CMMC Proposed Rule: Notable Updates

December 24, 2023

WELCOME

December 22, 2023 the Office of the Department of Defense Chief Information Officer (CIO), Department of Defense (DoD) issued a long-awaited Proposed Rule for the Cybersecurity Maturity Model Certification (CMMC) program. This 234-page Proposed Rule will be/has been published to the Federal Register December 26, 2023.

In an effort to help the CMMC Ecosystem quickly identify the material changes/additions/deletions from the current CMMC 2.0 program, CMMC Training Academy is publishing this CMMC Proposed Rule: Notable Updates document.

CMMC Proposed Rule: Notable Updates ONLY highlights the changes/additions/deletions from the current program; it DOES NOT provide the full details of the program. This document MUST be used in reference with existing knowledge of the current CMMC program. This document DOES NOT outline the full proposed program. If the reader would like a full understanding of the proposed program it is required to read the entire Proposed Rule.

This document is segmented into topical groupings. The information noted in each grouping may contain notable items from various parts of the Proposed Rule.

Please let us know if there are any errors or areas that you feel are material and should be included.

TERMS

- **CMMC Certified Professional (CCP)** changed from Certified CMMC Professional (CCP)
- **CMMC Certified Assessor (CCA)** changed from Certified CMMC Assessor (CCA)
- **CMMC Certified Instructor (CCA)** changed from Certified CMMC Instructor (CCI)
- **CMMC Level 2 Conditional Certification Assessment**: The OSC has achieved CMMC Level 2 Conditional Certification Assessment if a POA&M exists upon completion of the assessment and the POA&M meets all CMMC Level 2 POA&M requirements.
- **CMMC Level 2 Conditional Self-Assessment**: OSAs have achieved CMMC Level 2 Conditional Self-Assessment if the LEvel 2 self-assessment results in a POA&M and the POA&M meets all the CMMC Level 2 POA&M requirements.
- **CMMC Level 2 Final Certification Assessment**: The OSC will achieve CMMC Level 2 Final Certification Assessment for the information systems within the CMMC Assessment Scope upon implementation of all security requirements and close out of the POA&M, as applicable.
- **CMMC Level 2 Final Self-Assessment**: The OSA will achieve CMMC Level 2 Final Self-Assessment compliance for the information system(s) within the CMMC Assessment Scope upon implementation of all security requirements and close out of the POA&M, as applicable.
- **CMMC Level 3 Conditional Certification Assessment**: The OSC has achieved CMMC Level 3 Conditional Certification Assessment if a POA&M exists upon completion of the assessment and the POA&M meets all CMMC Level 3 POA&M requirements.
- **CMMC Level 3 Final Certification Assessment**: The OSC will achieve CMMC Level 3 Final Certification Assessment for the information systems within the CMMC Assessment Scope upon implementation of all security requirements and close out of any POA&M, as applicable.
- **Organization Seeking Assessment (OSA)** means the entity seeking to conduct, obtain, or maintain a CMMC assessment for a given information system at a particular CMMC Level. The term OSA includes all Organizations Seeking Certification (OSCs).
- **Organization Seeking Certification (OSC)** means the entity seeking to contract, obtain, or maintain CMMC certification for a given information system at a particular CMMC Level. An OSC is also an OSA.

PROGRAM OPERATIONS

- Program Managers and requiring activities identify the applicable CMMC Level. Factors used to determine which CMMC Level will be applied are included but not limited to:
  - Criticality of the associated mission capability;
  - Type of acquisition program or technology;
  - Threat of loss of the FCI or CUI to be shared or generated in relation to the effort;
  - Potential for and impacts from exploitation of information security deficiencies; and
  - Other relevant policies and factors, including Milestone Decision Authority guidance.
- A DoD Service Acquisition Executive or a Component Acquisition Executive may elect to waive inclusion of CMMC Program requirements in a solicitation or contract.
- Level 2 OSA: In order to be eligible for a contract with a CMMC Level 2 Self-Assessment requirement, the OSA must have a Level 2 Conditional Self-Assessment or Level 2 Final Self-Assessment and have submitted an affirmation.
- Level 2 OSA: After both Conditional Self-Assessment and Final Self-Assessment, the OSA must input their results into SPRS.
- Level 2 OSC: In order to be eligible for a contract with a CMMC Level 2 Certification Assessment requirement, the OSC must have a CMMC Level 2 Conditional Certification Assessment or CMMC Level 2 Final Certification Assessment and have submitted an affirmation.
- Level 2 OSC: After both Conditional Certification Assessment and Final Certification Assessment, the C3PAO will input the OSC's results into the CMMC instantiation of eMASS.
- Level 3 OSC: In order to be eligible for a contract with a CMMC Level 3 Certification Assessment requirement, the OSC must have a CMMC Level 3 Conditional Certification Assessment or CMMC Level 3 Final Certification Assessment and have submitted an affirmation.
- Level 3 OSC: After both Conditional Certification Assessment and Final Certification Assessment, DCMA DIBCAC will input the OSC's results into the CMMC instantiation of eMASS.
- Offerors and contractors will be informed of CMMC requirements in solicitations through (1) the specification of a required CMMC Level, and (2) inclusion of the appropriate DFARS provisions or clauses.
- There is no plan to advertise a list of solicitations that will or may include CMMC requirements.

PROGRAM IMPLEMENTATION

- The DoD is implementing a phased implementation for the CMMC Program and intends to introduce CMMC requirements in solicitations over a three-year period to provide appropriate ramp-up time.
- The Department anticipates it will take two years for companies with existing contracts to become CMMC certified.
- DoD intends to include CMMC requirements for Levels 1, 2, and 3 in all solicitations issued on or after October 1, 2026, when warranted by any FCI or CUI information protection requirements for the contract effort.
- In the intervening period, DoD Program Managers will have discretion to include CMMC requirements in accordance with DoD policies.
- The phased implementation plan is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements.
- An extension of the implementation period or other solutions may be considered in the future to mitigate any C3PAO capacity issues, but the Department has no such plans at this time.

- Phase 1: Begins on the effective date of the CMMC revision to DFARS 252.204- 7021. DoD intends to include CMMC Level 1 Self-Assessment or CMMC Level 2 Self-Assessment for all applicable DoD solicitations and contracts as a condition of contract award.
    - DoD may, at its discretion, include CMMC Level 1 Self-Assessment or CMMC Level 2 Self-Assessment for applicable DoD solicitations and contracts as a condition to exercise an option period on a contract awarded prior to the effective date.
    - DoD may also, at its discretion, include CMMC Level 2 Certification Assessment in place of CMMC Level 2 Self-Assessment for applicable DoD solicitations and contracts.
- Phase 2: Begins six months following the start date of Phase 1. In addition to Phase 1 requirements, DoD intends to include CMMC Level 2 Certification Assessment all for applicable DoD solicitations and contracts as a condition of contract award.
    - DoD may, at its discretion, delay the inclusion of CMMC Level 2 Certification Assessment to an option period instead of as a condition of contract award.
    - DoD may also, at its discretion, include CMMC Level 3 Certification Assessment for applicable DoD solicitations and contracts.
- Phase 3: Begins one calendar year following the start date of Phase 2. In addition to Phase 1 and 2 requirements, DoD intends to include CMMC Level 2 and Level 3 Certification Assessment for all applicable DoD solicitations and contracts as a condition of contract award and, for CMMC Level 2, as a condition to exercise an option period on a contract awarded prior to the effective date.
    - DoD may, at its discretion, delay the inclusion of CMMC Level 3 Certification Assessment to an option period instead of as a condition of contract award.
- Phase 4 (Full Implementation): Begins one calendar year following the start date of Phase 3. DoD will include CMMC Program requirements in all applicable DoD solicitations and contracts including option periods on contracts awarded prior to the beginning of Phase 4.

DISPUTES

- Each C3PAO is required to have a time-bound, internal appeals process to address disputes related to perceived assessor errors, malfeasance, and unethical conduct.
- Requests for appeals will be reviewed and approved by individual(s) within the C3PAO not involved in the original assessment activities in question.
- If a dispute regarding assessment findings cannot be resolved by the C3PAO, it will be escalated to the Accreditation Body.
- The decision by the Accreditation Body will be final.
- A request for an appeal about an assessor's professional conduct that is not resolved with the C3PAO will be escalated and resolved by the Accreditation Body.
- The issue of C3PAO liability is between an OSC and the C3PAO with which it contracts to do the assessment.

SECURITY REQUIREMENTS

- The numbering scheme for security requirements remains DD.L#-REQ where the 'DD' is the two-letter domain abbreviation, the 'L#' is the CMMC Level, and the 'REQ' is based directly on the numbering in the source.
- The number sources include FAR 52.204-21, NIST SP 800-171, and NIST SP 800-172.
- The notable change is for CMMC Level 1 where the numbering of controls there are now aligned to FAR 52's b.1.i-b.1.xv (e.g., AC.L1-b.1.i); whereas for Level 2 it uses NIST SP 800-171 numbering (e.g., AC.L2-3.1.1).

EXTERNAL SERVICE PROVIDERS

- If an OSA utilizes an ESP, other than a Cloud Service Provider (CSP), the ESP must have a CMMC certification level equal to or greater than the certification level the OSA is seeking.
- If the ESP is internal to the OSA, the security requirements implemented by the ESP should be listed in the OSA's SSP to show connection to its in-scope environment.
- CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP.
- An OSC may use a Federal Risk and Authorization Management Program (FedRAMP) Moderate (or higher) cloud environment to process, store, or transmit CUI in execution of a contract or subcontract with a requirement for CMMC Level 2 under the following circumstances:
    - CSP's product or service offering is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline; or
    - meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline.
        - CSP equivalency is met if the OSA has the CSP's System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 Rev 2 requirements.
        - The OSA's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSA's System Security Plan (SSP).

SCOPE

- Level 3 Assessment Scope also includes all Specialized Assets but allows an intermediary device to provide the capability for the Specialized Asset to meet one or more CMMC security requirements, as needed. These assets (or the applicable intermediary device, in the case of Specialized Assets) are fully assessed against the applicable CMMC security requirements.
- When a CMMC Level 2 Certification Assessment is performed as a precursor to a CMMC Level 3 Certification Assessment, the IOT and OT (and all other Specialized Assets) should be assessed against all CMMC Level 2 security requirements.
    - For CMMC Level 3, an OSC's IoT or OT located within its CMMC Assessment Scope are assessed against all CMMC security requirements unless they are physically or logically isolated.

SCORING

- Controls with a value of 5 or 3 are considered highest and not eligible for a POA&M.
- Level 3 controls have a value of 1.
- Description of Level 2 Out of Scope Assets has been extended and now states: 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.

DEFINE THE WORD

HIGHEST

"Being at a point or level higher than all others."

"...have a point value of greater than 1..."

ASSESSMENTS

- It is possible for an organization to need a new assessment during the validity period.
- If the CMMC Assessment Scope changes due to infrastructure modifications or expansion of the CMMC Assessment Scope due to new acquisition, a new assessment may be required.
- The information system(s) in the new CMMC Assessment Scope may not be used to process, store, or transmit CU for any contract until it is validated via a new CMMC assessment.
- At the time of a new self-assessment or certification, a new affirmation is submitted into SPRS affirming that the organization meets the CMMC requirements and will maintain the applicable information system (within the CMMC Assessment Scope) at the required CMMC level.
- A NOT MET requirement may be re-evaluated during the course of the assessment and for 10 business days following the active assessment period if all of the following conditions exist:
  - Additional evidence is available to demonstrate the security requirement has been MET;
  - The additional evidence does not materially impact previously assessed security requirements; and
  - The CMMC Assessment Findings Report has not been delivered.
- Certified CMMC Assessors working at their place of business or from home must use their C3PAO's IT infrastructure.
- Unless disposition is otherwise authorized by the CMMC PMO, C3PAO must maintain all assessment related records for a period of six (6) years including any materials provided by OSC, generated by the C3PAO in the course of an assessment, any working papers generated from Level 2 Certification Assessments; and materials relating to monitoring, education, training, technical knowledge, skills, experience, and authorization of all personnel involved in inspection activities; contractual agreements with OSCs; and organizations for whom consulting services were provided.
- Individual assessors may only use IT, cloud, cybersecurity services, and end-point devices provided by the authorized/accredited C3PAO that they support and has received a CMMC Level 2 Certification Assessment or higher for all assessment activities.
- Individual assessors are prohibited from using any other IT, including IT that is personally owned, to include internal and external cloud services and end-point devices, to store, process, handle, or transmit CMMC assessment reports or any other CMMC assessment-related information.
    - If during a Level 3 Assessment DCMA DIBCAC identifies that a Level 2 security requirement is NOT MET, the Level 3 assessment process may be placed on hold or terminated.

PLAN OF ACTION & MIILESTONE (POA&M)

- Permitted at Level 2 (both self-assessment and C3PAO assessment) if:
  - the assessment score divided by the total number of security requirements is greater than or equal to 0.8; and
  - none of the security requirements included in the POA&M have a point value of greater than 1 except SC.L2-3.13.11 CUI Encryption
    - may be included on a POA&M if it has a value of 1 or 3.
- No security requirements may be placed on a POA&M for Level 1.
- Level 2 Self-Assessment: If the minimum score has been achieved and some security requirements are in a POA&M, the OSA has a Conditional Self-Assessment; if the minimum score has been achieved and no security requirements are in a POA&M, the OSA has a Final Self-Assessment.
- POA&M must be closed within 180 days of the assessment.
- After both Conditional Self-Assessment and Final Self-Assessment, the OSA must input their results into SPRS.
  - Any Level 2 POA&M items must be closed prior to the initiation of the CMMC Level 3 Certification Assessment.

LIMITED PRACTICE DEFICIENCY PROGRAM

- Program eliminated.

ANNUAL AFFIRMATIONS

- Annual affirmations required at all CMMC levels.
  - Affirm continuing compliance with the specified security requirements.
  - Affirmation by a senior official at the contractor after every assessment, including POA&M closeout.
- Entered into SPRS.
- Monitoring contractor compliance with the terms of the contract is the responsibility of the contractor, with the government contracting officer.
- DoD is not utilizing a continuous monitoring capability in lieu of compliance requirements.

STATUS REVOCATION

- If the CMMC PMO determines that the provisions of Level 1 or Level 2 of this rule have not been achieved or maintained then standard contractual remedies will apply and the OSC will be ineligible for additional awards with CMMC Level 2 Certification Assessment or higher requirements for the information system within the CMMC Assessment Scope until such time as a valid CMMC Level 2 Certification Assessment is achieved.

ACCREDITATION BODY

- There is only one Accreditation Body for the DoD CMMC Program at any given time, and its primary mission is to authorize and accredit the C3PAOs.
- The Accreditation Body must be a member in good standing with the Inter-American Accreditation Cooperation (IAAC) and become an International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA) signatory, with a signatory status scope of ISO/IEC 17020:2012 and be compliant with ISO/IEC 17011:2017.
- Prior to the Accreditation Body being compliant with ISO/IEC 17011:2017 and completing a peer assessment of conformity with the IAAC in accordance with the ISO Committee on Conformity Assessment, the Accreditation Body may authorize but not accredit C3PAOs.
- The Accreditation Body may accredit C3PAOs after it has achieved compliance with ISO/IEC 17011:2017 and completed a peer assessment of conformity with the IAAC in accordance with the ISO Committee on Conformity Assessment.

CMMC ASSESSOR AND INSTRUCTOR ORGANIZATION (CAICO)

- There is only one CAICO for the DoD CMMC Program at any given time.
- The CAICO must comply with ISO/IEC 17024:2012, as well as with the Accreditation Body's policies for CoI, CoPC, and Ethics.

CMMC THIRD-PARTY ASSESSMENT ORGANIZATION (C3PAO)

- C3PAOs need to comply with ISO/IEC 17020:2012, as well as with the Accreditation Body's policies for CoI, CoPC, and Ethics.
- Prior to a C3PAO being compliant with ISO/IEC 17020:2012, the C3PAO may be authorized but not accredited.
- After a C3PAO is compliant with ISO/IEC 17020:2012, the C3PAO may be accredited.
- C3PAOs must achieve and maintain the ISO/IEC 17020:2012 requirements within 27 months of authorization.
- If ISO/IEC 17020:2012 is revised or superseded, the Accreditation Body shall require full compliance with the updated standard within 12 months of the date of revision.
- Must obtain a CMMC Level 2 Certification Assessment conducted by DCMA DIBCAC, which shall meet all requirements for a Level 2 Final Certification Assessment but will not result in a CMMC Level 2 certificate.
- The CMMC Level 2 assessment process must be performed on a triennial basis.
- All C3PAO company personnel participating in the CMMC assessment process to complete a Tier 3 background investigation.
- C3PAO must conduct quality assurance reviews for each assessment, including observations of the Assessment Team's conduct and management of CMMC assessment processes.

CMMC QUALITY ASSURANCE PROFESSIONAL (CQAP)

- Tier 3 background investigation is also required for the CMMC Quality Assurance Professional (CQAP).
- CQAP must be a CCA.
- CQAP cannot be a member of an Assessment Team for which they are performing a quality assurance role.

LEAD ASSESSOR

- Obtain and maintain CCA certification.
- At least 5 years of cybersecurity experience, 5 years of management experience, 3 years of assessment or audit experience, and at least one baseline certification aligned to either paragraph IAM Level II or Advanced Proficiency Level for Career Pathway Certified Assessor 612 through 15 February 2025 and aligned to Advanced Proficiency Level for Career Pathway Certified Assessor 612 only beginning 16 February 2025.
    - (i) IAM Level II (i.e., CAP, CASP+ CE, CISM, CISSP (or Associate), GSLC, CCISO, HCISPP) from DoD Manual 8570 Information Assurance Workforce Improvement Program.
    - (ii) Advanced Proficiency Level for Career Pathway Certified Assessor 612 from DoD Manual 8140.03 Cyberspace Workforce Qualification & Management Program.
        - DoDM 8140.03 Advanced Proficiency Level
            - The role requires an individual to:
                - 1. Have an in-depth understanding of advanced concepts and processes and experience applying these with little to no guidance.
                - 2. Be able to provide guidance to others.
                - 3. Be able to perform successfully in complex, unstructured situations.

CMMC CERTIFIED ASSESSOR (CCA)

- Obtain and maintain certification.
- Three (3) assessment experience requirement not listed.
- Comply with Conflict of Interest, Code of Professional Conduct and Ethics.
- Complete Tier 3 background investigation or equivalent.
    - DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only.
- Be a CCP with at least 3 years of cybersecurity experience, 1 year of assessment or audit experience, and at least one baseline certification aligned to either: IAT Level II (i.e., CCNA-Security, CySA+, GICSP, GSEC, Security+ CE, CND or SSCP) or Intermediate Proficiency Level for Career Pathway Certified Assessor 612 from DoD Manual 8140.03 Cyberspace Workforce Qualification & Management Program)
    - DoDM 8140.03 Intermediate Proficiency Level:
        - The role requires an individual to:
            - 1. Have extensive knowledge of basic concepts and processes and experience applying these with only periodic high-level guidance.
            - 2. Be able to perform successfully in non-routine and sometimes complicated situations.

CMMC CERTIFIED PROFESSIONAL (CCP)

- Obtain and maintain certification.
- Comply with Conflict of Interest, Code of Professional Conduct and Ethics.
- Complete Tier 3 background investigation or equivalent.
    - DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only.

CMMC CERTIFIED INSTRUCTOR (CCI)

- Obtain and maintain certification.
- Cannot provide CMMC consulting services while serving as a CMMC instructor.
- Cannot participate in the development of exam objectives and/or exam content or act as an exam proctor while at the same time serving as a CCI.

INCORPORATED BY REFERENCE

- Source for Definitions: Federal Information Processing Standard (FIPS) Publication (PUB) 200, "Minimum Security Requirements for Federal Information and Information Systems"
- Source for Definitions: FIPS PUB 201-3, titled "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- Source for Definitions: NIST SP 800-37, revision 2, titled "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"
- Source for Definitions: NIST SP 800-39, titled "Managing Information Security Risk: Organization, Mission, and Information System View"
- Source for Definitions: NIST SP 800-53, revision 5, titled "Security and Privacy Controls for Information Systems and Organizations"
- Source for Definitions: NIST SP 800-82, revision 2, titled "Guide to Industrial Control Systems (ICS) Security"
- Source for Definitions: NIST SP 800-115, titled "Technical Guide to Information Security Testing and Assessment"
- Source for Definitions: NIST SP 800-160, Volume 2, revision 1, titled "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach"
- Foundational Source for Definitions and Security Requirements: NIST SP 800-171, revision 2, titled "Security Requirements for Controlled Unclassified Information"
- Foundational Source for Definitions and Assessment: NIST SP 800-171A, titled "Assessing Security Requirements for Controlled Unclassified Information"

- Foundational Source for Security Requirements: NIST SP 800-172, titled "Enhanced Security Requirements for Controlled Unclassified Information"
- Foundational Source for Definitions and Assessment: NIST SP 800-172A, titled "Assessing Enhanced Security Requirements for Controlled Unclassified Information"
- Source for Definitions: Committee on National Security Systems (CNSS) Instruction No. 4009
- Source for CMMC Ecosystem Requirements: ISO/IEC 17011:2017, titled "Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies"
- Source for CMMC Ecosystem Requirements: ISO/IEC 17020:2012, titled "Conformity assessment — Requirements for the operation of various types of bodies performing inspection"
- Source for CMMC Ecosystem Requirements: ISO/IEC 17024:2012, titled "Conformity assessment — Requirements for the operation of various types of bodies performing inspection"

CHANGE CONTROL

Date		
December 24, 2023	Version 1.0	Initial baseline.