

DEFENSE LOGISTICS AGENCY

Established 1961



Cybersecurity Maturity Model Certification (CMMC)

Brooke Taylor Wunderly, DLA Senior Procurement Analyst

October 2025



THE NATION'S LOGISTICS COMBAT SUPPORT AGENCY

November 2025: CMMC Overview



Purpose:

Provide an overview of CMMC to DLA Contractors.

Agenda:

- CMMC Overview
- Q&A During Presentation

Information
 Guidance
 Decision
 Other

The overall classification of this presentation is:
Cleared for Open Publication



- Title 48 refers to the Federal Acquisition Regulations (FAR), and agency-specific supplements like DFARS, which govern how the federal government purchases goods and services in the United States.
- It includes regulations related to the CMMC program for cybersecurity compliance in DoD contracts. It encompasses the rules published in the Federal Register by various government departments and agencies.
- DFARS rule published September 10, 2025: “Assessing Contractor Implementation of Cybersecurity Requirements”.
 - Applies to contractors handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
 - Introduces pre-award assessment protocols for NIST SP 800-171 compliance.

**What:**

A consistent pre-award assessment methodology to determine whether a prospective contractor has implemented cybersecurity protections necessary to adequately safeguard DoD information.

Why:

To increase the cybersecurity posture of the DIB and better protect sensitive unclassified information.

How:

All defense contractors and subcontractors will show compliance with applicable security requirements through self-assessment or independent assessment, prior to contract award (excluding Commercial-Off-The-Shelf procurements).

When:

Effective November 10, 2025, with three-year phase-in





Phased Implementation of CMMC Requirements

Phase 1 – Initial Implementation

- Begins at 48 CFR Rule Effective Date, 10 Nov 25
- Where applicable, solicitations will require Level 1 (Federal Contract Information (FCI)) or 2 Self-Assessment (Controlled Unclassified Information (CUI))

Phase 2

- Begins 12 months after Phase 1 start, 10 Nov 26
- Where applicable, solicitations will require Level 2 Certification (CUI)

Phase 3

- Begins 24 months after Phase 1 start, 10 Nov 27
- Where applicable solicitations will require Level 3 Certification (CUI)

Phase 4 – Full Implementation

- Begins 36 months after Phase 1 start, 10 Nov 28
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

CMMC Framework Requirements



CMMC Model	Model	Assessment
<p>LEVEL 3</p>	<p>134 requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)</p>	<ul style="list-style-type: none"> • DIBCAC assessment every 3 years • Annual Affirmation
<p>LEVEL 2</p>	<p>110 requirements aligned with NIST SP 800-171 r2</p>	<ul style="list-style-type: none"> • C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs. • Annual Affirmation
<p>LEVEL 1</p>	<p>15 requirements aligned with FAR 52.204-21</p>	<ul style="list-style-type: none"> • Annual self-assessment • Annual Affirmation

When specified in a solicitation, all CMMC requirements must be met prior to award



- Two types of CMMC approvals:
 - **Conditional-** Initial assessment with passing score of 88 with Plan of Action and Milestones (POA&M) to achieve Final approval.
 - **Final-** Assessment with a passing score with no POA&M, or when the POA&M has been closed out within 180 days of achieving a Conditional approval.
- In DFARS, Final and Conditional approval permitted for CMMC Level 2 and CMMC Level 3 (does not apply to CMMC Level 1).



- DFARS clause 252.204-7021
 - Relies on the requiring activity to identify the appropriate CMMC requirements based on the type of information to be processed, stored, or transmitted.
 - Applicable to new solicitations, contracts, task orders, delivery orders, modifications, and options that contain FCI or CUI.
 - Requires the contractor/subcontractor to:
 - Develop and update Artifacts and Deliverables per RFI/RFP
 - Conduct Self-Assessment or request a C3PAO or DIBCAC to perform a CMMC Certification Assessment, depending on the sensitivity of the data on the contractor's or subcontractor's information system
 - Complete annual affirmation of continued compliance in SPRS
 - Flow-down the DFARS clause 252.204-7021 to subcontractors



- Please refer to the **official DoD CMMC Program website**, including the FAQ page, for more information about CMMC: <https://dodcio.defense.gov/CMMC/>
- **Small Business Project Spectrum**: <https://www.projectspectrum.io/#/>
- **DLA Small Business Cyber Resources**: <https://www.dla.mil/Small-Business/Resources/Cybersecurity-Resources/#cmmccert>
- **DoD no-cost cybersecurity compliance resources** can be found at dibnet.dod.mil under *DoD DIB Cybersecurity-As-A Service (CSaaS) Services and Support*.
- **Additional cybersecurity resources** can be found at:
 - <https://www.cisa.gov/shields-up>
 - <https://www.nist.gov/mep>
 - <https://www.apexaccelerators.us/#/>
- To **locate a C3PAO**, visit the CMMC Accreditation Body Marketplace at cyberab.org.
- To **obtain additional information on CMMC Assessments, Scoping, and Hashing**, visit: <https://dodcio.defense.gov/cmmc/Resources-Documentation/>
- The Department's **CUI Quick Reference Guide** includes information on the marking and handling of CUI: <https://www.dodcui.mil/>
- To find a **FedRAMP Moderate Authorized Service Provider**, please visit: <https://marketplace.fedramp.gov/assessors>



