- Phase 1 of the rollout has been extended to a 1-year length from 6 months. It also won't start until CFR 48 is final.
- Records retention is 6 years for ANY material generated for an assessment and any evidence provided by the OSC.
- Assessment teams must consist of a minimum of 3 CCAs. 1 Lead CCA, a 2nd CCA, and a CCA that conducts the QA that wasn't a part of the assessment team.
    - Side note on the QA CCA. They must also observe the assessment team's conduct and management of the CMMC assessment process.
- If there is a significant change to the CMMC Program requirements, CCPs, CCAs, and CCIs, could be required to recertify.
- ODPs for Level 3 have been defined by the DoD.
- Specialized assets, in a Level 3 assessment, will be assessed against all level 3 requirements. Intermediary devices are permitted to provide capability for the specialized assets.
- Contractor Risk Managed Assets (CRMA) are considered a CUI asset in a Level 3 assessment.
- CSPs must be FedRAMP or equivalent if processing, storing, or transmitting CUI. If they are only processing Security Protection Data, then the CSP's services would be assessed as Security Protection Assets.
- ESPs may process, store, or transmit CUI and the services that are provided would be assessed as part of the OSA's assessment. An ESP may voluntarily undergo a CMMC cert assessment, which would reduce the level of effort for the ESP for their clients' assessments.
- Security requirement re-evaluation - requirements that are NOT MET may be re-evaluated during the assessment and within 10 business days following if additional evidence is available, the evidence doesn't change or limit the effectiveness of other requirements that have already been MET, and the Assessment Findings Report has not been delivered.
- An endpoint hosting a VDI client, configured to not allow any processing, storage, or transmission of FCI/CUI beyond the Keyboard/Video/Mouse sent to the VDI client, is considered out-of-scope.
- DIBCAC High assessments that were conducted prior to the effective date of the rule and resulted in a perfect score will convert to CMMC Level 2 (C3PAO).
- A control described as Not Applicable might be allowable without DoD CIO approval.

Dates: 60 days after publication in the Federal Register. The FR stated that the rule will be published on 10/15/2024, making this rule in effect 12/15/2024.

History of the program (key notes):

- September 2020 DoD published the interim final rule CFR 48, which implemented the DoD's vision for the initial CMMC Program and outlined basic features of the framework.

- November 30, 2020 - CFR 48 the interim rule became effective and established a five-year phase-in period.
- November 2021 - announced the revised CMMC program that included:
    - Tiered Model based on type and sensitivity of the information and flow down requirements to subcontractors
    - Assessment requirement to verify implementation
    - Phased Implementation - 4-phase implementation over a three-year period.

Current Status of the CMMC Program

- The 48 CFR part 204 will allow the DoD to require a specific CMMC level in a solicitation or contract. Award of contract will not be given if the contractor does not have the passing results or a current certification. An affirmation requirement for continuous compliance was also added.
- ***It is also noted that the DoD may include CMMC requirements on contracts awarded prior to 48 CFR part 204***
- DCMA has assessed 357 entities.
- § 170.3 talks about the phase-in plan, but does NOT preclude entities from immediately seeking a CMMC certification assessment prior to the 48 CFR part 204 Acquisition rule being finalized and/or the clause being added to new or existing DoD contracts.
- Estimated that 8350 medium and large entities will be required to meet Level 2, with a C3PAO assessment requirement.
- Estimated that 135 (C3PAO)-led assessments will be completed in the first year, 673 in the second, 2252 in the third, and 4452 in the fourth.
- Program does not currently include any requirements for contractors operating systems on behalf of the DoD.

Page 384 (start of the rule):

§ 170.3 Applicability

- Phase 1 will not start until 48 CFR part 204 is a final rule. With some level 2 C3PAO assessments showing up in contracts in place of level 2 self-assessments, solely at the discretion of the DoD.
- Phase 2 will now begin 1 year after the start date of Phase 1 instead of 6 months. This is the phase where most of the C3PAO assessments will be required in contract. The DoD, at its discretion, can delay the inclusion of a C3PAO assessment to an option period instead of a condition of contract award.
- Phase 3 is one calendar year after phase 2. This phase is mainly a roll out of Level 3 assessments in contract.
- Phase 4 is one calendar year after phase 3 (2028), when CMMC is in full swing. CMMC will be required in all contracts including option periods.

§ 170.4 Acronyms and definitions (selection of some we found more interesting – not an exhaustive list)

- *Affirming Official* - "senior" level representative. Has the authority to affirm continuing compliance.
- *POA&M closeout certification assessment* - evaluate ONLY the not met requirements that were identified during the initial assessment.
- *CMMC Status* - officially stored in SPRS AND additionally presented on a Certificate of CMMC Status
    - Potential CMMC Statuses:
        - Final Level 1 (Self)
        - Conditional Level 2 (Self)
        - Final Level 2 (Self)
        - Conditional Level 2 (C3PAO)
        - Final Level 2 (C3PAO)
        - Conditional Level 3 (DIBCAC)
        - Final Level 3 (DIBCAC)
- *Enduring Exception* - special circumstance or system where remediation and full compliance with CMMC security requirements is not feasible. Examples: systems required to replicate the configuration of 'fielded systems', medical devices, test equipment, OT, and IoT. **Must be documented within an SSP. Specialized and GFEs may be enduring exceptions.
- *External Service Provider (ESP)* - means external people, technology, or facilities that the organization uses for provision and management of IT and/or cybersecurity services on behalf of the organization. CUI or Security Protection Data (log data, config data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP.
- *Operational plan of action* - as used in security requirement CA.L2-3.12.2, means the formal artifact which identifies temporary vulnerabilities and temporary deficiencies (e.g., necessary information system updates, patches, or reconfiguration as threats evolve) in implementation of requirements and documents how they will be mitigated, corrected, or eliminated. The OSA define the format (e.g., document, spreadsheet, database) and specific content of its operational plan of action. An operational plan of action does not identify a timeline for remediation and is not the same as a POA&M, which is associated with an assessment for remediation of deficiencies that must be completed within 180 days.
- *Organization-Defined Parameters (ODPs)* - enhanced security requirements from 800-172. **Note to ODPs: The organization defining the parameters is the DoD.**
- *Periodically* - Regular intervals determined by the OSA, to not exceed one year.
- *Plan of Action and Milestones (POA&M)* - Identifies tasks needing to be accomplished. Details resources to accomplish the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

- *Restricted Information Systems* - means systems and associated IT components that are configured based on government requirements and are used to support a contract.
- *Security Protection Data (SPD)* - data stored or processed by Security Protection Assets. Relevant information and includes but is not limited to: config data required to operate the SPA, log files generated by or ingested by an SPA, data related to the config or vulnerability status of in-scope assets, and passwords that grant access to the in-scope environment.
- *Specialized Assets* - Government Furnished Equipment (GFE), Internet of Things (IoT) or Industrial Internet of Things (IIoT), Operational Technology (OT), Restricted Information Systems, and Test Equipment.
- *Temporary Deficiency* - where remediation of a condition of a discovered deficiency is feasible, and a known fix is available or is in process. MUST be documented in an operational plan of action. NOT based on an 'in progress' implementation of a security requirement, but arises AFTER implementation. No standard duration for which a temporary deficiency may be active. Example: FIPS-validated cryptography that requires a patch and the patched version is no longer the validated version may be a temporary deficiency.
- *Test Equipment* - hardware and/or associated IT components used in testing of products, system components, and contract deliverables.

§ 170.5 Policy

- The CMMC program provides a means of verifying implementation of the security requirements set forth in 48 CFR 52.204-21, NIST SP 800-171 R2, and NIST SP 800-172 Feb2021. **Noted that DFARS 252.204-7012 is not being verified by this program.

§ 170.6 CMMC PMO

- Responsible for:
    - Oversight of the program, establish assessment, accreditation, and training requirements.
    - Monitoring of CMMC AB.
    - Right to review decisions of the CMMC AB and any alleged conflicts of interest.
    - Sponsoring necessary DCSA activities including FOCI risk assessment and Tier 3 security background investigations.
    - Investigating any active CMMC status that has been called into question. For any findings that the stated CMMC status hasn't been achieved, the DIBCAC results will take precedence.

§ 170.7 DCMA DIBCAC

- DIBCAC assessors will:
    - Complete CMMC level 2 & 3 training.
    - Conduct Level 3 assessments and upload into CMMC eMASS.

- Issue certifications for CMMC status of level 3 assessments
- Conduct level 2 assessments of AB and prospective C3PAO systems that store, process, and/or transmit CUI.
- Create and maintain process for assessors to collect assessment artifacts to include:
  - Artifact name
  - Return value of hashing algorithm
  - The hashing algorithm used
  - Upload that data into CMMC Emass
- Enter and track OSC appeals and updated results from level 3 certification assessments into eMASS.
- Retain all records in accordance with DCMA-MAN 4501-04: Records and Information Management Program (dcma.mil).
- Conduct assessments of the OSA, when requested by the CMMC PMO (§ 170.6(e)(f) - CMMC status checks).
- Identify assessments that meet the criteria in § 170.20 and verify SPRS accurately reflects the CMMC status.
- OSCs, the AB, and C3PAOs may appeal the outcome of a DIBCAC assessment within **21 days** by submitting a written basis for appeal with the requirements in question. For contact info www.dcma.mil/DIBCAC.

Subpart C -- CMMC Assessment and Certification Ecosystem

§ 170.8 Accreditation Body

- Roles and Responsibilities
  - Authorizing and ensuring C3PAOs are in accordance with ISO/IEC 17020:2012 and all applicable auth and accreditation requirements
  - Establishing C3PAO accreditation requirements
  - Establish Accreditation Scheme
  - Submitting the previous 2 bullets to the CMMC PMO for approval.
  - Only one AB at anytime
- Requirements
  - US-based
  - A member in good standing with the Inter-American Accreditation Cooperation (IAAC)
  - Signatory with International Laboratory Accreditation Cooperation (ILAC) and Mutual Recognition Arrangement (MRA)
    - Signatory status scope of ISO/IEC 17020:2012
  - Member in good standing of the International Accreditation Forum (IAF)
    - MRA signatory status scope of ISO/IEC 17024:2012
  - Achieve and maintain full compliance with ISO/IEC 17011:2017
    - Complete a peer assessment by other ILAC signatories for competence in accrediting conformity assessment bodies to ISO/IEC 17020:2012, all within **24 months** of DoD approval

- Prior to achieving full compliance to ISO/IEC 17011:2017 and the peer review the AB shall:
  - Authorize C3PAOs who meet all the requirements and the administrative requirements set by the AB, to conduct Level 2 cert assessments and issue Certificates of CMMC status
  - Require C3PAOs to achieve and maintain ISO/IEC 17020:2012, within **27 months** of authorization
- Ensure that the AB's board of directors, professional staff, IT staff, accreditation staff, and independent CMMC certified assessor staff complete a Tier 3 background investigation
- Comply with FOCI by:
  - Complete Standard Form (SF) 328 - submitted to DCSA
  - Undergo a National Security Review - must receive a non-disqualifying eligibility determination by the CMMC PMO
  - Report any change to the info in the SF 328 by resubmitting to DCSA withing **15 business days** of the change being effective.
  - ID all prospective C3PAOs to the CMMC PMO. The CMMC PMO will sponsor the C3PAO for a FOCI risk assessment using the SF 328 as part of the process
  - Notify prospective C3PAOs of the CMMC PMO's eligibility determination resulting from the FOCI risk assessment
- Obtain a Level 2 cert, assessment to be conducted by DIBCAC, requirements for a Final Level 2 (C3PAO)
  - Will not result in a CMMC Status of Level 2, must be performed every **three** years
- Provide all docs and records in English
- Establish, maintain, and manage an up-to-date list of authorized and accreditation records and status in CMMC eMASS.
  - Data should include dates of authorized and accredited C3PAOs on a single publicly accessible website
- Provide the CMMC PMO with current data on C3PAOs in CMMC eMASS:
  - Authorization and accreditation records and status and the dates of both
- Provide the DoD with info about aggregate stats pertaining to the operations of the Ecosystem
- Provide inputs for assessor supplemental guidance to the CMMC PMO.
- Ensure that all info about individuals is encrypted and protected in all AB's info systems and databases.
- Provide all plans related to potential sources of revenue to the CMMC PMO, to include but NOT limited to:
  - Fees, licensing, processes, membership, and/or partnerships
- Ensure the CAICO is compliant with ISO/IEC 17024:2012
- Ensure training products, instruction, and testing materials are of **high** quality and subject to CAICO quality control.

        - Includes technical accuracy and alignment with legal, regulatory, and policy requirements.
    - Develop and maintain an internal appeals process. Render final decision on ALL elevated appeals
    - Develop and maintain the following that apply to all in the Ecosystem who provide Level 2 cert assessments and to be approved by the CMMC PMO:
        - Conflict of Interest (COI) policy - must include:
            - Detailed risk mitigation plan for all potential COI that may pose a risk to compliance with ISO/IEC 17011:2017
            - Require employees, Board directors, and members of ANY accreditation committees or appeals adjudication committees to disclose to the CMMC PMO (in writing), any actual, or potential, or perceived COI
            - Require the same as the previous who leave the board or org to enter a "cooling off period" of one year, where they are prohibited from working with the AB or participating in any and all CMMC activities
            - Require the Ecosystem members to actively avoid any activity or practice that could be perceived COI
            - Require Ecosystem members to disclose to the AB leadership (in writing) any actual or potential COI ASAP
        - Code of Professional Conduct (CoPC) - shall:
            - Describe the performance standards by which Ecosystem members will be held accountable and the procedures for addressing violations of those standards
            - Require the AB to investigate and resolve any potential violations that are reported or identified by the DoD
            - Inform the DoD in writing of new investigations within **72 hours**
            - Report to the DoD in writing the outcome of investigations within **15 business days**
            - Require Ecosystem members to represent themselves and their companies accurately. --to include:
                - no misrepresentation of credentials or status
                    - CMMC Status or authorization
                    - Exaggerating the services that they or their company are capable or authorized to deliver
            - Require Ecosystem members to be honest and factual in all CMMC related activities
            - Prohibit Ecosystem members from participating in Level 2 cert assessments process for which they previously served as a consultant to prepare the org for **any** CMMC assessment within **3 years**
            - Require Ecosystem members to maintain the confidentiality of customer and gov data to preclude unauthorized disclosure

        - Require Ecosystem members to report results and data from level 2 assessments, objectively, completely, clearly, and accurately.
        - Prohibit cheating or assisting another in cheating on CMMC examinations
        - Require that official training content developed by the CAICO is utilized in ALL cert courses
    - Ethics Policy - shall:
        - Require Ecosystem members to report to the AB within **30 days** of convictions, guilty pleas, or no contest pleas to crimes of:
            - Fraud, larceny, embezzlement, misappropriation of funds, misrepresentation, perjury, false swearing, conspiracy to conceal, or similar offense
            - Prohibit harassment or discrimination by ecosystem members in all interactions
            - Require ecosystem members to have and maintain a record of integrity and business ethics

§ 170.9 CMMC Third-Party Assessment Organizations (C3PAOs)

- Roles and responsibilities:
    - Responsible for conducting Level 2 cert assessments and issuing Certificates of CMMC status.
    - Must be accredited or authorized by the AB
- Requirements:
    - Obtain authorization or accreditation from the AB
    - Comply with the AB policies for COI, CoPC, and Ethics.
    - Achieve/Maintain compliance with ISO/IEC 17020:2012, within **27 months** of authorization
    - Require all company personnel participating in the Level 2 cert assessment process to complete a Tier 3 background check (suitability)
        - This includes assessment team AND the quality assurance individual
    - Require all personnel participating in the assessment process NOT eligible for a Tier 3 background check to meet the equivalent of a favorably adjudicated. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program **only**.
    - Comply with FOCI by:
        - Submit SF 328
        - Receive a non-disqualifying eligibility determination from the CMMC PMO resulting from a DIBCAC Level 2 assessment.
        - Report any change to SF 328 within **15 business days** of the change being effective. A disqualifying eligibility determination will result in the C3PAO losing it authorization or accreditation.

- Undergo a Level 2 certification assessment meeting all the requirement for a Final Level 2 (C3PAO)
  - Conducted by DIBCAC
  - Does not result in a Certificate or a result of CMMC Status of Level 2 (C3PAO)
- Provide all documentation and records in English
- Submit pre-assessment and planning material, final assessment reports, and CMMC certs of assessment into CMMC eMASS
- Unless disposition is otherwise authorized by the CMMC PMO, maintain **ALL** assessment related records for a period of **six (6) years**
  - To include: **Any** materials generated by the C3PAO in the course of an assessment, **any** working papers generated from Level 2 cert assessments; **and** materials relating to monitoring, education, training, tech knowledge, skills, experience, and authorization of all personnel involved in assessment activities; contractual agreements with OSCs; and organizations for whom consulting services were provided.
- Provide any requested audit info, including any out-of-cycle from ISO/IEC 17020:2012, to the AB
- Ensure all PII is encrypted and protected in all C3PAO systems and databases
- Assessment Team composition: Must include at least **two** people: A Lead CCA (§ 170.11), and at least one other CCA. Other CCAs and CCPs may also participate.
- Implement a QA function that ensures the accuracy and completeness of assessment data prior to upload into CMMC eMASS.
  - This individual **MUST** be a CCA **AND** cannot be a member of the assessment team for which they are performing the QA for.
  - This individual shall manage the QA reviews **AND** the appeals process.
  - Conduct QA reviews for each assessment, **including** observations of the assessment team's conduct and management of CMMC assessment processes.
- Ensure all assessment activities are performed on the IS within the CMMC assessment scope.
- Maintain all facilities, personnel, and equipment involved in CMMC activities that are in scope of the C3PAO's cert assessment
- Ensure all assessment data and info is compliant with the CMMC assessment data standard set forth in eMASS CMMC Assessment Import Templates (https://cmmc.emass.apps.mil) - only accessible to authorized users.
- Issue certificates of CMMC status in accordance with § 170.17
  - To include (at a minimum):

        - all industry CAGE codes associated with the IS addressed by the CMMC assessment scope
        - The C3PAO name
        - Assessment unique identifier
        - The OSC name
        - The CMMC status, date, and level
    - Address all OSC appeals. If the OSC or C3PAO is not satisfied with the result of the appeal, either can elevate the matter to the AB
    - Submit assessment appeals, review records, and decision results of assessment appeals to DoD using eMASS.

§ 170.10 CMMC Assessor and Instructor Certification Organization (CAICO)

- Roles and responsibilities:
    - Training, testing, authorizing, certifying, and recertifying CMMC assessors, instructors, and related professionals.
    - ONLY one that may make decisions relating to examination certifications
    - Only one CAICO at any given point of time.
- Requirements:
    - Comply with the AB's, COI, CoPC, and Ethics
    - Achieve/maintain ISO/IEC 17024, within **12 months** of [60 days after the publication in the FR] [most likely Dec 15, 2024]
    - Provide all documentation and records in English
    - Train, test, and designate Pis
    - Ensure the instructor and assessor cert examinations are certified under ISO/IEC 17024:2012, by a recognized US-based accreditor who is not a member of the AB.
    - Establish QC policies and procedures for the generation of training products, instruction, and testing materials.
    - Oversee development, admin, and management pertaining to the quality of generated materials
    - Establish and publish and appeals process for auth and certifications.
    - Address all appeals
    - Maintain records for a period of **six (6) years** of all procedures, processes, and actions related to the AB's requirements
    - Provide the AB info about auth and accreditation status of assessors, instructors, etc.
    - Ensure separation of duties between testing activities, training activities, and cert activities
    - Safeguard and require and CAICO training service providers to safeguard the confidentiality of applicant, candidate, and cert holder info.
    - Ensure that all PII is encrypted in CAICO's IS and databases AND those of any CAICO training support service providers
    - Ensure the security of assessors and instructors exams and the fair and credible admin of examinations

- Do not disclose nor allow any CMMC data or metrics to any entity other than the AB
- Require retraining and redesignation of PIs and retraining and recertification of CCPs, CCAs, and CCIs upon **significant** change to DoD's CMMC Program.
- Require reporting to CAICO within **30 days** of convictions, guilty pleas, etc..

§ 170.11 CMMC Certified Assessor (CCA)

- Roles and responsibilities:
  - In support of a C3PAO, conduct level 2 cert assessments, in accordance with NIST SP 800-171A Jun2018
- Requirements
  - Obtain/maintain cert from CAICO. Cert is valid for **three (3) years** from the date of issuance.
  - Comply with the AB's COI, CoPC, and Ethics.
  - Complete a Tier 3 background check (suitability)
  - Meet the equivalent of a favorable adjudicated Tier 3 when not eligible for a Tier 3
  - Provide all documentation and records in English
  - Be a CCP who has at least **3 years** of cybersecurity experience, at least **1 year** of assessment or audit experience, at least **1 foundational qualification**, aligned to at least the Intermediate proficiency level of DoD cyberspace workforce framework's security control assessor from 8140.03, https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf
  - Only use IT, cloud, cyber services, and end-point devices provided by the authorized/accredited C3PAO. Prohibited from using any other IT, including personal devices, to process, store, or transmit CMMC assessment reports or related CMMC info
  - Immediately notify C3PAO of any breach or potential breach of security to assessment related materials under the assessor's purview
  - Not share **any** info about an OSC obtained during CMMC pre-assessment and assessment activities with any person not involved with that specific assessment.
  - ****Qualify as a Lead CCA****: have **5 years** of cybersecurity experience, **5 years** management, **3 years** of assessment or audit experience, at least **1 foundational qualification**.

§ 170.12 CMMC Instructor

- The PI role ends **18 months** after Dec 15, 2024
- CMMC Certified Instructor (CCI) roles and responsibilities
  - Teaches CCP, CCA, and CCI candidates
  - Required to maintain assessor and instructor certs from CAICO
  - A CCI with a CCP may instruct CCPs. A CCI with a CCA may instruct CCP, CCA, and CCI candidates.

    - Certs valid for **3 years** from date of issuance.
- Requirements:
    - Maintain designation or cert from CAICO
    - Obtain/maintain CCP or CCA cert to deliver CCA training
    - Obtain/maintain CCA cert to deliver CCA training
    - Comply with Ab's COI, CoPC, and Ethics
    - Provide all docs and records in English
    - Provide the AB and CAICO **annually** with
        - Accurate info detailing their qualifications
        - Training experience
        - Professional affiliations
        - Certifications
        - Upon reasonable request, documentation verifying the above info
    - Not provide consulting while serving as a CMMC instructor, subject to COI and CoPC can serve on an assessment team
    - Not participate in the development of exam objectives and/or exam content or act as an exam proctor while a CCI
    - Keep all info confidential relating to training activities and trainee records
    - Not disclose CMMC related data/metrics that is PII, FCI, or CUI without prior coordination and approval from DoD
    - Notify the AB or CAICO to release confidential info
    - Not share any training related info not previously publicly disclosed.

§ 170.13 CMMC Certified Professional (CCP)

- Roles and responsibilities:
    - Provides advice, consulting, and recommendations to their OSA clients
- Requirements:
    - Obtain/maintain cert from CAICO, valid for **3 years**
    - Comply with AB's COI, CoPC, and Ethics
    - Complete Tier 3 background
    - Favorable result of equivalent, if not eligible for a Tier 3
    - Provide all docs and records in English
    - Not share any info obtained during pre or post assessment with any person not involved with that specific assessment.

Subpart D--Key Elements of the CMMC Program

§ 170.14 CMMC Model

- Overview
    - Incorporates security requirements from 48 CFR 52.204-21 (FCI)
    - Security requirements from NIST SP 800-171 R2 (CUI/Level 2)
    - Selected requirements from NIST SP 800-172 Feb2021 (CUI/Level 3)
- CMMC Domains

    - Consists of domains that map to the security requirement families in NIST SP 800-171 R2
- CMMC level requirements
    - Numbering scheme: DD.L#-REQ
        - DD is the two-letter domain
        - L# is the CMMC level number
        - REQ is the requirement number from either the paragraph number of 48 CFR 52.204-21 or requirements number of NIST SP 800-171 R2 & NIST SP 800-172 Feb2021
    - Level 1 - 48 CFR 52.204-21
    - Level 2 - Identical to the requirements in NIST SP 800-171 R2
    - Level 3 - Selected from NIST SP 800-172 Feb2021
        - Where applicable ODPs are assigned.
        - Looks like 25 controls were selected, which includes 83 assessment objectives, and 22 ODPs. 10 controls were not selected, that included 21 assessment objectives, and 15 ODPs
    - Implementation
        - Periodically means occurring at regular intervals, with an interval length of no more than one year.

§ 170.15 CMMC Level 1 self-assessment and affirmation requirements

- Meet all level 1 requirements, no POA&Ms
- Must complete a self-assessment annually
- Submit results into SPRS to include:
    - CMMC Level
    - CMMC status date
    - CMMC assessment scope
    - All industry CAGE codes(s) associated with the system addressed by the scope
    - Compliance results
    - [reserved]?
    - Affirmation of results
- Prior to award, must submit CMMC status of level 1 (self) and submit affirmation of compliance
- In any assessment objective that refers to CUI, FCI should be substituted.
- Artifacts used as evidence for the assessment must be retained by the OSA for **six (6) years** from the CMMC status date.

§ 170.16 CMMC Level 2 self-assessment and affirmation requirements

- Must meet all the requirements of Level 1 and level 2
- Must conduct this assessment every **three years** and submit the results in SPRS, within **three years** of the CMMC status date with the conditional level 2 (self)
- SPRS submission to include at a minimum:
    - CMMC Level

    - CMMC Status date
    - CMMC assessment scope
    - All industry CAGE code(s) associated with the scope
    - Overall level 2 self-assessment score (e.g., 105 out of 110)
    - POA&M usage and compliance status, if applicable
        - A level 2 POA&M is allowed only in accordance with requirements listed in § 170.21
- Must remediate any NOT MET requirements and post results to SPRS within 180 days of status date. If not closed within 180 days, the conditional cert status expires. If CMMC status expires within the period of performance, standard contractual remedies will apply and the OSA will be ineligible for additional awards.
- DoD reserves the right to conduct an assessment of the OSA. If the results show that adherence has not been achieved, the DIBCAC results will take precedence over any pre-existing CMMC status.
- Affirmation is required for all level 2 self-assessments at each assessment and annually thereafter.
- Level 2 self-assessment with a CSP
    - Allowed to use CSP **IF** the CSP is authorized at the FedRAMP Moderate (or higher) baseline or they meet a FedRAMP Moderate equivalent baseline, in accordance with DoD policy.
    - If the OSA's infrastructure connects to the CSP's product **or** service offering.
        - The security requirements from the CRM **must** be documented or referred to in the OSA's SSP.
- Level 2 self-assessment with a ESP
    - The use of the ESP, its relationship to the OSA, and the services provided are documented in the OSA's SSP **and** described in the ESP's service description and CRM.
    - The ESP services used to meet the OSA requirements are assessed within the scope of the OSA's assessment against all Level 2 security requirements
- Artifacts used as evidence for the assessment must be retained by the OSA for **six (6) years** from the CMMC status date

§ 170.17 CMMC Level 2 certificate assessment and affirmation requirements

- Undergo a level 2 assessment by an authorized C3PAO - achieving a status of level 2 (C3PAO) also satisfies the requirements for level 1 & level 2 self-assessment.
- C3PAO submits results into CMMC eMASS. Electronically submits to SPRS
    - Date and level of the assessment.
    - C3PAO name.
    - Assessment unique identifier.
    - For each Assessor conducting the assessment, name and business contact information.
    - All industry CAGE codes associated with the information systems addressed by the CMMC Assessment Scope.
    - The name, date, and version of the SSP.

    - CMMC Status Date.
    - Assessment result for each requirement objective.
    - POA&M usage and compliance, as applicable.
    - List of the artifact names, the return value of the hashing algorithm, and the hashing
    - algorithm used.
- Same rules for POAM closeout as in the level 2 self-assessment, but the C3PAO is the one that submits the results
- DoD reserves the rights to inspect an OSC
- Affirmation required for all assessments at the time of assessment and annually thereafter
- Same eligibility requirements as the level 2 self-assessment
- Final results are communicated to the OSC through a CMMC Assessment Findings Report
- **Security requirement re-evaluation**. A requirement that is NOT MET may be re-evaluated during the course of the level 2 cert assessment and for **10 business days** following the active assessment period if all the following conditions exist:
    - Additional evidence is available to demonstrate the security requirement has been MET
    - Cannot change or limit the effectiveness of other requirements that have been scored MET
    - The CMMC Assessment Finding Report has NOT been delivered.
- The hashed artifacts used as evidence for the assessment must be retained by the OSC for **six (6) years** from the CMMC Status Date.
    - To ensure that the artifacts have not been altered, the OSC must hash the artifacts using a NIST-approved hashing algorithm.
    - The OSC must provide the C3PAO with a list of the artifact names, the return value of the hashing algorithm, and the hashing algorithm for upload into eMass
- Same CSP and ESP requirements of the level 2 self-assessment

§ 170.18 CMMC Level 3 certification assessment and affirmation requirements

- Must have a CMMC Status of Final Level 2 (C3PAO)
- DIBCAC to perform the assessment
- Must be performed every **three years** and a level 2 (C3PAO) must also be conducted every **three years** to maintain a CMMC Level 3 (DIBCAC) status.
- Same submission and POA&M requirements as a level 2
- Affirmation is required for all level 3 cert assessments and annually thereafter
- The OSC (including ESPs that voluntarily elect to undergo a level 3 cert assessment) initiate the request by emailing DCMA DIBCAC. The request must include the level 2 cert assessment unique identifier. DIBCAC will validate and then contact the OSC to schedule their Level 3.
- For assets that change asset category or requirements between level 2 and level 3, DIBCAC will perform limited checks of the level 2 security requirements, if found to

be NOT MET, the level 3 may be paused to allow remediation, placed on hold, or immediately terminated.

- Same security requirement re-eval as level 2.
- Same artifact retention requirements of a level 2
- Same CSP allowance with the one note:
    - Use of a CSP does not relieve an OSC of the 24 level 3 requirements.
    - The 24 requirements apply to every environment where CUI is.
    - Must show a Customer Implementation Summary/CRM and associated BoE
    - The BoE must clearly indicate whether the OSC or the CSP is responsible and which are implemented vs inherited.
- ESP allowance is the same as a level 2

§ 170.19 CMMC Scoping

- Assessment scope must be specified prior to assessment.
- The scope is the set of all assets in the OSA's environment that will be assessed.
- Level 1
    - Assets which process, store, or transmit FCI are in scope and must be assessed
    - Out of scope assets are any that DO NOT store, process, or transmit FCI. ** Example ** an endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of FCI beyond the KVM sent to the VDI client is considered out of scope. (page 448)
    - Specialized assets that can store, process, or transmit FCI but cannot be fully secured. Specialized assets are not assessed against CMMC
    - People, technology, facilities, and ESPs are considered when scoping.
- Level 2
    - CUI Asset
        - Assets that process, store, or transmit CUI
            - Document in the asset inventory
            - Document asset treatment in the System Security Plan (SSP)
            - Document in the network diagram of the CMMC Assessment Scope
            - Prepare to be assessed against CMMC Level 2 security requirements
            - Assess against all Level 2 security requirements
    - Security Protection Asset
        - Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope
            - Document in the asset inventory
            - Document asset treatment in the System Security Plan (SSP)
            - Document in the network diagram of the CMMC Assessment Scope
            - Prepare to be assessed against CMMC Level 2 security requirements

        - Assess against all Level 2 security requirements that are relevant to the capabilities provided
- Contractor Risk Managed Assets
    - Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place
    - Assets are not required to be physically or logically separated from CUI assets
        - Document in the asset inventory
        - Document asset treatment in the System Security Plan (SSP)
        - Document in the network diagram of the CMMC Assessment Scope
        - Prepare to be assessed against CMMC Level 2 security requirements
        - Review the SSP:
            - If sufficiently documented, do not assess, except as noted
            - If OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies
            - The limited check(s) shall not materially increase the assessment duration nor the cost
            - The limited check(s) will be assessed against CMMC security requirements
- Specialized Assets
    - Assets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment
        - Document in the asset inventory
        - Document asset treatment in the SSP
        - Show these assets are managed using the contractor's risk-based security policies, procedures, and Practices
        - Document in the network diagram of the CMMC Assessment Scope
        - Review the SSP:
            - Do not assess against other CMMC security requirements
- Out-of-scope Assets
    - Assets that cannot process, store, or transmit CUI;
    - and do not provide security protections for CUI Assets
    - Assets that are physically or logically separated from CUI assets

- Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset
- An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset
    - Prepare to justify the inability of an Out-of-Scope Asset to process, store, or transmit CUI

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

Table 4 to § 170.19(c)(2)(i)—ESP Scoping Requirements

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

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

- Level 3 Scoping - key notes
  - Some possible checks for CUI/SPA assets for level 2 requirements
  - Specialized assets will be assessed against all level 3 requirements
  - The level 3 assessment scope **must** be equal to or a **subset** of the level 2 assessment scope
  - Any level 2 POA&Ms must be closed prior to initiating a level 3 assessment.
  - DIBCAC may check **any** level 2 security requirements, if anything from level 2 is found to be NOT MET, the level 3 may be paused or cancelled

§ 170.20 Standards acceptance

- An OSC that achieved a perfect score with NO open POA&M from a DIBCAC High **conducted prior to the effective date of this rule**, will be given a CMMC Status of Level 2 Final (C3PAO).
  - To be valid for **three (3) years** from the date of the DIBCAC High Assessment.
  - DIBCAC will identity which assessments meet the criteria and verify that SPRS accurately reflects the CMMC status.
  - The scope of the Level 2 assessment must be identical to the scope of the DIBCAC High
  - The OSC must submit an affirmation in SPRS and annually after for eligibility.

§ 170.21 Plan of Action and Milestones requirements

- For Conditional CMMC Status permitted POA&M requirements:
  - Level 1 - No POA&Ms permitted
  - Level 2
    - Assessment score divided by the total number of requirements is greater or equal to 0.8 (SPRS 88)
    - No point value of greater than 1 **except** SC.L2-3.13.11 may be included if encryption is employed but is not FIPS-validated, which would result in a point value of 3
    - 1 point controls not allowed:
      - AC.L2-3.1.20 - External Connections
      - AC.L2-3.1.22 - Control Public Information
      - CA.L2-3.12.4 - System Security Plan
      - PE.L2-3.10.3 - Escort Visitors

        - PE.L2-3.10.4 - Physical Access Logs
        - PE.L2-3.10.5 - Manage Physical Access
    - Level 3
        - Same score requirements of level 2, score divided by the total number of level 3 requirements is greater or equal to 0.8. § 170.24(c)(3) If they are all worth 1, then you would have to have met 20 of the 24 controls that have been selected for level 3.
        - Controls that cannot be on a POA&M:
            - IR.L3-3.6.1e - Security Operations Center
            - IR.L3-3.6.2e - Cyber Incident Response Team
            - RA.L3-3.11.1e - Threat-Informed Risk Assessment
            - RA.L3-3.11.4e - Security Solution Rationale
            - RA.L3-3.11.6e - Supply Chain Risk Response
            - RA.L3-3.11.7e - Supply Chain Risk Plan
            - SI.L3-3.14.3e - Specialized Asset Security
- POA&M closeout
    - Only the NOT MET requirements identified during the initial assessment
    - Must be closed within **180 days** from the Conditional CMMC Status Date, if not then the conditional status expires
    - Level 2 self-assessment - to be closed out in the same manner as the initial assessment
    - Level 2 cert assessment - closeout cert assessment **must** be performed by an authorized/accredited C3PAO
    - Level 3 cert assessment - DIBCAC will perform the closeout certification

§ 170.22 Affirmation

- An affirming official must affirm after every assessment (including POA&M closeout), and annually afterwards.
- To be entered in SPRS
- Affirming Official **must** be a **senior level representative** from within each OSA.
    - Responsible for ensuring compliance with the OSA's CMMC Program requirements
    - Has the authority to affirm the OSA's continuing compliance
- Affirming Content shall include:
    - Name, title, and contact info for the Affirming Official
    - Affirmation statement attesting that the OSA has implemented and will maintain implementation of all applicable CMMC security requirements to their CMMC Status for all information systems within the relevant CMMC Assessment Scope.
- Affirmation SPRS Submission happens:
    - Achievement of Conditional CMMC Status
    - Final CMMC Status (self & cert)
        - Annually following a Final CMMC Status date
    - Following a POA&M closeout assessment

§ 170.23 Application to subcontractors

- Applies to **all** prime and subcontractors throughout the supply chain at **all** tiers that will process, store, or transmit FCI or CUI.
- Prime contractors shall comply and require subcontractors to comply **and** flow down CMMC requirements to all tiers.
    - If the sub will only access FCI then a CMMC Status of Level 1 (Self) is required
    - If the sub will access CUI, then a CMMC Status of Level 2 (Self) is the **minimum** requirement
    - If the sub will access CUI **and** the associated prime contract has a requirement of CMMC Status Level 2 (C3PAO) then that is the minimum for the sub
    - If the sub will access CUI **and** the associated prime contract has a requirement of **CMMC Status Level 3 (DIBCAC)** then **CMMC Status Level 2 (C3PAO)** is the minimum for the sub

§ 170.24 CMMC Scoring Methodology

- Met
    - ALL applicable objectives are satisfied based on evidence.
    - All evidence must be final form and not draft.
    - Unacceptable forms of evidence examples (not limited to):
        - Working papers
        - Drafts
        - Unofficial or unapproved policies
    - Enduring exceptions (see definition above), when described, along with any mitigations, in the SSP **shall** be assessed as MET
    - Temporary deficiencies that are appropriately addressed in **operational plans of action** (to include deficiency reviews and show progress toward the implementation of corrections to reduce or eliminate identified vulnerabilities) **shall** be assessed as MET
- Not Met
    - One or more applicable objectives is not satisfied.
    - The assessor will document why the evidence does not conform
- Not Applicable (N/A)
    - The requirement or objective does not apply at the time of the CMMC assessment.
    - Example: SC.L2-3.13.5 (Public-Access System Separation) might be N/A if there are no publicly accessible systems within the CMMC Assessment Scope.
    - An assessment objective assessed as N/A is equivalent to the same objective being assessed as MET.
- Scoring
    - Level 1 - all requirements must be fully implemented

- Level 2 - Equal to the total number of the level 2 security requirements
  - For each NOT MET, the associated value is subtracted from the maximum score (which may result in a negative score)
  - Each requirement has a value (e.g., 1, 3, or 5), related to the control designation by NIST as basic or derived security.
    - Basic requirements are obtained from FIPS PUB 200 Mar2006
    - Derived requirements are from NIST SP 800-53 R5
    - For both basic and derived if the control is not implemented, would lead to significant exploitation of the network or exfiltration of CUI, **five (5) points** are subtracted. 23 basic and 18 derived for, 41 5-point controls
    - 3 point controls that would have a specific and confined effect on the security of the network. 7 basic controls and 7 derived for, 14 3-point controls
    - Limited or indirect effect on the security of the network are 1 point
    - IA.L2-3.5.3 and SC.L2-3.13.11 can be partially effective and the points deducted may be adjusted depending on how it is implemented
      - IA.L2-3.5.3, if **only** implemented for remote and privileged users would subtract 3 points. If not implemented at all would subtract 5
      - SC.L2-3.13.11, if encryption is employed, but is not FIPS-validated, 3 points would be subtracted. If no encryption the 5 points would be subtracted
  - OSAs MUST have an SSP. So for CA.L2-3.12.4, if there is an absence of an up to date SSP at the time of the assessment, it would result in a finding that *'an assessment could not be completed due to incomplete information and noncompliance with 48 CFR 252.204-7012.'*
  - Each NOT MET must have a POA&M in place. A POA&M addressing a NOT MET is not a substitute for a completed requirement.
  - Specialized assets must be evaluated for their category based on the scoping guidance for the level in question.
  - Previous adjudication from the DoD CIO indicating that a requirement is not applicable or that an alternative measure is equally effective **must** be included in your SSP to receive consideration during an assessment.
- Level 3 - does not use varying values. All level requirements use a value of 1.
  - Maximum score would be 24.
  - Score is reduced by 1 for each NOT MET requirement.
  - Maximum score from level 2 is required prior to a level 3 assessment.