CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

CMMC Assessment Methodology Guide (CM2CAM)

Version 1.0_Baseline. Not for distribution.

FOREWORD

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. CMMC-AB 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.

INTRODUCTION TO THE CMMC ASSESSMENT METHODOLOGY

The CMMC ecosystem is explicitly designed to address cybersecurity requirements for the DoD's Defense Industrial Base (DIB) contracts, products, services, and supply chain. This CMMC Assessment Methodology provides the definitive set of processes, rules, and activities required for conducting official CMMC Accreditation Body (AB) approved certification assessments against the Department of Defense's CMMC model.

Consisting of 3 Primary Phases, the CMMC Assessment Methodology is the definitive source for CMMC Certification Assessments, and describes the critical activities taken to ensure that CMMC Certification Assessments meet the following objectives:

- Achieve the highest possible accuracy, fidelity, and quality for CMMC Certification Assessments conducted by Certified 3rd Party Assessing Organizations (C3PAOs) and their Certified Assessors
- Maximize consistency in results to ensure that different assessments conducted by different C3PAOs and Certified Assessors yield the same verifiable results and outcomes each time
- Continuously improve the Assessment Method by incorporating feedback and best practices from the DoD, DIB and all CMMC stakeholders and their related CMMC assessment activities
- Maximize the cybersecurity resilience of the DoD and DIB by providing effective and efficient assessments that are well-planned, executed and reported

TABLE OF CONTENTS

1.0 Phase I: Plan and Prepare Assessment

1.1 Analyze Requirements

All activities in Phase I are iterative and incremental, and certified assessors should not construe these actions to be single events. Assessors need to continuously review and update the requirements and plan for the assessment as more information is gathered. All the activities in this Phase that are executed in order to complete an initial plan will then be updated as final scoping is completed and the assessor can plan a successful assessment. Scoping may be initially difficult based on an Organization Seeking Certification's (OSC) understanding of CMMC and how it applies to their contract and organization, so the Certified Assessor must factor this into the length of time needed to complete all the Phase 1 requirements. Assessment planning could last from one to three days in duration depending on communications, context, and the ability of the OSC to provide required information.

The Certified Assessor (CA) works with the OSC Point of Contact (POC) to determine the assessment objectives based on business objectives, contractual requirements, and applicable CMMC model scope. In ongoing coordination with an Assessment Sponsor, the CA determines:

- The host unit's target CMMC scope and assessment boundaries, including target Maturity Level
- The organizational objectives, location(s), scope and boundaries, including the host unit, any supporting units, or associated enclaves, and identify staff that will provide objective evidence and context for the assessment
- OSC processes and process roles and corresponding Objective Evidence (OE)
- A Rough Order of Magnitude (ROM) estimate for the approximate duration and timing for the assessment
- The assessment outputs that will be provided to the OSC's Sponsor
- Reporting requirements to the C3PAO and CMMC AB, as applicable

The list of requirements, scoping, and analysis results are included in a draft assessment plan (template provide in the CA toolkit) or are referenced in the assessment plan as a separate document, as included as part of the assessment plan by reference.

	Phase 1.1 Required Outputs:
Completed CMMC Intake Form	To be completed by OSC with support from C3PAO or Certified Assessor
Recorded Draft Assessment Requirements	May be recorded in a combination of the CMMC Intake Form and draft assessment plan
Rough Order of Magnitude Estimate	Based agreed-upon requirements

1.1.1 Assessment Request Received by C3PAO from OSC

Unless otherwise notified by the CMMC AB, any OSC can select any CMMC C3PAO in good standing to submit a request to conduct an assessment with a C3PAO and the CMMC marketplace and website. Once the request has been received, the C3PAO has 5 business days to respond in writing, e.g., email, automated system response, to the request and assign a Certified Assessor, and team, if applicable. The request may include the identification or preference for a specific Certified Assessor, but the final decision for selecting and assigning the Certified Assessor and team lies with the C3PAO.

1.1.2 Identify Certified Assessor

The C3PAO reviews the OSC's RFA, considering their certification and quality status, certified level, i.e., ML1-5, skills and experience, geographical location, familiarity with the OSC's type of contract and work, and other factors to align and assign an available CA. Once the CA selection and assignment is completed, the C3PAO notifies the OSC in writing.

1.1.3 Identify OSC Sponsor and OSC POC

If not the initial POC, the Certified Assessor then works with the POC to identify an assessment Sponsor. The Sponsor is responsible for all OSC required actions for an assessment, including the funding and payment for the assessment. If needed, the Sponsor can then delegate a POC to act as assessment coordinator who will work

with the CA for planning, preparing and executing the assessment. Only the Sponsor can agree to and sign/approve the assessment scope, once determined through coordination with the CA and C3PAO.

1.1.4 High-Level Scoping Discussion

The CA works with the OSC Sponsor to determine the assessment scope, which consists of the CMMC model scope and the general scope of the OSC. The model scope includes the Maturity Level targeted to be appraised. These are defined by the CMMC model. This discussion also incudes identifying the initial location(s), timing, and dates for conducting the assessment. The CA also determines if an Assessment Team will be used for the assessment and identify the count of people needed as Assessment Team Members.

The CA works with the Sponsor and/or OSC POC to collect information to define the OU scope, which consists of the organization, host unit, supporting units and any enclaves in scope that will provide OE of their CMMC process implementation. This information is captured in the CMMC-AB Intake Form.

- Organization: The Legal Entity that will be delivering services or products under the terms of the contract (one or many). They could receive a CMMC Maturity Level, but also can designate a Host Unit.
- Host Unit: The people, processes, and technology that will be applied to the contract (one or many teams that are doing the work). This is the UNIT that is requesting a CMMC Maturity Level
- Supporting Units: The people, processes, and technology that support the Host unit. They will need to be part of the assessment, but will NOT receive a CMMC Maturity Level unless an enterprise assessment is conducted.

1.1.5 Determine, Record & Review Assessment Scope and Assessment Objectives

Based on the initial high-level scoping, the CA continues to work with the OSC Sponsor and/or POC, to determine the details on model, assessment, organizational, and contractual boundaries and scope. This may require several iterations with the OSC, but once the final detailed scope is determined by the CA and confirmed/agreed to by the Sponsor, the detailed scoping information is submitted to the C3PAO via the CA. The OSC must provide a set of initial OE, such as Systems Security Plans (SSPs), network diagrams, organizational charts to the CA to determine the scoping specifics. For any potential disagreements about scoping, the CA and the POC need to agree before the assessment can continue.

1.1.5.1. Evaluating Model Reciprocity

Reciprocity for alternative models is permitted within the CMMC Assessment Methodology (CAM). The Certified or Provisional Assessor has sole authority to accept results from the examination of controls or practices from an organization's prior assessments/audits/assessments ("examinations") based on alternative models such as Fedramp, NIST 800-181, CMMI V2.0, ISO 27001, or others.

The following assumptions must be validated by the Certified Assessor prior to acceptance of reciprocity:

1. The Examination being presented for reciprocity consideration was conducted by a credentialed assessor/auditor/appraiser ("examiner") on behalf of a certification or regulatory body authorized to award accreditations for that model, i.e., an ISO 17020:2012 certified organization.
2. Each control or practice to be considered for reciprocity must be functionally equivalent to the CMMC practice or control it is replacing, verified by objective evidence, such as documents, verbal or written affirmations, and demonstrations and tests. It is the responsibility of the OSC to present evidence of functional equivalency of that practice or control, and evidence of equivalency is examined, accepted at the sole discretion of the Certified Assessor.
3. The OE used for the requested reciprocity assessment results must be available for review by a C3PAO assigned Certified Assessor to verify.
4. All alternative controls/practices/requirements presented for reciprocity have received a passing score, characterization, or finding. For any given CMMC practice, control or process, there are no allowances for partial compliance or implementation, major nonconformances, weaknesses, or other noncompliances.
5. There is no Plan Of Action and Milestones (POAM), list of non-conformances, or rating deficiencies reported as a result of the examination. Objective evidence must be based on processes already executed or performed and show what has already been done, or put in place, and any real-time observation/test, and not what is going to be done.

6. No missing gaps of CMMC practices, controls or processes can be present
7. The reciprocity examination was conducted within 180 days prior to Phase II (onsite) of the CMMC Assessment.

The following rules of evidence apply to all CMMC practices/controls where reciprocity may apply:

1. CAM identifies three evidence types, with at least two being required for each control or practice to be rated as "pass." For controls or practices that are eligible for reciprocity, only one type of evidence will be required, eliminating as much as 70% of the time and effort required to examine the control or practice
2. Additional OE may be required and provided by the OSC when a thread of evidence indicates that there may be a potential issue with a given CMMC practice or set of practices. This will be determined solely by the Certified CMMC Assessor in conjunction with, if applicable, the Assessment Team. This may be done by looking at all related OE, or a suitable sample of OE, again, determined solely by the Certified Assessor
3. Controls or practices eligible for reciprocity must also be examined in the context of the CMMC ML2 "Institutionalization" processes, plans, and policies, and the Certified CMMC Assessor must account for this when interpreting the evidence for the eligible controls or practices.
4. Controls/Practices validated successfully using the reciprocity rules of evidence are to be considered implemented and will not be identified in the assessment report as having met a reduced standard of evidence.

1.1.6 Provide, Negotiate and Confirm Rough Order of Magnitude (ROM)

The C3PAO, through the CA, works with the Sponsor to determine a ROM estimate of what it will take to successfully execute a CMMC assessment. Once agreed upon by the CA and Sponsor, this ROM estimate becomes the basis for determining:

- Other needed information to complete the ROM as listed in the CMMC-AB Intake Form used as the basis for establishing an assessment contract between the OSC and C3PAO
- The assessment maturity level target, including the CA's verification of any potential Not Applicable practices as requested by the OSC
- The scope and boundaries of the OSC
- Approximate duration for planning and preparing (Phase 1) for the assessment, conducting the assessment (Phase 2) and reporting results (Phase 3)
- Nominal timing (month/quarter, etc.) for when the assessment will occur
- Number of assessment team members, including person-hours needed to conduct the assessment
- Nominal dates and duration for each phase
- Pricing for the assessment, including labor, travel and expenses and other direct costs
- The Certified Assessor verifies accuracy and completeness of the CMMC-AB Intake Form with the Sponsor and provides a final copy to the OSC and C3PAO. The completed and verified CMMC-AB Intake form provides the initial basis and scope for the assessment plan

1.1.7 Identify/map OSC Processes and Process Roles

Working under the guidance and in coordination with their assigned CA, the OSC provides the CA with:

- Results of most recent OSC pre-assessment or self-assessment
- A list of all Objective Evidence for the target CMMC Maturity Level
- A list of all the policies, processes and related plans in scope for the OSC
- A list of all personnel with any role in the processes in scope
- All of the above mapped to targeted in-scope CMMC practices and maturity level from the OSC's pre-assessment

1.1.8 Verify and Record Objective Evidence (OE) Against Adequacy and Sufficiency Criteria

The CA determines and confirms the number of needed interviews, observations, reviews and related OE that is needed for each practice, control or process that corresponds to the organizational functional areas and process roles. This is based on the requirements for OE:

- **Adequacy** – criteria needed to determine if a given artifact, interview response (affirmation), demo or test meets the CMMC practice. Answers the question: "Does the assessment team have the right evidence?"
    - Artifacts: 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 processes that

can be mapped to one or more CMMC practices and those artifacts must be produced by people who implement or perform the processes.
    - Affirmations: For an affirmation to be accepted as evidence in an assessment, it must demonstrate the extent of implementing, performing, or supporting the host, supporting function or enclave processes that can be mapped to one or more CMMC model practices; affirmations must be provided by people who implement, perform, or support processes.
    - Tests/Demonstrations: For a test/demonstration to be accepted as evidence in an assessment, it must pass it's requirements and criteria while being observed by the CA and assessment team. Any failed test results in a failed CMMC practice/control or process.
- **Sufficiency** – criteria needed to verify, based on assessment and organizational scope, that coverage by domain, practice and host unit, supporting units and enclaves is enough (sufficient) to rate against each practice by the process role performing the work. Answers the question: "Does the assessment team have enough of the right evidence?" All OE must:
    - Cover sampled host units, supporting units and enclaves
    - Cover the model scope of the assessment (target Maturity level)
    - Correspond to the OSC host unit, supporting unit or enclave in the OE collection approach

If the Certified Assessor determines the results of the pre-assessment do not meet adequacy and sufficiency, the CA is authorized to fail or stop the assessment.

1.1.9 Determine and Confirm Assessment Outputs

The CA works with the Sponsor to identify the outputs for the assessment, which include:

- Initial ROM estimate of assessment scope
- Assessment plan and schedule (demonstrating how the requirements in this method ha e been implemented)
- Certification Assessment Readiness Review (CA-RR) results
- Preliminary and Final Recommended Findings
- All recommended in-scope domains and practice pass/fail ratings
- Any potential remediation actions, if applicable

1.2 Develop Assessment Plan

Purpose: Record the assessment plan including requirements, agreements, risks, COI, tailoring, and logistics for all Phases. Obtain and record Assessment Sponsor approval of the assessment plan. Based on the scope, requirements and initial ROM estimate, the assessment plan must be kept up-to-date throughout Phases 1-2, and the final plan submitted during Phase 3 must be reflective of the actual results, timing, events and scope that the assessment covered. The plan must be updated whenever any significant change occurs, including, but not limited to:

- If/when the OSC in-scope government contract changes
- If/when any scope changes to the OSC-C3PAO contract occur
- If/when the maturity level targets changes
- Any change in the OSC organizational scope or functions (added or removed units, added or removed process roles)
- Changes to dates/times or scheduled assessment events, including the scheduled dates for the assessment itself
- Changes to the assessment team
- Any unplanned disruptions, e.g., COVID-19 travel restrictions or protocols, natural disasters, etc. before (Phase 1) or during the assessment (Phase 2)

Any official CMMC Certification Assessment must have a recorded and current assessment plan, using the standard CMMC Assessment Plan template.

Phase 1.2 Required Outputs:	
Recorded Final Assessment Requirements	May be recorded in a combination of the CMMC Intake Form and draft assessment plan
Recorded Final Assessment Plan and Schedule	To be completed by OSC with support from C3PAO or Certified Assessor using the required CMMC Assessment Plan template. Detailed schedule must include all Phase 2 activities.

1.2.2 Develop OE Collection Approach

The CA identifies methods, techniques, and responsibilities, etc. for collecting, managing and reviewing OE, including:

- Artifact gathering and availability
- Interviews approach
- Test or demonstration observation approach
- Requests for Information (email or surveys)
- Conduct for the preliminary findings briefing

The OE collection approach is part of the overall assessment plan, and has implications:

- Amount of time and effort expended by the organization in preparing for the assessment
- Ability of the assessment team to make accurate judgments
- Usefulness and accuracy of the assessment results
- Overall cost of the assessment

During the Planning Phase (Phase 1), the OE collection approach must record the use of any virtual data collection techniques, including any risks and mitigations, including how any CUI will be managed and protected. During the Conduct Assessment Phase (Phase 2), the 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. If the OSC has security, e.g., a firewall, that prevents access to artifacts by the assessment team, ensure at least one team member for each team has access to the artifacts, e.g., physically onsite, OSC provided hard copy, or electronic copies.

Table 1.2.2-A: OE Collection Approach Items

Item	Detail
Techniques for collecting artifacts	• Document reviews, demonstrations, access to tool repositories or environments, or presentations • Approach for using prior assessment events for OE collection or readiness review (if used for that purpose)
Techniques for collecting affirmations	Interviews, demonstrations, emails, messaging or presentations
Use of virtual methods for OE collection	Video conferences, teleconferences, and other similar technology
Responsibility for collection of OE	Typically, the OSC Sponsor or POC directs and facilitates this responsibility
Responsibility for verification of OE	Assignment of practices or model components to assessment team members
Summary of initial OE provided by the OSC	• Including any additional projects in the OSC for which OE was requested • Identification of artifacts still needed
A detailed schedule of affirmation-gathering activities	List of participants to be involved in affirmation and test/demonstration activities
The schedule for readiness reviews	• Explicit criteria for determining readiness • At least one readiness review shall be conducted

1.2.3 Select Assessment Team Members (ATMs), if applicable

This activity involves identifying available personnel, assessing their qualifications, and selecting them to become ATMs. It is the sole responsibility of the CA to identify and verify assessment team members and their qualifications.

- Must be CMMC-AB Registered Practitioners, Certified Professionals, or Certified Assessors
- Possess industry domain experience aligned with the OSC
- For CMMC ML3 and above, possess a total of 20 years of aggregate experience
- For CMMC ML1, the minimum team size is one (CA)
- For CMMC ML2, the minimum team size is two (CA + 1)

- For CMMC ML3 or above, the minimum team size is four (CA + 3)

1.2.4 Identify Resources and Schedule

Through iterative dialog, the Certified Assessor and the OSC Sponsor determine the resources, cost, and schedule within which the assessment is conducted. The preferences of the Assessment Sponsor, the limits of the method, and the consequent resource, cost, and schedule constraints are balanced to arrive at an optimal assessment plan, and the Certified Assessor has the primary responsibility for verifying that the CMMC Assessment method planning requirements are met, including:

- Recording detailed resource needs beyond those already identified in the ROM estimate
- Identifying assessment participants, recording:
    - The names of people who are candidates for affirmation, e.g., interviewees
    - The names and functions of assessment support personnel (if any)
    - The organizational or project affiliation of participants
    - Assessment team members and verified qualifications
- Identify any facilities including the location, seating capacity, and configuration of rooms to be used
    - Identify any specific equipment needed
    - Identify any other assessment resources
    - Identify any facilities needed, e.g., rooms, platforms, secured facility constraints
- Determine and record schedule constraints
- Determine and record cost and schedule
    - Estimate:
        - The duration of key activities
        - The effort required for the assessment team
        - Any cost associated with using facilities and equipment
        - Any cost associated with incidentals, e.g., travel, meals
- Record detailed schedule for each day of the assessment: show how the team effort estimates are applied over the scheduled assessment duration
- Record criteria and any triggers for when replanning and updating the assessment plan is required, e.g., schedule overruns, unavailability of resources
- Determine any OE or performance data access constraints, e.g., security clearance or classification requirements

1.2.5 Identify and Manage Conflicts of Interest (COI)

This activity involves identifying and handling COI that may impair an assess team's ability to function objectively. The Certified Assessor is responsible for handling potential COIs by avoiding or developing strategies to manage them

1.2.6 Identify and Manage Assessment Risks and Their Mitigation & Contingency Plans

The CA is responsible for recording and communicating risks and associated mitigation plans to the Assessment Sponsor and ATMs. Given the potential common Risk Sources in Table 1.2.6-A: Potential Common Risk Sources, it is required that the assessment plan includes comprehensive documentation of risks. Assessment Plans with minimal treatment of risks, e.g., no risks, or only one risk, will not be accepted by the C3PAO or AB.

Table 1.2.6-A: Potential Common Risk Sources

Potential Risk Sources	Examples
Personnel	Experience level, availability of ATMs, Assessment Sponsors, interviewees, and POC
Logistics	Team members working in remote facilities including the use of virtual technology during the Conduct Assessment Phase, coordination of reviews for classified artifacts
Facilities	Use of technology for remote affirmations, e.g., dropped lines, video bandwidth
Schedule	Sufficiency of OE as determined during readiness review
Cost	Funding constraints
Data	Protection of proprietary data such as performance data

1.2.7 Obtain and Record Commitment to the Assessment Plan

The CA records the results of assessment planning including the requirements, agreements, estimates, risks, method tailoring, and practical considerations; e.g., schedules, logistics, and contextual information about the organization; associated with the assessment. The assessment plan constitutes a contract between the Assessment Sponsor and the CA, so it is vital that this agreement be formally reviewed, approved and signed. The agreed-upon plan is then sent to the C3PAO to confirm adequate and appropriate scope.

1.3 Verify Readiness to Conduct Assessment

Ensure readiness to conduct the assessment in terms of team preparedness, availability of OE, risks, and logistics in determining the feasibility of the assessment as planned.

Phase 1.3 Required Outputs:	
Completed and Recorded CMMC Assessment Readiness Review Results	To be completed by CA, and assessment team, if applicable
Trained Assessment Team	Applicable if there is an assessment team
Updated Assessment Plan and Schedule	Based on any updates from Readiness Review results

1.3.1 Prepare and Train assessment team

The Certified Assessor verifies that ATMs are sufficiently prepared for performing the planned assessment activities. This preparation includes ensuring ATMs are familiar with the assessment scope, the assessment method, the assessment plan, and the tools and techniques to be used during the assessment. The CA assigns roles and responsibilities for assessment tasks. The assessment team participates in team building exercises to practice facilitation skills and reach consensus in understanding the team objectives and how they will be satisfied.

1.3.2 Identify, Obtain, Inventory, and Verify OE

Obtain information that facilitates preparation and an understanding of the implementation of CMMC practices, controls, and related processes, policies and plans across the OSC resulting from a pre-assessment. Identify potential issues, gaps, or risks to aid in refining the plan.

The CA is responsible for verifying any CMMC practices in-scope that the OSC proposes to be Not Applicable or N/A for that host unit, supporting unit or associated enclave.

1.3.3 Perform Certification Assessment Readiness Review

The purpose of the Certification Assessment Readiness Review is to determine whether the assessment team and OSC (host unit, supporting functional units and any enclaves) are ready to conduct the assessment as planned, and in the time allocated. The readiness review addresses several aspects of readiness to conduct the assessment, which include at a minimum: OE readiness, assessment team readiness, logistics readiness, assessment risk status, and overall assessment feasibility. The readiness review results in a decision to continue as planned, replan or reschedule, or cancel the assessment. The Certified Assessor and Assessment Sponsor are responsible for identifying and recording the criteria that will determine whether an assessment will proceed, but that criteria must be reviewed and approved by the C3PAO and AB.

The readiness review is not intended to be a comprehensive determination of whether an OU will meet any targeted maturity level rating. The CMMC AB does not permit performing a readiness review with the intent of identifying weakness in the OE so the OSC can fix them prior to the start of the Conduct Assessment Phase (Phase 1).

Verify at a minimum the following five readiness review criteria:

- OE readiness
- Assessment team readiness
- Logistics readiness
- Assessment risk status
- Overall assessment feasibility

Based on all of the above and the assessment objectives, plan and schedule, evaluate if the assessment is feasible without excessive stress, problems or impact on the team and organization. The Certified Assessor must identify and record feasibility criteria in the assessment plan, e.g., assessment team will work 9-hour days to shorten schedule. If determined there are feasibility concerns, the Certified Assessor must discuss with the Assessment Sponsor and keep the assessment plan and schedule updated.

1.3.4: Update the Assessment Plan and Schedule as Needed, Based on CA-RR

Once the results of the CA-RR is completed, the Certified Assessor updates the assessment plan and schedule and communicates the results and outcomes and their potential impact on the assessment.

Phase 2 – Conduct Assessment

2.1 Collect and Examine Objective Evidence

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

The purpose of this phase is to examine information about processes implemented in the OSC to meet CMMC practices, controls and processes. The assessment team will verify the sufficiency of OE to determine whether the practices and related components for each in-scope host unit, supporting unit or enclave has been met. The assessment team identifies, describes and records any gaps in processes related to model practices, controls or processes and presents the results of each day to the OSC during a daily checkpoint described in Phase 2.2.

Phase 2.1 Required Outputs:	
Recorded and Presented Opening Briefing	To be completed and presented by the CA, using the required CMMC Opening Brief template
Detailed Records of OE Reviewed and Examined	Using the CMMC Assessment Tracker Template/tool
Updated Assessment Plan and Schedule	Based on any updates from Readiness Review results

2.1.1 Assessment Kickoff – Opening Briefing

All members of the OSC who participate in the assessment are informed of their role during the assessment, including the OSC staff being interviewed/providing OE, the Sponsor, and the CA and Assessment team. The CA briefs assessment participants and other members of the OSC and provides an overview of the assessment process, purpose, and objectives. The CA also communicates specific information about scheduled events and the locations where they occur during this briefing. Any questions, issues or concerns are discussed and resolved with participants.

2.1.2 Collect and Analyze Artifacts

Assumption: Certified Assessor has verified that the organization is prepared for the assessment through a pre-assessment and/or readiness review.

Artifact review is an effective means to gain detailed insight about the processes implemented in the OSC, and how those processes are performed. The OSC must provide a current and organized list of their objective evidence and process mappings from any internal or 3rd party gap analysis as well as the CA-RR results from Phase 1.3.3. For each relevant Practice in the CMMC, the Assessment Team will review and collect Artifacts to demonstrate that the practice is being performed, or that the control, and any related policy, plan or process is effectively implemented.

- The list of OE to be examined is provided to the CA during Phase I, including verification that the organization is prepared for the assessment.
- Artifacts may not have a one-to-one relationship with CMMC Practices, resulting in a requirement for multiple artifacts
- As a Maturity Model, practices must be evaluated for organizational maturity, and their ability to demonstrate habitual and persistent behavior
- It is incumbent upon the Assessment Team to ensure that the artifact is current, and was produced by the individuals who are performing the work

- Artifacts that represent policies and procedures must also demonstrate deployment and adoption by the affected team members

THE CMMC Assessment Methodology recognizes three types of Objective Evidence:

- **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 can be a printed hard-copy, soft- or electronic copy of a document or file or embedded in a system or software, but must be a result or output from performing a process in the OSC..
- **Affirmations**: Spoken or written word from a person performing a role in an OSC practice, control or process that verifies the performance and resulting outcome of a practice or process. Affirmations can be written and submitted electronically, e.g., email, as long as the identify of the person providing the affirmation can be verified as having a process role in the OSC and is the one responsible for performing that work.s
- **Observation / Test**: A real-time demonstration or review of a system, tool, software, hardware, practice, control or process being performed and witnessed first-hand by the CA and if applicable, Assessment team.

2.1.3 Collect and Analyze Affirmations

Affirmations or interviews are an effective means to gain detailed operational insight into the effectiveness and outcomes of the practices, controls and related policies and plans implemented in the OSC, including understanding of how those practices or processes are performed. The CA works with the OSC POC to identify staff in the OSC who perform processes or have a role in supporting the processes. The CA 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 CA's understanding of the OSCs practices, controls, and related processes, policies and plans. During the interview session, the CA and, if applicable 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
- Maps responses from interviewees to CMMC model practices to aide in determine and support the rating of that practice

Conducting affirmations may be an iterative activity, requiring some follow-up interview sessions or requests for information. Affirmations resulting from daily checkpoint sessions should also be recorded and verified by the CA and assessment team.

2.1.4 Observe Tests or Demonstrations

Observing live tests or demonstrations provides the CA and assessment team with detailed operational insight into the effectiveness and outcomes of the practices, controls and related policies and plans implemented in the OSC, including understanding of how those practices or processes are performed using a given system, test, or other similar approach. The CA works with the OSC POC to identify staff in the OSC who perform processes or have a role in supporting the processes. The CA schedules test/demonstration observations with identified staff as part of the assessment planning activities. These may be single or group tests or demonstration, as determined by the CA's understanding of the OSCs practices, controls, and related processes, policies and plans. During the test or demonstration observation session, the CA and, if applicable, assessment team:

- Takes steps to ensure and verify that confidentiality and non-attribution is addressed for any 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 processes to verify and determine CMMC practice implementation and records their answers in the form of notes
- Maps responses from tests and demonstrations to CMMC model practices to aide in determine and support the rating of that practice

- For any test or demonstration that fails to demonstrate how a CMMC practice is implemented also then fails that CMMC practice

2.1.5 Verify OE and Record Gaps

The primary intent of this activity is to derive records, from the OE gathered and reviewed, that describe the gap between what the OE shows and what the assessment team requires to support a claim that the intent and value of model practices has been met.

It is during this phase when the CA and assessment team verify both OE adequacy and sufficiency.

- **Adequacy** criteria will determine if a given artifact, interview response (affirmation), demo or test meets the CMMC practice. Answers the question: "Does the assessment team have the right evidence?"
    - Artifacts (examine): For an artifact to be accepted as objective evidence, it must demonstrate the extent of implementing, performing, or supporting the organizational practice or control that can be mapped to one or more CMMC practices, and those artifacts must be produced by people who implement or perform the processes.
    - Affirmations: For an affirmation to be accepted as objective evidence, it must demonstrate the extent of implementing, performing, or supporting the host, supporting function or enclave processes or controls that can be mapped to one or more CMMC model practices; affirmations must be provided by people who implement, perform, or support processes.
    - Observation / Test: For an observation or test to be accepted as objective evidence, it must be observed by an assessment team member, and must be the actual system or control that is used in the production system environment (a screen shot is an artifact)

- **Sufficiency** criteria is needed to verify, based on assessment and organizational scope, that coverage by domain, practice and host unit, supporting units and enclaves is enough (sufficient) to rate against each practice by the process role performing the work. Answers the question: "Does the assessment team have enough of the right evidence?" All OE must:
    - Address the full scope of the assessment (sampled host units, supporting units and/or enclaves)
    - Cover the model scope of the assessment (target Maturity level)
    - Correspond to the OSC host unit, supporting unit or enclave in the OE collection approach

The assessment team methodically works its way through the OE and records any gaps against CMMC model practices, controls, processes, policies or plans. The gaps are recorded as weaknesses or nonconformances for each practice in scope where applicable. The assessment team also records any in-scope practices determined to be fully compliant.

2.1.6 Update OE Review Approach and Status

The OE collection 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 OE collection effort and records the status on a minimum of a daily basis throughout the assessment. The OE collection status summarizes the differences between the OE reviewed so far, and the evidence needed to support the completion of the assessment results, including the recommended ratings and findings.

2.2 Rate Practices and Validate Preliminary Results

These activities in this assessment phase will be iterative based on the daily review results. The assessment team rates each CMMC practice, based on and including any related controls, processes, policy or plan reviewed, affirmations obtained, and results of observations/tests. The assessment team then reviews and validate their ratings of the in-scope practices with assessment participants from the OSC host unit during the daily review. The OSC, as appropriate, may then present additional OE, as agreed upon/accepted by the CA, which the assessment team may then use to update or verify practice ratings.

- In order for a Practice / Control in the CMMC to be rated as Satisfied ("pass"):
    - The Assessment team must examine and accept two of the three objective evidence types:
        - Artifact (examine)
        - Affirmation
        - Test or Demonstration Observation

- The objective evidence examined must be applicable to the practice, control, and related policy, plan and process being evaluated, and must always include either an artifact or an observation / test
- The evidence accepted must be adequate, and fully reflect the performance of the control or practice
- Practices subject to Reciprocity Agreements (TBD), will be subject to a reduction in objective evidence review and will be described in the Tailoring section of the assessment plan, based on any CMMC differences or delta gaps between the in-scope CMMC practices and those of the reciprocity model.

Phase 2.2 Required Outputs:	
Recorded and Presented Preliminary Recommended Findings	To be completed and presented by the CA, using the required CMMC Findings Brief template
Detailed Records of OE Reviewed and Examined, Resulting Practice Ratings and Justification	Using the CMMC Assessment Tracker Template/tool
Recorded and updated Daily Checkpoint log	Which must include attendee list, time/date, location/meeting link, results from all discussed topics, including any resulting actions and due dates from the OSC or assessment team

2.2.1 Determine and Record Initial Model Practice Ratings

When the initial OE for each CMMC in-scope practice has been reviewed, verified, and rated, the assessment team records the initial pass/fail rating and prepares to review it with the assessment participants during the daily checkpoint. For any CMMC practices, controls and related processes, policies, plans that are controlled by staff across the host unit, supporting units and enclaves, the assessment team records the results for each and uses that to then aggregate to the resulting practice rating at the OSC host unit level.

The CA holds the final interpretation authority for the ratings and their related findings.

2.2.2 Generate Preliminary Recommended Findings

In preparation for validating OE collected (or missing), the assessment team generates preliminary recommended findings to summarize all practice pass/fail ratings and indicate the extent to which the in-scope practice, control, or related processes, and policies meet the intent of CMMC practices. This is done using the Recommended Findings template.

2.2.3 Validate Preliminary Recommended Findings and Ratings

Validation of preliminary findings and ratings is an OE collection activity, and the intent is to validate the assessment team's understanding of the practices, controls and related processes, policies and plans implemented within the host unit, supporting unit and applicable enclave. Feedback from participants may result in modifications to the assessment team's recorded practice ratings and findings, and OE inventory. This activity is done during each day's daily checkpoint with the assessment participants. Assessment participants should be told that all additional OE will be verified by the assessment team as adequate, sufficient, and then rated accordingly during the next day's activities.

2.3 Generate Final Recommended Assessment Results

Throughout the course of the assessment, the Assessment team captures and records the status and recommended ratings of each in-scope CMMC practice, control and any related process, policy or plan for each host unit, supporting function or enclave and then aggregates that to the final recommended assessment ratings and findings, including the recommended CMMC maturity level. This is reviewed with the OSC during the final daily review.

Phase 2.3 Required Outputs:	
Recorded and Presented Final Recommended Findings	To be completed and presented by the CA, using the required CMMC Findings Brief template

Final Records of OE Reviewed and Examined, Resulting Practice Ratings and Pass/Fail Justification	Final and complete, using the CMMC Assessment Tracker Template/tool
Recorded and final updated Daily Checkpoint log	Which must include attendee list, time/date, location/meeting link, results from all discussed topics, including any resulting actions and due dates from the OSC or assessment team
Final Assessment Plan and Schedule	Based on any real-time changes to plan/schedule during the assessment.

2.3.1 Determine Final Practice Pass/Fail Results

After all OE for each CMMC in-scope practices has been reviewed, verified, and rated, and discussed with the OSC participant during the daily reviews, the assessment team records the final recommended pass/fail rating and prepares to present the results to the assessment participants during the final review with the OSC and Sponsor.

The CA holds the final interpretation authority for the recommended practice ratings and their related findings.

2.3.2 Determine Maturity Level Recommendation

Prior to the final daily checkpoint, the assessment team records the final recommended pass/fail OSC maturity level rating and prepares to present it and the related assessment results to the assessment participants and Sponsor.

The CA holds the final interpretation authority for the recommended maturity level rating. All CMMC practices within the target maturity level must be rated as a "pass" rating with no major noncompliances or findings. Any deltas between the CMMC and any reciprocity model must also be addressed as pass from a CMMC practice perspective.

2.3.3 Create and Finalize and record Recommended Final Findings

The Recommended Findings template must be updated to it's final recommended state, based on all OE received and reviewed by the assessment team throughout the assessment, including any results from the daily reviews. It must include pass-fail ratings at the OSC aggregated level, and describe any noncompliances or nonconformances in enough detail as to show how the rating was derived by the assessment team. This includes a summary chart of all CMMC practices and their pass/fail status for each practice as well as the overall recommended maturity level rating.

Phase 3 – Report Recommended Assessment Results

3.1 Deliver Recommended Assessment Results

The CA and, if applicable, assessment team provides the Assessment Sponsor and OSC participants with assessment results. Using the Recommended Findings template, along with the details workbook or spreadsheet of all in-scope practice characterizations, the assessment findings results are delivered to the OSC Sponsor either during the final daily checkpoint, or in a separately scheduled final recommended findings review.

Phase 3.1 Required Outputs:	
Recorded and Presented Final Findings	To be completed and presented by the CA, and assessment team, if applicable, using the required CMMC Findings Brief template
Detailed Records of OE Reviewed and Examined, Resulting Practice Ratings and Justification	Using the CMMC Assessment Tracker Template
Final Assessment Plan and Schedule	Based on any real-time changes to plan/schedule during the assessment.

3.1.1 Deliver Final Findings

The CA presents the final recommended findings, using the required Recommended Findings template, a summary of the recorded pass/fail status of each CMMC practice within the assessment scope, as well as additional information that provides the context for any related findings. This activity communicates the final and complete recommended assessment results to the Assessment Sponsor 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 ratings are also presented and must included clear traceability from each finding, rating and practice pass/fail status.

As per CMMC assessment reporting requirements, the same results (same version) of findings summary (.ppt template), practice ratings and maturity level recommendations (excel tool/templatedare then submitted to the CA's C3PAO for initial processes and review. Once the C3PAO completes it's internal review, the recommended results are then submitted by the CA, through the C3PAO, to the CMMC AB for final quality review and rating approval.

3.2 Submit, Package and Archive Assessment Assets

The purpose of this phase is for the CA to package, baseline and retain all assessment assets and artifacts.

Phase 3.2 Required Outputs:	
Recorded and Presented Final Recommended Findings	To be completed and presented by the CA, using the required CMMC Findings Brief template
Submitted and archived Assessment Results Package	Final Assessment Plan, Schedule, Final Report Parts 1 and 2 (must be both), Daily Checkpoint Log
Recorded and final updated Daily Checkpoint log	Which must include attendee list, time/date, location/meeting link, results from all discussed topics, including any resulting actions and due dates from the OSC or assessment team

3.2.1 Submit Assessment Results Package

The assessment results package submitted to the C3PAO and AB by the CA, must include the following assessment artifacts:

- The final assessment plan and schedule, and the CA is responsible to verify and update the plan and schedule to reflect the actual final results and outcomes of all assessment activities
- **Final Report Part 1**: The final recommended Findings and Results summary level findings, including the recommended Maturity Level rating, using the required Recommended Findings template.
- **Final Report Part 2**: The detailed practice-level ratings, clearly traceable to each finding and rating results, using the CMMC Assessment Tracker (i.e., Excel workbook or spreadsheet with each practice ratings, findings, comments, etc.)
- **Daily Checkpoint Log**: For all daily checkpoints conducted throughout the assessment

The CA submits through the required AB assessment system portal, which then generates a notification to the C3PAO, and AB to initiate their quality reviews.

3.2.2 Provide Retrospective Feedback to C3PAO and AB

Survey to AB, C3PAO and CA
Required: AB, CA
Optional: C3PAO has its own survey?
Topics covered: Overall Assessment feedback (what went well, what didn't) feedback on CA, feedback on Assessment Team

3.2.3 Archive or Dispose of Any Assessment Artifacts

The CA 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, nondisclosure and any other CUI perspective for 3 years.

PHASE 4 REMEDIATION OF OUTSTANDING ASSESSMENT ISSUES

4.1 IDENTIFY REMEDIATION APPROACH

The purpose of remediation is intended to address situations where the initial assessment's target ML rating was not achieved, but only by a narrow margin. Accordingly, if eligible, a remediation follow-on assessment review is then conducted on a limited subset of the targeted CMMC model practices that failed to achieve a passing rating.

The CA is solely responsible for determining and recommending eligibility for remediation to the C3PAO and AB. This must first be reviewed and approved by the C3PAO and AB, and based on a request from the Sponsor to consider the assessment for eligibility for remediation.

If approved by the AB, the CA adds a Remediation approach addendum to the previous final assessment plan, which describes in detail, the review steps taken and activities performed in all subphases from Phase 2 and 3 that will be repeated for the remediation.

Planning for a remediation phase in advance of any assessment is strictly prohibited.

Phase 4.1 Required Outputs:	
Recorded Remediation Request and Response	To be completed and presented by the CA to their C3PAO and to the CMMC AB
Verified and Recorded Remediation Eligibility Analysis Results	To be completed and presented by the CA to their C3PAO and to the CMMC AB
Updated Assessment Plan and Schedule	Includes recorded eligibility results, and overall remediation approach

4.1.1 VERIFY AND CONFIRM OUTSTANDING ASSESSMENT ISSUES AND REMEDIATION ELIGIBILITY

It is the sole responsibility of the CA to review, verify and confirm any outstanding assessment issues related to a potential remediation assessment. The results of this verification must be recorded in the remediation addendum of the assessment plan. Once confirmed with the C3PAO and AB, and approved, the CA then confirms the remediation eligibility and potential follow-on activities and timing with the OSC Sponsor. All costs of any remediation activities are the sole responsibility of the OSC.

When no more than two CMMC domains or no more than 10% or the total practices in the scope of an assessment do not meet their targeted pass status, the organization may have the option to remediate any failed practices, controls, and related processes, policies and plans weaknesses during an agreed-upon remediation period not to exceed 90 calendar days. The 90-day calendar "clock" starts at the acceptance of the recommended Final Findings by the OSC, namely at the end of the Phase 2 Conduct Assessment activities are completed.

The assessment team must perform an eligibility analysis. The following criteria must be met for Remediation Eligibility:

- If the failed practices, controls or related processes, policies and plans are not systemic
- If the failed practices, controls, or related process, policies and plans can be addressed and produce expected outcomes within a 90-day timeframe, so all of the addressed failed practices must be completed by the last day of the Final Findings of the remediation events
- If the resulting actions and improvements can be made habitual and persistent within the 90-day timeframe, using the following criteria:
  - Whatever changes were made for a given practice or control, the CA and applicable assessment team determines the reason for the failed practices and what has been addressed, and that the event needs to happen more than once, i.e. a monthly test has been run at least twice before the end of remediation; a single instance will not suffice
  - Any related processes, plans, policies for any failed practice or control also must be in place before the remediation period ends and have

It is the OSC's responsibility to create a detailed, transparent and specific approach that they will take within the 90-day allowable remediation period. The CA is responsible for reviewing this and then recommending proceeding with the remediation, pending approval from the CMMC AB quality review board. Once approved or denied by the AB, the CA then notifies the OSC Sponsor that the remediation review will proceed.

The scope of the OSC, including the host unit, supporting units, and any applicable enclaves must be the same scope as the original assessment. The target maturity level must also be the same (remediation reviews cannot raise a ML rating, but may result in a lowered rating, depending on the OE provided. The OSC must use the

same CA, unless otherwise directed by the AB/C3PAO, and the assessment team, if applicable must be the same, or a subset of the original assessment team. The Sponsor must also be the same and the people providing OE must be the same people performing the work.

Any mergers or acquisition or other similar organizational change in the OSC that happens between or immediately following the initial assessment (within the 90-day period) will cause the remediation review to stop, and the previous assessment results and ratings will stand.

Only one remediation review is allowed per initial/original assessment. Whatever the final results from the remediation review are, after the CA submits the recommended results to the C3PAO and AB, and their remediation QA reviews are done, the subsequent results and ratings are then final.

4.1.2 Identify Remediation Approach and Update Assessment Plan

Once approved by the C3PAO, and Sponsor, the CA then updates the Assessment Plan Remediation Addendum with the various steps, actions and work that will be taken by the OSC to address their remediation. This is done by describing in the addendum remediation activities table:

- All the steps and activities that will be conducted by the OSC to address/remediate their failed practices, controls, and related processes, policies and plans
- How the remediation results will be verified and reviewed by the CA and, if applicable, assessment team, in a subsequent remediation assessment review
- Any differences or updated and repeated activities and steps from Phases 2 & 3 of the original initial assessment.

The CA and OSC are responsible to ensure that both the previous initial/original assessment results are kept baselined, as well as the updated remediation steps so that the C3PAO and AB can confirm both during their remediation QA reviews.

4.1.3 Submit Remediation Approach to C3PAO and AB for Verification to Proceed

Once the approach is updated in the Assessment Plan, and cover both the OSC's actions and subsequent assessment review actions are identified, the submitted to the C3PAO for review and approval to proceed. The C3PAO notifies the CA and Sponsor of their approval to proceed, and then the CA is responsible for monitoring and verifying that the remediation approach is being followed by both the OSC and by the assessment team, if applicable, in a subsequent remediation assessment review.

4.2 Execute Remediation Approach and Review

Phase 4.2 Required Outputs:	
Recorded and Verified Remediation Review Results	To be completed and presented by the CA as a part of an updated assessment plan and schedule, and Final Findings results using the required CMMC templates, any additional daily checkpoints
Updated Assessment Plan and Schedule	Includes recorded remediation review results, and overall remediation approach, plan or schedule updates

4.2.1 Review All Outstanding Issues Against Updated OE

Any new OE provided by the OSC must be reviewed by the CA and, if applicable, assessment team. The CA has the sole authority and is required to follow any related OE threads for any other practices, controls, or related processes, policies and plans for any practices that were previously rated as passing. Otherwise, the focus of the remediation assessment review is to verify that every failed practices from the initial original assessment have been adequately addressed by the OSC. This is done following the same steps and requirements from all applicable previous Phase 2 and 3 subphases and activities.

4.2.2 Update Previous Practice Pass/Fail Results and Findings

The CA, and if applicable, assessment team then updates any previously failed CMMC practices and all related assessment findings. It is the CA's responsibility to preserve both the updated and previous pass/fail assessment results for historical baselining.

4.2.3 Verify and Determine Remediated Recommendation of Maturity Level Rating

The CA, and if applicable, assessment team then updates any previously failed CMMC Maturity Level, if achieved. An updated ML rating is recorded in the updated assessment findings and results and submitted to the C3PAO and then AB for final QA review and approval.

4.2.4 Report Remediation Results

A "delta" assessment remediation package and results, including all the required artifacts cited in phase 3.2.1 above. All steps/activities in Phase 3 are then completed with both the original assessment results and the subsequent remediation results and ratings. These are submitted to the C3PAO for their internal quality board review, and those results are then submitted to the AB for it's final quality review and final assessment rating approval.

4.3: CMMC Assessment Adjudication

It is the goal of the AB, C3PAOs, and all CAs to perform and certify assessments with utmost integrity in an unbiased and professional manner. But, there will be times where the Assessor and the OSC may disagree on the results of an assessment.

- An adjudication request is submitted when the OSC disagrees with the CA and Assessment Team as to the outcome of the assessments.
- The Adjudication processes is designed to provide both transparency and rigorous review for the OSC, and due process for the CA, Assessment Team, and C3PAO
- It is the goal of the adjudication process to validate the results of the assessment, the performance of the CA and assessment team, and to be an unbiased third party that is the final arbiter of assessment results.
- An adjudication request must be submitted to the C3PAO and AB within 14 calendar days of receiving the OSC's recommended ratings and accompanying report.

Upon completion of a certified assessment, an Organization Seeking Certification (OSC) that does not achieve their planned CMMC Maturity Level, and believes the assessment result was due to errors, misinterpretation, malfeasance, or ethical lapses by the Certified Assessor or C3PAO, is entitled to submit an adjudication request for consideration to the Accreditation Body (AB).

The OSC must submit their adjudication request, along with specific detailed description and/or evidence of such lapses in writing along with the list of the controls and/or practices in question, within 14 calendar days after the completion of the Phase II (onsite) portion of their assessment. The OSC is required to pay for the cost of any subsequent adjudication appeal process conducted by the AB.

Upon receipt of the adjudication request, a Certified Quality Auditor (CQA) from the AB staff will acknowledge receipt of the request, and perform a preliminary evaluation of the Assessor or C3PAO's certification, training, quality status/standing, and licensing, and will validate their adherence to the CMMC Code of Professional Conduct (CoPC) and the CMMC Assessment Methodology (CM2CAM). The OSC will be notified of the result of the preliminary evaluation, and given the opportunity to either accept the recommendation of the CQA, or to request a secondary, more detailed, evaluation.

A secondary evaluation will be conducted if the OSC has a reasonable belief that the preliminary evaluation and evidence provided did not address the issues raised in the adjudication request. During a secondary evaluation the CQA, who is also a Certified Assessor in good standing, will plan and conduct, for a nominal fee, an onsite "delta or remediation assessment" of the controls and/or practices in question, and once completed, will submit the results, along with a recommendation, to the AB. AB quality staff will evaluate the result of the secondary evaluation and inform the OSC of the final result of the adjudication process.

Adjudicated assessments that result in a successful CMMC Maturity Level certification for the OSC will retain the validity period of three years from the last day of Phase II (onsite) of the original assessment.

APPENDIX A – CHANGE LOG

REVISION HISTORY

Revision #	Change(s)	Published Date
1.0	Initial release	xxxx
1.1	Updated Version for July 14, 2020 DIBCAC Mock Assessment Work Products	

SUMMARY OF VERSION CHANGES IN CURRENT VERSION

Change	Description of Change(s)
0	Initial release (no change)

APPENDIX B – KEY TERMINOLOGY

While it is the responsibility of the OSC to be fully aware of and compliant with all applicable statutory, regulatory and contractual obligations, the CMMC-AB wants OSC to be clear on the following key terminology:

Agreements / Arrangements[1]
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 limited to, contracts, grants, licenses, certificates, memoranda of When disseminating or sharing CUI with non-executive branch entities, agencies should enter into written agreement/arrangement or understanding and information-sharing agreements or arrangements. agreements or arrangements that include CUI provisions whenever feasible (see §2002.16(a)(5) and (6) for details). When sharing information with foreign entities, agencies should enter agreements or arrangements when feasible (see §2002.16(a)(5)(iii) and (a)(6) for details).

Affirmations
Spoken or written word from a person performing a role in an OSC practice, control or process that verifies the performance and resulting outcome of a practice or process. Affirmations can be written and submitted electronically, e.g., email, as long as the identify of the person providing the affirmation can be verified as having a process role in the OSC and is the one responsible for performing that work.

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 can be a printed hard-copy, soft- or electronic copy of a document or file or embedded in a system or software, but must be a result or output from performing a process in the OSC.

Authorized Holder[2]
Authorized holder is an individual, agency organization or group of users that is permitted to designate or handle CUI, in accordance with this part.

Certification Assessment Readiness Review
A review conducted by the CMMC CA and, as applicable, Assessment team verifying the OSC's readiness to conduct the Phase 2 portion of the Assessment against the identified assessment planning parameters and assessment scope

Controlled Environment (FCI/CUI environment)[3]
Controlled environment is any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect FCI/CUI from unauthorized access or disclosure.

Controlled Unclassified Information (CUI)[4]
The **CUI Registry** is the authoritative source for defining CUI.

Daily Checkpoint

[1] 32CFR §2002(c) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[2] 32CFR §2002(d) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[3] 32CFR §2002(f) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[4] NARA CUI Registry - https://www.archives.gov/cui

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.

Disseminating[5]

Disseminating occurs when authorized holders provide access, transmit or transfer CUI to other authorized holders through any means, whether internal or external to an agency.

Document[6]

Document means 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, whether 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.

Due Diligence[7]

Due diligence the care that a reasonable person exercises to avoid harm to other persons or their property. This is a subjective benchmark to determine if an organization's actions were sufficient enough to avoid harm. Specific to the CMMC, evidence of due diligence includes, but is not limited to:

- Documented policies, standards, and procedures;
- Developing a security-focused, multi-year business plan (e.g., roadmap) and resourcing it to achieve its goals;
- Verifying the scope of a vulnerability assessment or penetration test to ensure it is correct;
- Risk assessment of a potential vendor or other third-party; and
- Criminal background checks as a pre-requisite step in hiring decisions.

Due Care[8]

Due care is the care that an ordinarily reasonable and prudent person would use under the same or similar circumstances. This is a subjective benchmark to determine whether an organization was negligent in its duty to perform its applicable statuary, regulatory and/or contractual obligations. Specific to the CMMC, evidence of due care includes, but is not limited to:

- Identifying and assigning controls to address applicable statutory, regulatory, and contractual obligations;
- Conducting ongoing maintenance (e.g., patching operations);
- Maintaining situational awareness (e.g., log reviews);
- Performing periodic risk assessments;
- Periodically reviewing permissions and ensuring only users with legitimate business needs have access;
- Performing security awareness campaigns; and

[5] 32CFR §2002(v) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[6] 32CFR §2002(w) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[7] https://www.merriam-webster.com/dictionary/due%20diligence
[8] https://www.merriam-webster.com/legal/due%20care

- Conducting incident response tests to validate response plans are viable.

Federal Contract Information (FCI)[9]
FCI means 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[10]
Foreign entity is 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[11]
Handling is any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using and disposing of the information.

Mechanism(s)
A mechanism is flexible term to describe an established process, which can involve people, processes and/or technology:

- A technology-specific solution (e.g., antimalware, firewall, FIM, IPS, MFA, etc.);
- A manual procedure that an individual performs; or
- An administrative solution (e.g., acceptable use policy, human reviews, Non-Disclosure Agreements, etc.).

By using the term "mechanisms exist to…" in assessment criteria for CMMC practices, it provides flexibility for the OSC to define what is most appropriate for its unique business practices. For example, more mature organizations tend to automate their security solutions and prefer technology-specific solutions, where less mature organizations tend to rely on manual procedures or administrative solutions.

Misuse of CUI[12]
Misuse of CUI occurs when someone uses CUI in a manner not in accordance with the policy contained in the Order, this part, the CUI Registry, agency CUI policy or the applicable laws, regulations and Governmentwide 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 / Test
A real-time demonstration or review of a system, tool, software, hardware, practice, control or process being performed and witnessed first-hand by the CA and if applicable, Assessment team.

Unauthorized Disclosure[13]
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 controls or contrary to limited dissemination controls.

Working Papers (Drafts)[14]
Working papers are documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.

[9] https://www.federalregister.gov/documents/2016/05/16/2016-11001/federal-acquisition-regulation-basic-safeguarding-of-contractor-information-systems
[10] 32CFR §2002(y) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[11] 32CFR §2002(aa) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[12] 32CFR §2002(ee) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[13] 32CFR §2002(rr) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf
[14] 32CFR §2002(tt) - https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf

APPENDIX C – AUTHORS AND CONTRIBUTORS

PRINCIPLE AUTHORS:

Ron Lear
Jeff Dalton

CONTRIBUTORS

Kevin Schaaff
Mike Pitcher
Matt Gilbert
Michael West
Pete Barletto
Mary Segnit