Decoding the CMMC 2.0 Proposed Rule:
Key Insights for DoD Contractors

Written by:
Scott Singer, CCA, CCP | Rachel Leidy, CCA, CCP, CISSP

CyberNINES is excited to present this comprehensive analysis paper, crafted by our experts at CyberNINES, to provide you with a concise overview of the key facets of the CMMC 2.0 Proposed Rule (Proposed 32 CFR Part 170 CMMC Program). In response to the evolving landscape of cybersecurity threats, the Department of Defense (DoD) has proposed significant updates to the Cybersecurity Maturity Model Certification (CMMC) framework. This document serves as a distilled guide, condensing the essential information from the extensive 234-page proposed rule. Our aim is to empower you with insights into the proposed requirements, enabling your organization to navigate the complexities of compliance seamlessly. We encourage you to leverage this analysis to stay informed about the pivotal changes and proactively prepare for the future cybersecurity requirements outlined by CMMC 2.0.

Contents

Bottom Line Up Front (BLUF) **2**
CMMC 2.0 Program Highlights: 2
When Will CMMC Show Up in Contracts? **2**
Phased Approach for CMMC Program Implementation 2
What Assessment Level is RequiredShould I Prepare For? **3**
Section § 170.23 Application to Subcontractors 3
What Will an Assessment Entail? **4**
Assessment Types 4
CMMC Level 1 Self-Assessment 4
CMMC Level 2 Self-Assessment: 5
CMMC Level 2 Certification Assessment: 6
CMMC Level 3 Certification Assessment: 7
How Will Assessments Be Scored? **9**
Section § 170.24 CMMC Scoring Methodology 9
Are There Any Annual Requirements? **11**
Section 170.22 Affirmation 11
Conclusion: **12**
Encouraging Action: **12**

Bottom Line Up Front (BLUF)

CMMC 2.0 Program Highlights:

Navigating the intricacies of the Cybersecurity Maturity Model Certification (CMMC) 2.0 Program is essential for Department of Defense (DoD) contractors seeking a comprehensive understanding of key points crucial to their operations. This section serves as a guide, distilling essential information that contractors should be well-versed in to ensure strategic planning and compliance.

CMMC 2.0 Program – Proposed Rule:

- Applies to all DoD contract and subcontract awardees dealing with information processing, storage, or transmission meeting standards for Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) on contractor non-Federal information systems.
- When finalized, defense contract solicitations involving FCI or CUI on non-Federal systems will include CMMC level and assessment type requirements.
- Contractual processes related to CMMC will be addressed in a separate rulemaking (Defense Federal Acquisition Regulation Supplement (DFARS) Case 2019-D041).
- DoD is responsible for selecting the CMMC Level based on the type of information (FCI or CUI) processed on, stored on, or transmitted through a contractor information system.
- Application of CMMC Level for subcontractors is determined in accordance with § 170.23. (Included below is a summary of § 170.23 "Application to subcontractor")
- CMMC Program does not replace other applicable requirements to protect FCI or CUI. Existing requirements, such as Federal Acquisition Regulation (FAR) 52.204-21, DFARS 252.204-7012 and DFARS subpart 204.73, remain in effect.
- CMMC Program provides a means of verifying the implementation of security requirements outlined in FAR 52.204-21, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev 2, and NIST SP 800-172, as applicable. (See Assessment Types section for details)
- Phased Implementation: DoD adopts a phased approach for the inclusion of CMMC Program requirements in solicitations and contracts. It is predicted that DoD contractors can expect to start seeing CMMC as early as Q1 2025 (estimate). (See Phased Approach for CMMC Program Implementation section for details)

When Will CMMC Show Up in Contracts?

Phased Approach for CMMC Program Implementation

This section outlines DoDs phased implementation of the CMMC program with key milestones. The implementation and enforcement of the CMMC Program will start once the specified revision to DFARS 252.204-7021 becomes effective.

The timeline for making revisions effective can vary and is typically determined by the regulatory process. Revisions to regulations, such as DFARS clauses, typically go through a formal rulemaking process, which includes several stages like proposal, public comment period, adjudication, and final rule issuance. The specific duration for making revisions effective can depend on factors such as the complexity of the changes, the level of public input required, and any legal or procedural requirements in the rulemaking process.

Anticipate the inclusion of CMMC requirements in contracts and proposals for DoD contractors, with visibility expected as early as the first quarter of 2025.

DoDs phased implementation of the CMMC program:

1. **Phase 1: CMMC Revision to DFARS 252.204-7021**
    - Begins on the effective date of the CMMC revision.
    - CMMC Level 1 Self-Assessments or CMMC Level 2 Self-Assessments with both requiring Senior Official Attestations posted on SPRS as a condition of award (Note: The Senior Official can be held responsible under the False Claims Act).
    - DoD may include CMMC Level 2 Certification Assessment at its discretion.

2. **Phase 2: Six Months After Phase 1**
    - CMMC Level 2 Certification Assessment for all applicable DoD solicitations and contracts as a condition of award.
    - DoD has the option to delay the inclusion of CMMC Level 2 Certification Assessments to contracts at its discretion.
    - DoD may also include CMMC Level 3 Certification Assessments at its discretion.

3. **Phase 3: One Calendar Year After Phase 2**
    - DoD has the option to require a CMMC Level 2 Certification Assessment to a contract that was self-assessed prior to the effective date.
    - Intends to include CMMC Level 3 Certification Assessment for all applicable DoD solicitations and contracts as a condition of award.
    - DoD may delay the inclusion of CMMC Level 3 Certification Assessment to an option period at its discretion.

4. **Phase 4 (Full Implementation): One Calendar Year After Phase 3**
    - CMMC Program requirements included in all applicable DoD solicitations and contracts, including option periods on contracts awarded before the beginning of Phase 4.

What Assessment Level is Required?

Section § 170.23 Application to Subcontractors

Section 170.23 outlines the flow down of CMMC requirements from prime contractors to subcontractors across the supply chain.

Summary of § 170.23 Application to Subcontractors:

CMC Level Flow Down Requirements for Subcontractors:

- **If Subcontractor deals with FCI (not CUI):**
    - Requirement: CMMC Level 1 Self-Assessment.
- **If Subcontractor processes, stores, or transmits CUI:**
    - Minimum Requirement: CMMC Level 2 Self-Assessment.
- **Additional Requirements if Prime Contractor specifies:**
    - If Prime Contractor requires Level 2 Certification Assessment, Subcontractor minimum requirement is CMMC Level 2 Certification Assessment.
    - If Prime Contractor requires Level 3 Certification Assessment, Subcontractor minimum requirement is CMMC Level 2 Certification Assessment.

- CMMC is required at all levels of the supply chain from primes to subcontractors.
- CMMC levels for subcontractors depend on the type of unclassified information and the priority of the acquisition program or technology.
- DoD Program Managers or requiring activities are responsible for selecting the applicable CMMC Level based on the type of information (FCI or CUI) processed through a contractor's information system.
- Program Managers and requiring activities consider factors like criticality, type of program, threat level, potential impacts, and relevant policies to determine the CMMC Level for a procurement.
- Prime contractors must identify the required CMMC Level for subcontractors, following flow-down guidelines; however, the specific CMMC Level required for a subcontractor will be based on the type of unclassified information and the priority of the acquisition program and/or technology being developed.
- If uncertain about the appropriate CMMC Level for subcontract solicitations, prime contractors should consult with the government program office.
- Prime contractors are obligated to comply and ensure subcontractor compliance, adhering to the relevant CMMC level specified for each subcontract.
- Solicitations may specify multiple CMMC Levels if different enclaves are expected to process, store, or transmit information with varying security requirements.

What Will an Assessment Entail?

Assessment Types

The CMMC Program represents a significant shift in how the DoD assesses and ensures the cybersecurity practices of its contractors. Unlike DFARS 252.204-7012, where compliance with NIST SP 800-171 Rev. 2 was not consistently verified, the CMMC Program introduces a robust assessment framework. This framework comprises four distinct assessment types, each playing a crucial role in evaluating a contractor's adherence to specified cybersecurity standards. Under the CMMC Program, compliance checks are conducted by independent third-party assessors certified by the DoD, ensuring a more rigorous and standardized approach to cybersecurity verification. As the CMMC Program progresses, defense contract solicitations will include CMMC level and assessment type requirements, paving the way for a comprehensive and tailored evaluation of contractors' cybersecurity maturity. This section outlines each of the four assessment types in the CMMC Program, shedding light on their respective requirements and implications for contractors seeking eligibility for DoD contracts.

CMMC Level 1 Self-Assessment

- **CMMC Level 1 Self-Assessment Requirement:**
  - **Requirements:**
    1. The OSA (Organization Seeking Assessment) must fulfill the requirements specified in this section to comply with CMMC Level 1.
    2. A self-assessment must be completed, achieving a MET result for all security requirements in § 170.14(c)(2).
    3. No POA&Ms (Plan of Action and Milestones) are allowed for CMMC Level 1.
    4. The OSA must conduct an annual self-assessment and submit results in the Supplier Performance Risk System (SPRS).
  - **SPRS Inputs:**
    1. SPRS inputs for self-assessment results must include CMMC Level, Assessment Date, Assessment Scope, associated industry CAGE code(s), and Compliance result.

- **CMMC Status Revocation:**
    1. If CMMC Program Management Office (PMO) determines non-compliance, the CMMC Level 1 Self-Assessment's validity status may be revoked.
    2. Revocation triggers standard contractual remedies, and the OSA becomes ineligible for additional awards with CMMC Level 1 or higher requirements until a valid CMMC Level 1 Self-Assessment is achieved.
- **Affirmation:**
    1. Affirmations are mandatory for all CMMC Level 1 Self-Assessments.
    2. Affirmation procedures are outlined in § 170.22. (Included is a summary of § 170.22 "Affirmation")

- **Contract Eligibility:**
    - OSAs must comply with CMMC Level 1 Self-Assessment requirements and submit an affirmation of compliance in SPRS for all information systems within the CMMC Assessment Scope before being eligible for contract or subcontract awards with a CMMC Level 1 requirement.
- **Procedures for Self-Assessment:**
    - **CMMC Scoring Methodology:**
        1. Self-assessment must be scored according to the CMMC Scoring Methodology detailed in § 170.24. (Included is a summary of § 170.24 "CMMC Scoring Methodology")
        2. Must align with the CMMC Level 1 scope requirements in § 170.19(a) and (b).
    - **Use of NIST SP 800-171A:**
        1. Self-assessment must use objectives defined in NIST SP 800-171A for the security requirement mapping to CMMC Level 1.
        2. A mapping table specifies the correlation between CMMC Level 1 security requirements and NIST SP 800-171A objectives.

CMMC Level 2 Self-Assessment:

- **Level 2 Self-Assessment Requirement:**
    - **Requirements:**
        1. OSAs must meet Level 2 Self-Assessment requirements outlined in paragraphs (a)(1) and (2).
        2. Level 2 Self-Assessment also satisfies Level 1 Self-Assessment requirements for the same CMMC Assessment Scope.
    - **Self-Assessment:**
        1. OSAs must achieve a MET result for all security requirements in § 170.14(c)(3).
        2. Conduct a self-assessment in accordance with specified procedures and submit results in SPRS.
        3. Perform Level 2 Self-Assessment triennially and submit results in SPRS annually.
        4. SPRS inputs include CMMC Level, Assessment Date, Assessment Scope, industry CAGE code(s), Overall self-assessment score, and POA&M usage and compliance status, if applicable.
    - **Conditional Self-Assessment:**
        1. OSAs achieve Level 2 Conditional Self-Assessment if a POA&M results and meets Level 2 POA&M requirements.
        2. POA&M closeout required within 180 days; if not closed out, Conditional Self-Assessment expires, triggering standard contractual remedies.
    - **Final Self-Assessment:**

1. OSAs achieve Level 2 Final Self-Assessment upon implementing all security requirements and closing out the POA&M, if applicable.

- **CMMC Status Revocation:**
  1. If PMO determines non-compliance with Level 1 or Level 2, a revocation of Level 2 Self-Assessment validity status may occur, triggering standard contractual remedies.
- **Affirmation:**
  1. Affirmations are required at each assessment and annually thereafter for Level 2 Self-Assessments.
  2. Affirmation procedures are detailed in § 170.22. (Included is a summary of § 170.22 "Affirmation")

- **Contract Eligibility:**
  - **Requirements:**
    1. OSAs must achieve CMMC Level 2 Conditional or Final Self-Assessment as per (a)(1).
    2. Submission of an affirmation of compliance into SPRS is required.
- **Procedures:**
  - **Self-Assessment Process:**
    1. OSAs must perform a Level 2 Self-Assessment according to NIST SP 800-171A and specified CMMC Level 2 scoping requirements.
    2. Assessment scored using the CMMC Scoring Methodology in § 170.24. (Included is a summary of § 170.24 "CMMC Scoring Methodology")
    3. POA&M closeout assessment required within the 180-day period.
  - **Self-Assessment of Cloud Service Provider (CSP):**
    1. OSAs may use FedRAMP Moderate (or higher) cloud environment under certain conditions.
    2. Conditions include FedRAMP Authorization of CSP's product or service offering or equivalent security requirements.
    3. On-premises infrastructure connecting to the CSP's offering is part of the CMMC Assessment Scope and assessed accordingly.

CMMC Level 2 Certification Assessment:

- **Level 2 Certification Assessment Requirement:**
  - **Requirements:**
    1. OSCs must meet Level 2 Certification Assessment requirements in (a)(1) and (2).
    2. Certification Assessment satisfies Level 2 Self-Assessment requirements from § 170.16 for the same CMMC Assessment Scope.
  - **Certification Assessment:**
    1. Complete and achieve a MET result for all Level 2 requirements; contractors must implement 110 security requirements from NIST SP 800-171 Rev 2 (as required by DFARS clause 252.204-7012).
    2. Obtain CMMC Level 2 Conditional or Final Certification through a C3PAO.
    3. Triennial basis; results submitted to CMMC instantiation of eMASS, then SPRS.
  - **Inputs into eMASS:**
    1. Assessment results include date and level, C3PAO information, assessor details, industry CAGE codes, SSP details, program rule, certification date, assessment result for each requirement, POA&M status, and artifact information.
  - **Conditional Certification Assessment:**

1. Achieved if a POA&M exists upon assessment completion and meets Level 2 POA&M requirements.
2. POA&M closeout required within 180 days; expiration triggers standard contractual remedies.

- **Final Certification Assessment:**
  1. Achieved upon implementing all security requirements and closing out the POA&M, if applicable.
- **CMMC Status Revocation:**
  1. If PMO determines non-compliance with Level 1 or Level 2, revocation of Level 2 Certification Assessment may occur.
  2. Revocation automatically causes the revocation of any dependent Level 3 Certification Assessments.
- **Affirmation:**
  1. Affirmations required upon completion of each assessment and annually thereafter.
  2. Affirmation procedures detailed in § 170.22. (Included is a summary of § 170.22 "Affirmation")

- **Contract Eligibility:**
  - **Requirements:**
    1. OSCs must achieve either CMMC Level 2 Conditional or Final Certification Assessment.
    2. Submission of an affirmation of compliance into SPRS is required.
- **Procedures:**
  - **Assessment Process:**
    1. Authorized or accredited C3PAO performs assessment according to NIST SP 800-171A and Level 2 scoping requirements.
    2. Assessment scored using CMMC Scoring Methodology in § 170.24, and results communicated through a CMMC Assessment Findings Report. (Included is a summary of § 170.24 "CMMC Scoring Methodology")
  - **Security Requirement Re-evaluation:**
    1. A requirement NOT MET may be re-evaluated under specific conditions during and post-assessment.
  - **POA&M:**
    1. POA&M closeout assessment required within 180-day closeout period for Final Certification.
    2. Artifacts used as evidence must be retained for the certificate's validity period and at least six years, hashed using a NIST-approved algorithm.
  - **Assessment of Cloud Service Provider:**
    1. OSCs may use FedRAMP Moderate (or higher) cloud environment under specific conditions, including FedRAMP Authorization or equivalent security requirements.
    2. On-premises infrastructure connecting to CSP's offering is part of the CMMC Assessment Scope.

CMMC Level 3 Certification Assessment:

CMMC Level 3 requirements are identified for solicitations supporting critical programs and technologies.

- **Level 3 Certification Assessment Requirement:**
  - **Requirements:**

1. CMMC Level 2 Final Certification Assessment for systems within the Level 3 CMMC Assessment Scope is a prerequisite.

- **Certification Assessment:**
  1. Achieve CMMC Level 2 Final Certification Assessment on Level 3 CMMC Assessment Scope. C3PAOs can assess Level 2 controls.
  2. Complete and implement all Level 3 security requirements specified in table 1 to § 170.14(c)(4) before initiating CMMC Level 3 Certification Assessment; contractors and subcontractors must implement 24 selected security requirements from NIST SP 800-172.
  3. DCMA DIBCAC performs CMMC Level 3 Certification Assessment on a triennial basis. DoD DIBCAC performs Level 3 assessment on the Level 3 security requirements specified in table 1 to § 170.14(c)(4).
  4. Assessment results submitted to CMMC instantiation of eMASS, then SPRS.
- **Inputs into eMASS:**
  1. Assessment results include date and level, assessor details, industry CAGE codes, SSP details, certification date, result for each security requirement, POA&M status, and artifact information.
- **Conditional Certification Assessment:**
  1. Achieved if a POA&M exists upon assessment completion and meets all Level 3 POA&M requirements.
  2. POA&M closeout required within 180 days; expiration triggers standard contractual remedies.
- **Final Certification Assessment:**
  1. Achieved upon implementing all security requirements and closing out any POA&M.
- **CMMC Status Revocation:**
  1. Revocation may occur if provisions of the rule are not achieved or maintained.
  2. Revocation triggers standard contractual remedies and ineligibility for additional awards until a valid Level 3 Certification Assessment is achieved.
  3. Revocation of Level 2 Final Certification Assessment automatically revokes any dependent Level 3 Certification Assessments.
- **Affirmation:**
  1. Affirmations required upon completion of each assessment and annually thereafter.
  2. Affirmation procedures detailed in § 170.22. (Included is a summary of § 170.22 "Affirmation")

- **Contract Eligibility:**
  - **Requirements:**
    1. OSCs must achieve either CMMC Level 3 Conditional Certification Assessment or CMMC Level 3 Final Certification Assessment.
    2. Submission of an affirmation of compliance into SPRS is required.
- **Procedures:**
  - **Assessment Process:**
    1. Includes CMMC Level 2 Final Certification Assessment for the same scope before the Level 3 assessment.
    2. DCMA DIBCAC performs CMMC Level 3 Certification Assessment according to NIST SP 800-172A and CMMC Level 3 scoping requirements.
  - **Security Requirement Re-evaluation:**
    1. A requirement NOT MET may be re-evaluated under specific conditions during and post-assessment.
  - **POA&M:**

1. POA&M closeout assessment by DCMA DIBCAC required within 180-day closeout period for Final Certification.

- **Artifact Retention and Integrity:**
  1. OSC retains hashed artifacts for the certificate's validity period and at least six years.
  2. Hashed artifact details provided to the CMMC instantiation of eMASS.
- **Assessment of Cloud Service Provider:**
  1. OSC may use FedRAMP Moderate (or higher) cloud environment under specific conditions, including FedRAMP Authorization or equivalent security requirements.
  2. On-premises infrastructure connecting to CSP's offering is part of the CMMC Assessment Scope.

How Will Assessments Be Scored?

Section § 170.24 CMMC Scoring Methodology

Section 170.24 outlines the scoring methodology, utilized by CMMC Third-Party Assessment Organizations (C3PAO), self-assessors, and Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessors, to measure implementation of NIST SP 800-171 Rev 2 and, for CMMC Level 3, the specified NIST SP 800-172 security requirements.

Summary of § 170.24 CMMC Scoring Methodology for DoD Contractors:

- **General:**
  - Scoring measures OSA's implementation status of NIST SP 800-171 Rev 2 and specified NIST SP 800-172 security requirements.
  - Designed to credit partial implementation in limited cases (e.g., multi-factor authentication).

- **Assessment Findings:**
  - MET:
    - All objectives for the security requirement are satisfied based on final evidence.
    - All evidence must be in final form and not draft. Unacceptable evidence forms include drafts, working papers, and unofficial policies.
  - NOT MET:
    - One or more applicable objectives for the security requirement are not satisfied.
    - Assessor documents reasons for non-conformance.
  - NOT APPLICABLE (N/A):
    - Security requirement or objective does not apply at the time of assessment.
    - Assessment objective assessed as N/A is equivalent to MET.

- **Special Considerations:**
  - OSAs must have a system security plan (CA.L2-3.12.4) in place to describe each information system within the CMMC Assessment Scope, and a POA&M (CMMC Level 2 security requirement CA.L2-3.12.2) in place for each NOT MET security requirement
  - A POA&M for NOT MET requirements is not a substitute for completed requirements.
  - Specialized Assets ("enduring exceptions") must be evaluated for their asset category per the CMMC scoping guidance.

- **DoD CIO Adjudication:**
  - OSCs with a favorable DoD CIO adjudication for an alternative security measure must include it in the system security plan for consideration during assessment.

- **Assessment Scoring:**
  - **CMMC Level 1:**
    - Fully implement all CMMC Level 1 security requirements to be considered MET.
    - No POA&M permitted; self-assessment results are MET or NOT MET.
  - **CMMC Level 2:**
    - Maximum score equals the total number of CMMC Level 2 security requirements.
    - Subtract points for each NOT MET requirement, which may result in a negative score.

CMMC Level 2 Scoring Methodology for *Basic* Security Requirements		
Value	**Impact**	**Controls**
5	If not implemented, could lead to significant exploitation of the network, or exfiltration of CUI	AC.L2-3.1.1, AC.L2-3.1.2, AT.L2-3.2.1, AT.L2-3.2.2, AU.L2-3.3.1, CM.L2-3.4.1, CM.L2-3.4.2, IA-L2-3.5.1, IA-L2-3.5.2, IR.L2-3.6.1, IR.L2-3.6.2, MA.L2-3.7.2, MP.L2-3.8.3, PS.L2-3.9.2, PE.L2-3.10.1, PE.L2-3.10.2, CA.L2-3.12.1, CA.L2-3.12.3, SC.L2-3.13.1, SC.L2-3.13.2, SI.L2-3.14.1, SI.L2-3.14.2, and SI.L2-3.14.3.
3	If not implemented, has specific and confined effect on the security of the network and its data.	AU.L2-3.3.2, MA.L2-3.7.1, MP.L2-3.8.1, MP.L2-3.8.2, PS.L2-3.9.1, RA.L2-3.11.1, and CA.L2-3.12.2.

CMMC Level 2 Scoring Methodology for *Derived* Security Requirements		
Value	**Impact**	**Controls**
5	If not implemented, could lead to significant exploitation of the network, or exfiltration of CUI.	AC.L2-3.1.12, AC.L2-3.1.13, AC.L2-3.1.16, AC.L23.1.17, AC.L2-3.1.18, AU.L2-3.3.5, CM.L2-3.4.5, CM.L2-3.4.6, CM.L2-3.4.7, CM.L2-3.4.8, IA.L2-3.5.10, MA.L2-3.7.5, MP.L2-3.8.7, RA.L2-3.11.2, SC.L2-3.13.5, SC.L2-3.13.6, SC.L2-3.13.15, SI.L2-3.14.4, and SI.L2-3.14.6.
3 or 5	If not completely or properly implemented, could be partially effective and points adjusted depending on how the security requirement is implemented. • Partially effective implementation - 3 points • Non-effective (not implemented at all) - 5 points	IA.L2-3.5.3, SC.L2-3.13.11
3	If not implemented, has specific and confined effect on the security of the network and its data.	AC.L2-3.1.5, AC.L2- 3.1.19, MA.L2-3.7.4, MP.L2-3.8.8, SC.L2-3.13.8, SI.L2- 3.14.5, and SI.L2-3.14.7.

1	If not implemented, has a limited or indirect effect on the security of the network and its data.	Deduct 1 point for all other Derived Security Requirements.

- **CMMC Level 3 Assessment Scoring:**
  - All CMMC Level 3 security requirements have a value of "1" point each.
  - The score is equivalent to the total number of CMMC Level 3 security requirements, reduced by one point for each NOT MET requirement.
  - CMMC Level 2 assessment score is a prerequisite for a CMMC Level 3 Certification Assessment.

Are There Any Annual Requirements?

Section 170.22 Affirmation

A contractor senior official must annually affirm continuing compliance with all CMMC levels following the requirements outlined in Section 170.22.

Summary of § 170.22 Affirmation for DoD Contractors:

1. **Affirmation Requirements:**
   - The Organization Seeking Assessment (OSA) must affirm continuing compliance with the appropriate level of CMMC Self-Assessment or CMMC Certification Assessment.
2. **Affirming Official:**
   - Affirmations must be submitted by the OSA senior official responsible for ensuring OSA compliance with CMMC Program requirements.
3. **Affirmation Content:**
   - Each affirmation must include the following information:
     - Name, title, and contact information for the affirming official.
     - Affirmation statement attesting that the OSA has implemented and will maintain implementation of all applicable CMMC security requirements for all information systems within the relevant CMMC Assessment Scope at the applicable CMMC Level.
4. **Affirmation Submission Instances:**
   - Affirmations must be submitted in the following instances:
     - Upon completion of the assessment (conditional or final).
     - Annually thereafter.
     - Following a POA&M closeout assessment, as applicable.
5. **Submission Procedures:**
   - All affirmations must be completed in the SPRS.
   - The Department will verify submission of the affirmation in SPRS to ensure compliance with CMMC solicitation or contract requirements.
6. **CMMC Level 1 Self-Assessment Affirmation:**
   - At the completion of a self-assessment and annually thereafter, the affirming official must submit a CMMC affirmation attesting to continuing compliance with all CMMC Level 1 security requirements.
7. **CMMC Level 2 Self-Assessment Affirmation:**
   - At the completion of a self-assessment and annually thereafter, the affirming official must submit a CMMC affirmation attesting to continuing compliance with all CMMC Level 2 security requirements.
   - An affirmation is also required at the completion of a POA&M Closeout assessment.
8. **CMMC Level 2 Certification Assessment Affirmation:**

- At the completion of a C3PAO assessment and annually thereafter, the affirming official must submit a CMMC affirmation attesting to continuing compliance with all CMMC Level 2 security requirements.
- An affirmation is also required at the completion of a POA&M Closeout assessment.

9. **CMMC Level 3 Certification Assessment Affirmation:**
    - At the completion of a Defense Contract Management Agency (DCMA) DIBCAC assessment and annually thereafter, the affirming official must submit a CMMC affirmation attesting to continuing compliance with all CMMC Level 3 security requirements. This is in addition to the ongoing requirement for Level 2 affirmation.
    - An affirmation is also required at the completion of a POA&M Closeout assessment.

Conclusion:

In conclusion, navigating the intricacies of the CMMC 2.0 Program is vital for DoD contractors as it impacts all levels of the supply chain. Key takeaways include the broad applicability of the program, phased implementation, and the specific requirements for different CMMC levels. It's crucial for contractors to understand the assessment types, ranging from self-assessments to certification assessments, and the corresponding obligations at each phase.

To prepare for CMMC certification, contractors should align their strategic planning with the phased approach outlined in the program. Cybersecurity maturity levels, self-assessment requirements, and certification assessments vary across the phases. Contractors must be diligent in adhering to the specific requirements for each level to ensure compliance with the CMMC 2.0 Program.

Encouraging Action:

Given the complexity of the CMMC 2.0 Program, we encourage DoD contractors to take proactive steps to understand, assess, and implement the necessary controls for compliance. CyberNINES is committed to assisting contractors in preparing for CMMC certification. Our expertise lies in designing environments and implementing the NIST SP 800-171 control requirements to ensure a smooth audit process. For any questions or assistance with CMMC certification preparation, we invite readers to reach out to CyberNINES for comprehensive support.

By partnering with CyberNINES, contractors can navigate the CMMC landscape with confidence, ensuring that their information systems meet the stringent security requirements set forth by the Department of Defense. Don't hesitate to contact us for personalized guidance tailored to your specific needs.

Contact Information:
Email: inquiry@cybernines.com
Phone: 608.512.1010
Website: https://cybernines.com/