



## CHIEF INFORMATION OFFICER



(<https://dodcio.defense.gov/>)

## **Phased Implementation of CMMC Requirements Has Begun!**

CMMC Phase 1 Implementation (Nov 10, 2025 - Nov 9, 2026) to focus primarily on CMMC  
Level 1 and Level 2 self-assessments

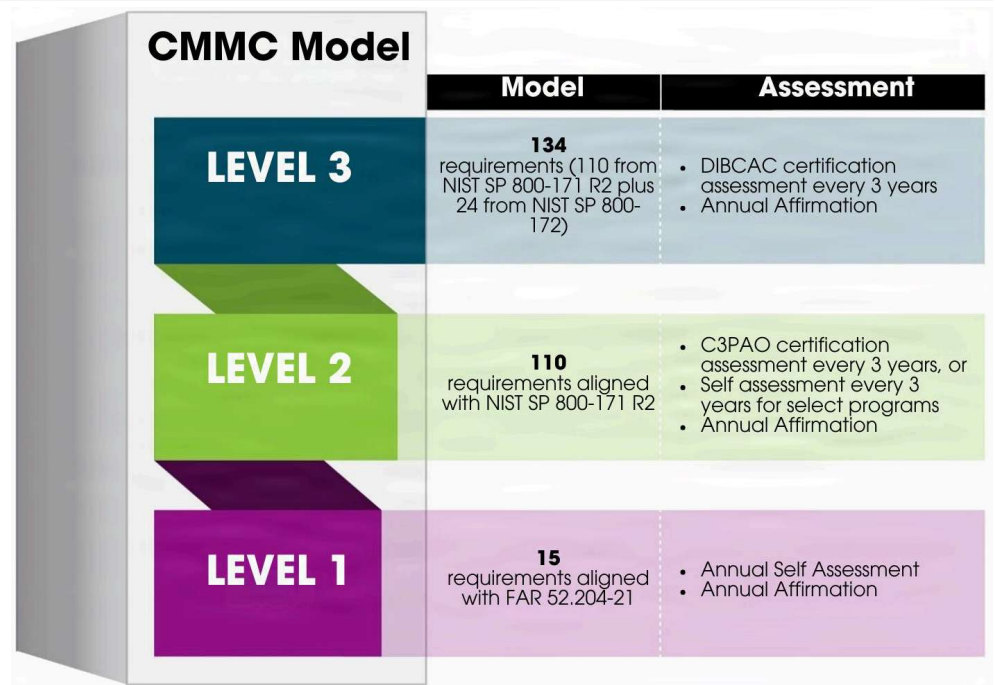
**\*\*Reminder to submit AFFIRMATIONS with your CMMC assessments in SPRS\*\***

## **ABOUT CMMC**

---

Cybersecurity is a top priority for the Department of War (DoW or Department). The defense industrial base (DIB) faces increasingly frequent and complex cyber-attacks. To strengthen DIB cybersecurity and better protect DoW information, the Department developed the Cybersecurity Maturity Model Certification (CMMC) Program (<https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program>). CMMC assesses defense contractor compliance with existing information safeguarding requirements for federal contract information (FCI) and controlled unclassified information (CUI).

## Overview of the CMMC Program



(<https://d34w7g4gy10iej.cloudfront.net/graphics/2512/39613.png>)

The CMMC Program aligns with the Department's existing information safeguarding requirements for the DIB. The program provides the DoW with increased assurance that prospective contractors and subcontractors have implemented contractually required cybersecurity standards for nonfederal information systems that will process, store, or transmit FCI or CUI during contract performance.

Key features of the CMMC Program:

- **Tiered Model:** CMMC assesses compliance with cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the FCI or CUI. The program also outlines protection requirements for information flowed down to subcontractors.
- **Assessment Requirement:** CMMC assessments allow the Department to verify DIB implementation of foundational cybersecurity standards.
- **Implementation through Contracts:** DoW contractors and subcontractors entrusted with FCI or CUI must achieve a specific CMMC level as a condition of contract award.

## Protected Information

The CMMC model is designed to enforce the protection of FCI and CUI.

- **Federal Contract Information (FCI):** As defined in section 4.1901 of the Federal Acquisition Regulation (FAR), FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, excluding information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments."
- **Controlled Unclassified Information (CUI):** As outlined in Title 32 CFR 2002.4(h), CUI is "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls." For more information regarding specific CUI categories and subcategories, see the DoW CUI Registry website.

[Skip to main content \(Press Enter\).](#)

## Overview of Assessments

The CMMC Program provides assessments at three levels, each incorporating security requirements from existing regulations and guidelines.

### Level 1: Basic Safeguarding of FCI

- **Requirements:** Annual self-assessment and annual affirmation of compliance with the 15 security requirements in FAR clause 52.204-21.

### Level 2: Broad Protection of CUI

- **Requirements:**
  1. Either a self-assessment or an independent assessment by an authorized CMMC Third-Party Assessment Organization (C3PAO) every three years, as specified in the solicitation.
    - Decided by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems.
  2. Annual affirmation, verify compliance with the 110 security requirements in NIST SP 800-171 Revision 2.

### Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats

- **Requirements:**
  1. Achieve CMMC Status of Final Level 2.
  2. Undergo an assessment every three years by the Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).
  3. Provide an annual affirmation verifying compliance with the 24 identified requirements from NIST SP 800-172.

| CMMC Status                         | Source & Number of Security Reqts.                                                                             | Assessment Reqts.                                                                                                                                                                                                        | Plan of Action & Milestones (POA&M) Reqts.                                                                                                                                                                                             | Affirmation Reqts.                                                                                                                                                                          |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Level 1 (Self)                      | <ul style="list-style-type: none"><li>• 15 required by FAR clause 52.204-21</li></ul>                          | <ul style="list-style-type: none"><li>• Conducted by Organization Seeking Assessment (OSA) annually</li><li>• Results entered into the Supplier Performance Risk System (SPRS)</li></ul>                                 | <ul style="list-style-type: none"><li>• Not permitted</li></ul>                                                                                                                                                                        | <ul style="list-style-type: none"><li>• After each assessment</li><li>• Entered into SPRS</li></ul>                                                                                         |
| Level 2 (Self)                      | <ul style="list-style-type: none"><li>• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012</li></ul> | <ul style="list-style-type: none"><li>• Conducted by OSA every 3 years</li><li>• Results entered into SPRS</li><li>• CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4</li></ul> | <ul style="list-style-type: none"><li>• Permitted as defined in 32 CFR § 170.21(a)(2) and must be closed out within 180 days</li><li>• Final CMMC Status will be valid for three years from the Conditional CMMC Status Date</li></ul> | <ul style="list-style-type: none"><li>• After each assessment and annually thereafter</li><li>• Assessment will lapse upon failure to annually affirm</li><li>• Entered into SPRS</li></ul> |
| Skip to main content (Press Enter). |                                                                                                                | <ul style="list-style-type: none"><li>• Conducted by C3PAO every 3 years</li></ul>                                                                                                                                       |                                                                                                                                                                                                                                        |                                                                                                                                                                                             |

|                             |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                            |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Level 2<br/>(C3PAO)</b>  | <ul style="list-style-type: none"> <li>110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012</li> </ul>                                                                                                    | <ul style="list-style-type: none"> <li>Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS)</li> <li>CMMC Status will be valid for three years from the CMMC Status Date as defined in 32 CFR § 170.4</li> </ul> | <ul style="list-style-type: none"> <li>Permitted as defined in 32 CFR § 170.21(a)(2) and must be closed out within 180 days</li> <li>Final CMMC Status will be valid for three years from the Conditional CMMC Status Date</li> </ul> | <ul style="list-style-type: none"> <li>After each assessment and annually thereafter</li> <li>Assessment will lapse upon failure to annually affirm</li> <li>Entered into SPRS</li> </ul>                                                                                  |
|                             |                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment</li> </ul>                                                               |                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                            |
| <b>Level 3<br/>(DIBCAC)</b> | <ul style="list-style-type: none"> <li>110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012</li> <li>24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to 32 CFR § 170.14(c)(4)</li> </ul> | <ul style="list-style-type: none"> <li>Conducted by DIBCAC every 3 years</li> <li>Results entered into CMMC eMASS</li> <li>CMMC Status will be valid for three years from the CMMC Status Date as defined in 32 CFR § 170.4</li> </ul>     | <ul style="list-style-type: none"> <li>Permitted as defined in 32 CFR § 170.21(a)(3) and must be closed out within 180 days</li> <li>Final CMMC Status will be valid for three years from the Conditional CMMC Status Date</li> </ul> | <ul style="list-style-type: none"> <li>After each assessment and annually thereafter</li> <li>Assessment will lapse upon failure to annually affirm</li> <li>Level 2 (C3PAO) affirmation must also continue to be completed annually</li> <li>Entered into SPRS</li> </ul> |

### CMMC Post-Assessment Remediation: Plans of Actions and Milestones

The CMMC Program allows limited use of Plans of Action and Milestones (POA&Ms).

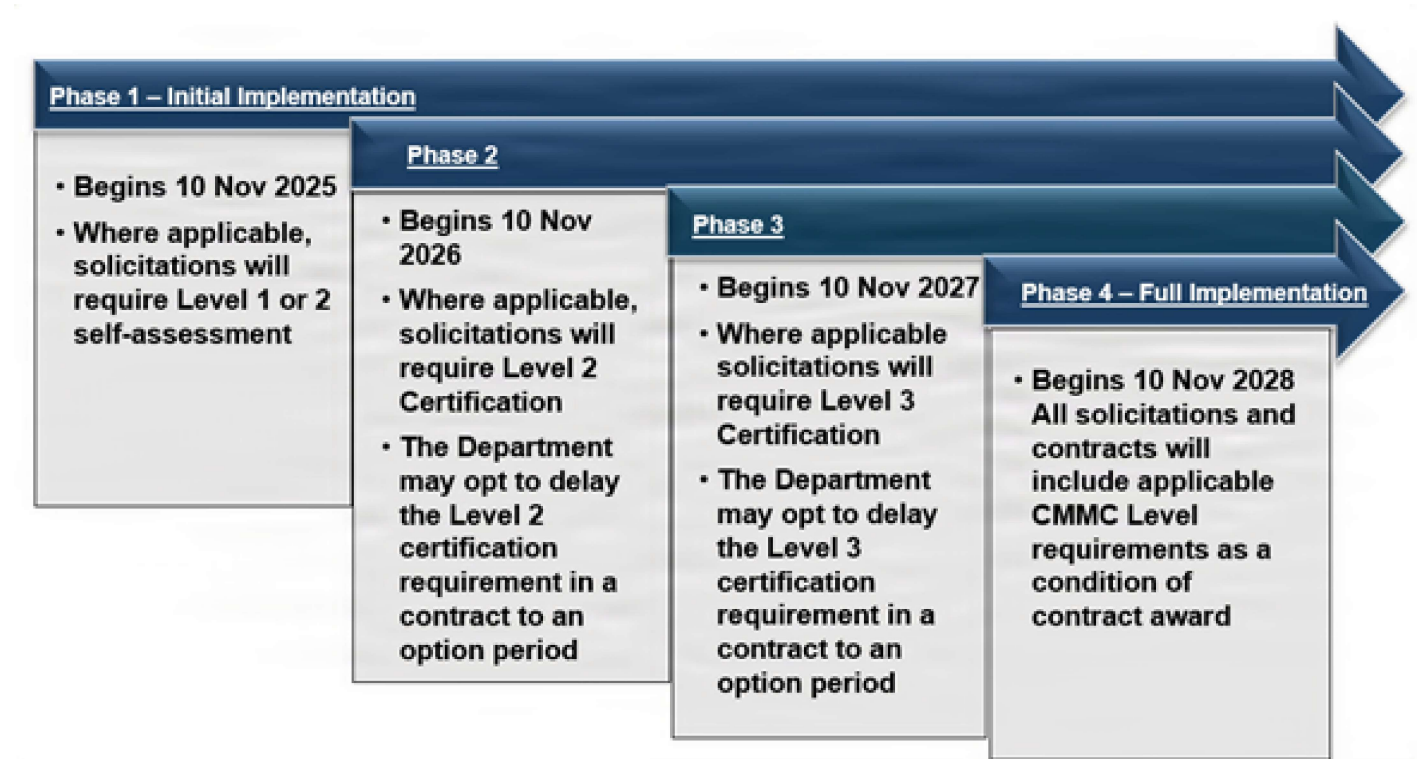
- Level 1:** POA&Ms are not permitted.
- Level 2 and Level 3:** Refer to §170.21 of the 32 CFR CMMC Program final rule for POA&M requirements, including critical requirements that cannot be included in a POA&M.

A POA&M closeout assessment is a CMMC assessment that evaluates only the NOT MET requirements identified in the initial assessment. The closing of a POA&M must be confirmed by a POA&M closeout assessment within 180 days of the Conditional CMMC Status Date. If the POA&M is not successfully closed out within this timeframe, the Conditional CMMC Status for the information system will expire.

- Level 2 Self-Assessment:** The POA&M closeout self-assessment shall be performed by the OSA in the same manner as the initial self-assessment.
- Level 2 Certification Assessment:** The POA&M closeout certification assessment must be performed by an authorized or accredited C3PAO.
- Level 3 Certification Assessment:** The POA&M closeout certification assessment will be performed by DCMA DIBCAC.

## CMMC Implementation

The first phase of CMMC implementation began on **November 10, 2025**. CMMC assessment requirements will be implemented using a four-phase plan over three years. The phases add CMMC Level requirements incrementally, starting with self-assessments in Phase 1, and ending with full implementation of program requirements in Phase 4. This phased approach allows time to train assessors and for companies to understand and implement CMMC assessment requirements.



**DoW may implement CMMC Level 2 (C3PAO) requirements in some Phase 1 procurements or Level 3 requirements in some Phase 2 procurements, which may limit competitors or drive cost**

|                                                                                                                                                                                           |                                                                                                                         |                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>About DoW CIO (/About-DoW-CIO/)</b>                                                                                                                                                    | <b>No FEAR Act</b><br>( <a href="https://prhome.war.gov/NoFear/">https://prhome.war.gov/NoFear/</a> )                   | <b>Public Use Notice</b><br>( <a href="#">/PublicUseNotice/</a> )                             |
| <b>Contact Us (/Contact/)</b>                                                                                                                                                             | <b>Open Government</b><br>( <a href="https://open.defense.gov">https://open.defense.gov</a> )                           | <b>Section 508 (/508/)</b>                                                                    |
| <b>War.gov</b><br>( <a href="https://www.war.gov">https://www.war.gov</a> )                                                                                                               | <b>Plain Writing</b><br>( <a href="http://www.esd.whs.mil/DD/plainwriting">http://www.esd.whs.mil/DD/plainwriting</a> ) | <b>Site Map (/DevSiteMap/)</b><br><b>Social Media (/Social-Media/)</b>                        |
| <b>DoW Careers</b><br>( <a href="https://www.dodciviliancareers.com/">https://www.dodciviliancareers.com/</a> )                                                                           | <b>Privacy Impact Assessments (/PIA/)</b>                                                                               | <b>Strategic Plan</b><br>( <a href="#">/Portals/0/Documents/Library/FulcrumAdvStrat.pdf</a> ) |
| <b>External Links Disclaimer</b><br>( <a href="#">/ELD/</a> )                                                                                                                             | <b>Privacy Policy (/Privacy-Policy/)</b>                                                                                | <b>USA.gov</b><br>( <a href="https://www.usa.gov/">https://www.usa.gov/</a> )                 |
| <b>FOIA</b><br>( <a href="https://open.defense.gov/Transparency/FOIA.aspx">https://open.defense.gov/Transparency/FOIA.aspx</a> )                                                          | <b>Privacy Program</b><br>( <a href="https://open.defense.gov/Privacy.aspx">https://open.defense.gov/Privacy.aspx</a> ) | <b>Web Policy (/DoD-Web-Policy/)</b>                                                          |
| <b>Information Quality</b><br>( <a href="https://dod.defense.gov/Resources/DoD-Information-Quality-Guidelines">https://dod.defense.gov/Resources/DoD-Information-Quality-Guidelines</a> ) |                                                                                                                         |                                                                                               |

## STAY CONNECTED



(https://www.scribd.com/document/44916042/Py-actv-cio)

Hosted by Department of War Information Activity - WEB.mil (<https://www.web.dma.mil/>)



(<https://www.veteranscrisisline.net/get-help-now/military-crisis-line/>)