and rated, and discussed with the OSC participant during the daily checkpoints, the Lead Assessor records the final recommended MET/NOT MET/NA score and prepares to present the results to the Assessment participants during the final review with the OSC and its Assessment Official.

The C3PAO holds the final interpretation authority for the recommended practice scores and their related findings.

2.3.1.1 Determine Final Practice Results (Considering Limited Practice Deficiency Correction)

If the overall scoring of the Assessment after placing eligible items on the Limited Practice Deficiency Correction program results in **less than 80%** (88/110 practices "MET"), the OSC will receive a final finding of **"Not Achieved"** for CMMC Level 2 Certification. The OSC will be required to correct deficiencies and reapply for CMMC L2 Certification.

If the overall scoring of the Assessment after placing items on the Limited Practice Deficiency Correction program results in **greater than or equal to 80%** (88/110 practices "MET"), the OSC will be required to correct deficiencies within five (5) business day from the Final Findings Briefing or by an alternative date determined by the Lead Assessor, but a date not to exceed five (5) calendar days prior to the submission of the Final Findings Report into CMMC eMASS.

2.4.1.1 Execute POA&M Review

CMMC will allow conditional use of Plans of Action and Milestones (POA&M) to remediate practices that are not fully or successfully implemented. The POA&Ms will be strictly time-bound with a validity period of no more than 180 days from the Assessment Final Recommended Findings Briefing (Phase 3). POA&Ms will not be allowed for the highest-weighted CMMC requirements. Rather, the Department of Defense has established a minimum-score requirement to support Certification.

The Certified CMMC Assessor evaluating CA.L2-3.12.2, will validate the following criteria for an OSC to satisfy the requirements for CA.L2-3.12.2 and receive a CMMC Level 2 Conditional Certification:

- 80% of all CMMC Level L2 practices scored "MET"
  - Current CMMC L2 scoring would result in 88/110 Practices must be found as "MET"
- All POA&M items must meet the criteria in Appendix K, "CMMC Scoring with DoD Assessment Scoring Methodology"

The POA&M's purpose is to identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in an organization's programs and system.

A POA&M must document all proposed actions to remediate deficiencies and the respective timeframe for doing so. The POA&M should detail the progress of corrective actions as they are carried out and thus be updated regularly.

2.4.1.2 *Validate OSC POA&M*

The Lead Assessor is solely responsible for reviewing and determining the legitimacy and validity of a POA&M at the time of the assessment closeout. A credible and effective POA&M should include, at a minimum, the following:

- The specific security weakness (see 2.1.5 Evidence Gaps) revealed in the Assessment and tied to specific practice;
- The severity of each weakness;
- The scope of each weakness with the assessed environment;
- The proposed mitigation approaches;
- The estimated costs for remediation;
- Documented records of mitigation status and delays; and
- A risk Assessment of the deficiency

The Lead Assessor will ensure all practices that are authorized by DoD to be on a POA&M for CMMC are documented correctly on the CMMC Assessment Results Form.

2.4.2 Create and Finalize and Record Recommended Final Findings

The CMMC Assessment Findings Brief must be updated to its final recommended state, based on all Evidence received and reviewed by the Assessment Team throughout the Assessment, including any results from the daily checkpoint reviews. It must include MET/NOT MET scores at the OSC aggregated level and describe any practice has not been implemented in enough detail as to show how the score was derived by the Assessment Team. This includes a summary chart of all CMMC practices their MET/NOT MET status for each practice.

2.4.3 Support Assessment Appeals Process

If the OSC feels that there is an issue with the scoring on a practice and there is substantial evidence showing ALL the objectives of the practice have been "**MET**", the OSC can submit a dispute using the Assessment Appeals Process outlined in Appendix N.

PHASE 3 – REPORT RECOMMENDED ASSESSMENT RESULTS

The formal submission of the final Assessment results codifies the adjudication of the CMMC Assessment. In this phase, the Lead Assessor (with or without the Assessment Team Members) shall deliver the recommended Assessment results to the OSC during the Final Findings Briefing. Following that, the CMMC Quality Assurance Professional (CQAP), Lead Assessor, and C3PAO will verify completeness and accuracy of the Assessment packet prior to its upload into CMMC eMASS.

3.1 Deliver Recommended Assessment Results

The Lead Assessor shall provide the OSC Assessment Official and OSC participants with the Assessment results.

Using the CMMC Final Findings Briefing, along with the Pre-Assessment Form data, the Assessment results are delivered to the OSC Assessment Official either during the final daily checkpoint, or in a separately scheduled findings and recommendations review.

3.1.1 Deliver Final Findings

The Lead Assessor presents the final recommended findings, using the required Assessment Findings Brief Template, a summary of the recorded MET/NOT MET status of each practice within the CMMC Assessment Scope, as well as any additional information that provides more context for the findings. This activity communicates the final and complete recommended Assessment results to the OSC Assessment Official and OSC participants. These findings may be in a summarized form, but the detailed findings must also be provided as backup information. In addition to the recorded final recommended findings, the details of the CMMC practice scores are also presented and must include clear traceability from each finding, score, and practice status (*i.e.*, MET/NOT MET).

As per CMMC Assessment reporting requirements, the same results of the findings summary, practice, and respective scores are submitted to the C3PAO for review. Once the C3PAO CQAP completes the internal quality review (paragraph 3.2.2), the results are then submitted by the designated C3PAO CMMC eMASS account holder into CMMC eMASS (section 3.2.3).

3.2 Submit, Package, and Archive Assessment Documentation

The purpose of this phase is to package, baseline, and retain all Assessment documentation and artifacts.

Phase 3.2 Required Outputs:	
Recorded and Presented Final Recommended Findings	To be completed and presented by the Lead Assessor, using the required CMMC Findings Briefing template or equivalent.
Submitted and archived Assessment Results Package into CMMC eMASS	Final Report, CMMC Assessment Results
OSC Artifacts Hash	Using the *CMMC Artifact Hashing Tool User Guide*
Recorded and final updated Daily Checkpoint	Must include results from all discussed practices (artifact reviews, interviews, and examinations/tests) including any resulting actions and due dates

3.2.1 Limited Practice Deficiency Correction Evaluation

The C3PAO Assessment Team will review Evidence provided by the OSC to close out items on the Limited Practice Deficiency Correction Program. If all items are found to be corrected and “fully implemented”, the

OSC's score for that practice will be changed to "MET". For any practices in which the evidence still shows deficiencies, the score will remain, "NOT MET."

If all practices on the Limited Practice Deficiency Correction Program result in a score of "MET," the Lead Assessor will close out the Assessment using the steps in Phase 3, paragraph 3.1-3.2. The Lead Assessor shall then recommend the OSC be granted a Final CMMC Level 2 Certification.

If any practices on the Limited Practice Deficiency Correction Program FAIL to result in a score of "MET," the Lead Assessor will recommend moving the OSC's practice deficiencies to a POA&M using the steps in paragraph 2.3.1.2 of Phase 2.

The current score of the Assessment, after executing a POA&M review, must be greater than or equal to 80% (88/110 practices "MET"), to move the OSC to the POA&M Close-Out Assessment option. In this course of action, the OSC will remain on their Conditional CMMC Level 2 Certification, with their original start date.

If it is found that the POA&M Close-Out Assessment option cannot be utilized, the Lead Assessor will recommend the OSC NOT be recommend for CMMC Certification. As a result, the OSC will be required to correct deficiencies and reapply for another Assessment.

3.2.2 Verify Assessment Results Package

The CMMC Quality Assurance Professional (CQAP) shall verify Assessment documentation, prior to eMASS upload, to ensure the accuracy and completeness of the Assessment Results Package. (see CMMC Assessment Quality Review Checklist in Appendix L). The Final Report must be submitted to the CQAP for review no later than ten (10) business days from the Final Findings Briefing.

3.2.3 Upload Assessment Results Package into CMMC eMASS

All Assessment results, successful or not, are to be uploaded into CMMC eMASS for official recording and tracking.

The Assessment results package submitted to the C3PAO by the Lead Assessor must include the following Assessment artifacts:

- **Final Report:** The detailed practices and scores, clearly traceable to each finding and score, using the CMMC Assessment Results Template (*i.e.*, Excel workbook or spreadsheet with each practice scores, findings, comments, etc.).
- **Reports must be uploaded to eMASS no later than twenty (20) Business Days from the Final Findings Briefing.**

The C3PAO must use the proscribed CMMC eMASS JSON schema detailed in the eMASS CONOPS or an Assessment template the meets the format and field requirements for uploading into CMMC eMASS.

3.2.4 Archive or Dispose of any Assessment Artifacts

The Lead Assessor is responsible for maintaining and protecting any additional notes and information from the Assessment. These, along with the Assessment Results Package, must be retained and protected from a confidentiality, non-disclosure, and any other CUI perspective for three (3) years.

Because the artifacts of the Assessment are proprietary to the OSC and will remain with them, the Assessment Team Members will not take organizational artifacts offsite during or at the conclusion of the Assessment. Therefore, the Lead Assessor must ensure that the OSC has hashed all artifacts in accordance with the *CMMC Artifact Hashing Tool User Guide*. The OSC must hash and retain artifacts for three (3) years. The C3PAO will report the OSC's hash into CMMC eMASS.

THE PROTECTION AND DESTRUCTION OF CONTRACTOR ASSESSMENT MATERIALS TEMPLATE CAN BE USED TO VERIFY DISPOSAL OF ASSESSMENT ARTIFACTS FROM ALL ASSESSMENT TEAM MEMBERS. EACH ASSESSOR'S SIGNED DOCUMENT SHALL BE RETAINED BY THE C3PAO FOR THREE (3) YEARS.

3.2.5 Adjudicate Any Assessment Appeals

If the OSC believes their Assessment was compromised by either technical error or a breach of ethical conduct, the OSC can submit an official appeal of the Assessment and its findings using the Assessment Appeals Process outlined in Appendix N.

3.2.6 Schedule a CMMC POA&M Close-Out Assessment *(if necessary)*

The OSC is responsible for ensuring that all practice deficiencies listed on the validated POA&M are corrected within the 180-day timeframe from the CMMC Final Findings Briefing. This includes scheduling a CMMC POA&M Close-Out Assessment as described in Phase 4. While the same Lead assessor and/or C3PAO issuing the Conditional CMMC Certification **IS NOT** responsible for conducting the follow-up POA&M Close-Out Assessment, a Lead Assessor representing an Authorized C3PAO is still required to conduct the activities in Phase 4.

PHASE 4 – CLOSE-OUT POA&MS AND ASSESSMENT *(IF NECESSARY)*

The purpose of this phase is to allow OSCs that received a Conditional CMMC Level 2 Certification during Phase 3 to close out all practices validated on Plans of Action and Milestones (POA&M) during the C3PAO Assessment. With the introduction of CMMC v2.0, practice deficiencies that were documented prior to the CMMC Level 2 Assessment or created because of deficiencies found during the Assessment that meet the CMMC Scoring with DoD Assessment Scoring Methodology will be corrected post-Assessment. The final OSC POA&M must be validated in Phase 2 by the Lead Assessor and C3PAO prior to upload of the Assessment results into CMMC eMASS in Phase 3.

4.1 Perform POA&M Close-Out Assessment

Within 180 days from the Assessment Final Recommended Findings Briefing, the OSC will select a C3PAO to conduct a POA&M Close-Out Assessment. A Lead Assessor, and any additional Assessor, if necessary, will review the OSC's updated POA&M with any accompanied Evidence or scheduled collections (observations, interviews, or tests). Once all POA&M items have been validated by the below criteria, the Lead Assessor should proceed to paragraph 4.1.1.

- The specific security weakness revealed by POA&M during the Assessment has been "fully-implemented" and scored as "MET";
- All POA&M items "fully-implemented" do not change and/or limit the effectiveness of another practice that has been scored as "MET" during the Assessment for which the Conditional CMMC Level 2 Certification was issued;
- An updated risk assessment documents the removal of the previous CMMC practices listed on the POA&M; and
- An updated POA&M reflects no CMMC practice deficiencies.

In the event it was determined that one of the items above could not be satisfied, the Lead Assessor should proceed to paragraph 4.1.2.

4.1.1 Update POA&M Closeout

If all practices on the POA&M Review result in a score of "MET," the Lead Assessor will close out the Assessment using the steps in Phase 3, paragraph 3.2.2-3.2.4. Accordingly, the Lead Assessor will recommend the OSC be granted a CMMC Level 2 Final Certification.

4.1.2 Update POA&M – OSC Reapply

If any practices on the POA&M Review fail to result in a score of "MET," the Lead Assessor will recommend the OSC NOT be recommended for a CMMC Level 2 Final Certification. As a result, the OSC will be required to correct deficiencies and reapply for a CMMC Level 2 Certification. Upon this determination, the Conditional CMMC Level 2 Certification will be rendered null and void.

4.2 Support POA&M Close-Out Assessment Appeal Resolution

The C3PAO holds the final interpretation authority for validating the OSC's CMMC POA&M Close-Out findings. If the OSC feels that technical error or an ethical violation compromised the process, the OSC can submit an appeal using the Assessment Appeals Process outlined in Appendix N.

APPENDIX A – CHANGE LOG

Revision History

Revision #	Change(s)	Published Date
1.0	Initial Public DRAFT Release	July 26, 2022

Summary of Version Changes in Current Version

Change	Description of Change(s)
0	Initial DRAFT Release (no change)

APPENDIX B – GLOSSARY

Access
Ability to make use of any information system (IS) resource.

Access Authority
An entity responsible for monitoring and granting access privileges for other authorized entities.

Access Control
The process of granting or denying specific requests to:

- obtain and use information and related information-processing services; and
- enter specific physical facilities (e.g., federal buildings, company offices).

Agreements / Arrangements[4]
Agreements and arrangements are any vehicle that sets out specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements and arrangements include, but are not necessarily limited to, contracts, grants, licenses, certificates, and memoranda of understanding. When disseminating or sharing CUI with non-executive branch entities, agencies should enter into a written agreement/arrangement or understanding (see §2002.16(a)(5) and (6) for details). When sharing information with foreign entities, agencies should also enter agreements or arrangements, where feasible (see §2002.16(a)(5)(iii) and (a)(6) for details).

Artifacts
Tangible and reviewable records that are the direct outcome of a practice or process being performed by a system, person, or persons performing a role in that practice, control, or process. Artifacts may be a printed hard-copy or a soft- or electronic copy of a document or file embedded in a system or software but must be a result or an output from the performance of a process within the Organization Seeking Certification.

Assessment
The testing or evaluation (e.g., interviews, document reviews, observations) of security practices to determine the extent to which the practices are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. Source: NIST SP 800-37 Rev. 2 Also referred to as “CMMC Assessment”.

Assessment is the term used by CMMC for the activity performed by the C3PAO to evaluate the CMMC level of a DIB contractor. Source: CMMC

Assessment Appeals Process
A formal process managed by the Cyber AB to seek resolution of a disagreement of an assessment result.

Assessment Official
The most senior representative of an Organization Seeking Certification (OSC) who is directly and actively responsible for leading and managing the OSC’s engagement in the Assessment.

Assessor
An individual who is both certified and authorized to participate on a C3PAO Assessment Team and evaluate the conformity of an Organization Seeking Certification to meeting a particular CMMC level standard. *See also Provisional Assessor.*

[4] 32CFR §2002(c) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf

Certificate
A Record issued to an OSC upon successful completion of an Assessment which evidences the CMMC Level against which the OSC has been successfully assessed by an authorized C3PAO. See also Limited CMMC Certification.

Certification
The official CMMC credential that attests to: 1) an organization's conformance to a particular CMMC Level; or 2) an individual's achievement of meeting the requirements and standards of a specific CMMC profession (*e.g.*, Assessor, Instructor). See also Limited CMMC Certification.

Certified CMMC Assessor (CCA)
A person who has successfully completed all certification program requirements as outlined by the CAICO for becoming a Level 2 CMMC Assessor. A Provisional Assessor (PA) will become a CCP and then a CCP by passing the associated certification exam(s).

CMMC Certified Professional (CCP)
A person who has successfully completed all certification program requirements as outlined by the CAICO for becoming a Level 1 CMMC Assessor. A Provisional Assessor (PA) will become a CCP by passing the associated certification exam.

CMMC Certification Boundary
Defines the assets to which an Assessor will evaluate conformity with applicable CMMC practices. This is the boundary to which a CMMC Certification will be applied.

CMMC Certified Assessor
An individual who holds official CAICO Certification as a CMMC Certified Assessor. Lead Assessors can be certified at Level 2 or Level 3, which correspond to the CMMC Level against which they are authorized to conduct CMMC Assessments. Also referred to as "CMMC Assessor" or "Assessor".

CMMC Ecosystem
The interactive community of all CMMC professionals, including C3PAOs, Assessors, Instructors, Licensed Training Providers, Licensed Publishing Partners, Registered Practitioners, Registered Provider Organizations, as well as the Department of Defense and the CMMC Accreditation Body.

CMMC Level
A specific step or level within the CMMC Standard against which CMMC Assessments are conducted.

CMMC Standard
A framework that combines widely accepted NIST cybersecurity standards and maps those controls and requirements across several maturity levels that range from basic to expert cyber hygiene, and that, when implemented, will reduce risk against a specific set of cyber threats.

CMMC Third-Party Assessment Organization (C3PAO)
An Entity that is authorized to be contracted to conduct independent CMMC Assessments and issue CMMC Certifications for Organizations Seeking Certification (OSCs).

Conflict of Interest (COI)
A situation within the CMMC Ecosystem in which the concerns or objectives of two different parties are incompatible with one another. Conflicts of Interest must be disclosed where they exist and, if possible, mitigated. Conflicts of Interest left unattended by CMMC actors can threaten the impartiality of CMMC Assessments and the integrity of the CMMC Ecosystem overall.

Controlled Environment[5]

Any area or space an Authorized Holder deems to have adequate physical or procedural practices (*e.g.*, barriers or managed access practices) to protect FCI/CUI from unauthorized access or disclosure. Also called "FCI/CUI Environment".

Controlled Unclassified Information (CUI)[6]

Government-created or owned UNCLASSIFIED information that must be safeguarded from unauthorized disclosure. DoDCUI.Mil is the authoritative source for DoD CUI[7] as defined in DoDI 5200.48[8]

Daily Checkpoint

An immediate "after-action" discussion and evaluation of an OSC's current compliance status against CMMC practices conducted with the OSC Assessment participants, following the completion of that day's Assessment activities such as objective Evidence review, interviews, or observations/tests. Also known in industry as a "hot wash" or "hot wash review." Daily Checkpoint results/discussion must be recorded in a log by the Lead Assessor.

Disseminating[9]

The act of transmitting, transferring, of providing access to FCI or CUI to other authorized holders through any means, whether internal or external to an agency.

Document[10]

Any tangible thing which constitutes or contains information and means the original and any copies (whether different from the originals because of notes made on such copies or otherwise) of all writings of every kind and description over which an agency has authority. A document may be inscribed by hand or by mechanical, facsimile, electronic, magnetic, microfilm, photographic or other means, as well as phonic or visual reproductions or oral statements, conversations or events and including, but not limited to: correspondence, email, notes, reports, papers, files, manuals, books, pamphlets, periodicals, letters, memoranda, notations, messages, telegrams, cables, facsimiles, records, studies, working papers, accounting papers, contracts, licenses, certificates, grants, agreements, computer disks, computer tapes, telephone logs, computer mail, computer printouts, worksheets, sent or received communications of any kind, teletype messages, agreements, diary entries, calendars and journals, printouts, drafts, tables, compilations, tabulations, recommendations, accounts, work papers, summaries, address books, other records and recordings or transcriptions of conferences, meetings, visits, interviews, discussions or telephone conversations, charts, graphs, indexes, tapes, minutes, contracts, leases, invoices, records of purchase or sale correspondence, electronic or other transcription of taping of personal conversations or conferences and any written, printed, typed, punched, taped, filmed or graphic matter however produced or reproduced. Document also includes the file, folder, exhibits and containers, the labels on them and any metadata, associated with each original or copy. Document also includes voice records, film, tapes, video tapes, email, personal computer files, electronic matter and other data compilations from which information can be obtained, including materials used in data processing.

CMMC eMASS

The Enterprise Mission Assurance Support Service (CMMC eMASS) is a web-based, U.S. Department of Defense off-the-shelf solution that automates a broad range of services for cybersecurity management. CMMC eMASS serves as the system of record for CMMC Assessment data and reporting.

Enclave[11]

[5] 32CFR §2002(f) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[6] NARA CUI Registry - https://www.archives.gov/cui
[7] DoD CUI Registry: https://www.dodcui.mil/
[8] DoDI 5200.48 Controlled Unclassified Information - https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF
[9] 32CFR §2002(v) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[10] 32CFR §2002(w) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[11] https://csrc.nist.gov/glossary/term/enclave

A set of system resources that operate within the same security domain and that share the protection of a single, common, and continuous security perimeter. A segmentation of an organization's network or data that is intended to "wall off" that network or database from all other networks or systems. A CMMC Assessment scope can be within the Assessment scope of an enclave.

Enterprise

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.

Evidence

The observable proof that an organization has either met or not met the standard for a particular CMMC practice.

Examine

The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more Assessment objects or artifacts to facilitate understanding, achieve clarification, or obtain additional Evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time. For an artifact to be accepted as Evidence in an Assessment, it must demonstrate the extent of implementing, performing, or supporting the organizational or project procedures that can be mapped to one or more CMMC practices and those artifacts must be produced by people who implement or perform or support the procedures.

External Cloud Service Provider

A Supporting Organization that is providing cloud computing services to the OSC through an external connection.

Federal Contract Information (FCI)[12]

Information, not intended for public release, that is provided by or generated for the U.S. Government under a contract to develop or deliver a product or service to the U.S. Government, but not including information provided by the U.S. Government to the public (such as on public web sites) or simple transactional information, such as necessary to process payments).

Foreign Entity[13]

A foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body or an international or foreign private or non-governmental organization.

Handling[14]

Any use of CUI, including, but not necessarily limited to, marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

Host Unit

The part of a company being assessed and considered the OSC for purposes of the CMMC Assessment. A Host Unit could be a location, a division, a product line, or any other logical segmentation of an organization that can be independently assessed. Assessment results will be codified with the Host Unit name.

HQ Organization

[12] https://www.federalregister.gov/documents/2016/05/16/2016-11001/federal-acquisition-regulation-basic-safeguarding-of-contractor-information-systems
[13] 32CFR §2002(y) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[14] 32CFR §2002(aa) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf

The legal entity that will be delivering services or products under the terms of a DoD contract. The HQ Organization itself could be the OSC, or it could designate a Host Unit as the OSC.

Interviews

The process of conducting discussions with individuals or groups of individuals in an organization to facilitate understanding, achieve clarification, or lead to the location of Evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time. For an interview statement to be accepted as Evidence in an Assessment, it must demonstrate the extent of implementing, performing, or supporting the CMMC practice. Interview affirmations must be provided by people who implement, perform, or support procedures.

Lead Assessor

The Certified CMMC Assessor (Lead Assessor) who oversees and manages a discrete CMMC Assessment Team.

Limited Practice Deficiency Correction

With CMMC v2.0, the DoD has adopted a method to allow OSCs to ability to correct deficient CMMC practices that are found during the assessment, prior to assessment closeout (Phase 3). These practices cannot change and/or limit the effectiveness of other practices that have been scored "MET", nor can they be previously listed on the OSCs Self-Assessment Practice Deficiency Tracker prior to the assessment. Finally, the practice(s) cannot lead to a significant exploitation of the OSCs network or exfiltration of CUI, basic and derived security requirements/practices are listed in Appendix K, paragraph e & f.

Mechanism

An established process, which can involve people and/or technology, by which something takes place that brings about an intended and predictable outcome. For CMMC purposes, a mechanism might include:

- A technology-specific solution (*e.g.*, anti-malware, firewall, file-integrity monitoring, intrusion-prevention system, multi-factor authentication, etc.);
- A manual procedure that an individual performs; or
- An administrative solution (*e.g.*, acceptable use policy, human reviews, non-disclosure agreements, etc.).

In Assessment criteria for CMMC practices, the phrase "mechanisms exist to…" provides flexibility for the OSC to define what is most appropriate for its unique business practices. For example, more mature organizations might automate their security infrastructure and prefer technology-specific solutions, whereas less mature organizations might rely on manual procedures or administrative solutions.

Misuse of CUI[15]

Actions involving the utilization of CUI in a manner discordant with the policies and provisions contained in Executive Order 13556, the CUI Registry, Department of Defense CUI policy, or the applicable laws, regulations, and government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.

Observation

A real-time demonstration or review of a test, system, tool, software, hardware, practice, control, or process being performed and witnessed first-hand by the Lead Assessor and if applicable, Assessment Team.

Organization Seeking Certification (OSC)

[15] 32CFR §2002(e) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf

The Defense Industrial Base (DIB) company or legal entity that is going through the CMMC Assessment process—and contracting with a C3PAO in pursuit of CMMC Certification—for a given environment and a particular CMMC Level. Also referred to as "HQ Unit".

Provisional Assessor (PA)

An individual who has received authorization from the CMMC-AB/CAICO to serve as a Provisional Assessor (PA) during the provisional CMMC Interim Voluntary Period. PAs are authorized to conduct CMMC Assessments during the CMMC Interim Voluntary Period only and will eventually be required to pass CCP, CCA, and/or Lead Assessor exams in order to attain their formal Assessor Certifications.

Supporting Organization

A logical organizational boundary that is supporting the Host Unit of enclave being assessed. Though not part of the logical segmentation, systems or people within the Supporting Unit may still have access to CUI or FCI, so therefore must be included within the scope of the Assessment.

Test

The process of exercising one or more Assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time and institutionalization. For a test/demonstration to be accepted as Evidence in an Assessment, it must pass its requirements and criteria while being observed by the Assessment Team. Any failed test results in a failed CMMC practice.

Unauthorized Disclosure[16]

Unauthorized disclosure occurs when an Authorized Holder of CUI intentionally or unintentionally discloses CUI without a lawful government purpose, in violation of restrictions imposed by safeguarding or dissemination practices or contrary to limited dissemination practices.

Working Papers[17]

Documents or materials, regardless of form, that an organization or user expects to revise prior to creating a finished product. Also referred to as "drafts".

[16] 32CFR §2002(rr) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[17] 32CFR §2002(tt) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf

APPENDIX C – CONTRIBUTORS

The following individuals contributed to the development of the *CMMC Assessment Process*:

Peter Barletto, *Global Process Solutions LLC*
Michael Cernetich, *Coalfire Federal*
Jeff Dalton, *CMMC Accreditation Body, Inc.*
Regan Edens, *DTC Global*
Matt Gilbert, *Baker-Tilly*
Stacy High-Brinkley, *Cask Government Services*
Ron Lear, *ISACA*
Tara Lemieux, *Schellman & Co.*
Mike Pitcher, *AWS*
Kevin Schaaff, *ISACA*
Mary Segnit, *Leading Edge Process Consultants, LLC*
Michael Snyder, *CMMC Accreditation Body, Inc.*
Michael West, *Natural SPI, Inc.*