SmartSuite

Framework / Cybersecurity / CMMC

CMMC 2.0 – Level 1 / Level 2 / Level 3

CMMC is the DoD program, 32 CFR Part 170, that requires contractors handling FCI or CUI to hold a Level 1, 2 or 3 status. Phase 2 was suspended on July 13, 2026.



What it is

The Cybersecurity Maturity Model Certification (CMMC) Program is the U.S. Department of Defense (DoD) rule, 32 CFR Part 170, that requires contractors and subcontractors handling Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) to hold a CMMC status at the level a contract names. The Part 170 rule took effect on December 16, 2024, and the first contract requirements began on November 10, 2025, when the matching DFARS rule took effect.

At a glance

PUBLISHER
U.S. Department of Defense (DoD)

TYPE
Certification / Assurance Program

VERSION
32 CFR Part 170 (CMMC Program rule); CMMC Model Overview and guides Version 2.13 (September 2024)

EFFECTIVE
December 16, 2024 (32 CFR Part 170); November 10, 2025 (DFARS rule and Phase 1)

DOMAIN
Cybersecurity

FAMILY
CMMC

REGION
United States

INDUSTRY
Aerospace & Defense

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: dowcio.war.gov/CMMC/

Why it matters

- **A status checked before award** The contractor must have, and keep for the life of the contract, a current CMMC status at or above the required level for every system that processes FCI or CUI (DFARS 252.204-7021(d)).
- **Three levels tied to three source documents** Level 1 uses the 15 requirements of FAR 52.204-21, Level 2 the 110 of NIST SP 800-171 Rev. 2, and Level 3 adds 24 selected from NIST SP 800-172 (32 CFR 170.14).
- **Limited remediation windows** A Conditional status allows a plan of action and milestones at Levels 2 and 3, closed out within 180 days. Level 1 allows none (170.21).
- **Supply chain coverage** Primes flow the right level down to every subcontractor that handles FCI or CUI, and subcontractors affirm before award (170.23; DFARS 252.204-7021(d)(4)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CMMC 2.0

Contract Level Register

Record each solicitation and contract with the CMMC level and assessment type it names, the clause 252.204-7021 and provision 252.204-7025 references, and whether you are prime or subcontractor (DFARS 204.7504).

Assessment Scope and Asset Inventory

Keep the Assessment Scope with each asset's category, owner and link to the system security plan and network diagram (32 CFR 170.19).

Status Dates and Affirmations

Track each CMMC Status Date, Conditional or Final status, the 180-day closeout date, the three-year reassessment date and the annual affirmation in SPRS, with automations that notify owners ahead of each date (170.16 to 170.22).

Subcontractor Flow-Down Tracker

Hold each subcontractor's information type (FCI or CUI), the level required under the prime contract and its affirmation before award (170.23; DFARS 252.204-7021(d)(4)).

Suspension and Phase Log

Log each Department of War notice, including the July 13, 2026 suspension, and link it to the solicitations it affects so teams know whether Level 2 (C3PAO) or Level 3 (DIBCAC) can be required.

Program Readiness Reporting

Build a dashboard of contracts by required level, status expiry dates and open plan-of-action items for leadership review.

Common framework mappings

CIS Controls v8.1 | DFARS 252.204-7012 | FedRAMP Rev. 5 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-171 Rev.2 | NIST SP 800-172 | NIST 800-53 Rev.5

Official resources

CMMC Program Status and Announcements

The Department of War CIO's CMMC home page, with the July 2026 Phase II suspension notice and program memos.

dowcio.war.gov/CMMC

CMMC Model Overview, Version 2.13

The CMMC model's three levels, 14 domains and every security requirement by level, from the CMMC program office.

dowcio.war.gov/Portals/0/Documents/CMMC/ModelOverviewv2.pdf

CMMC Program Rule, 32 CFR Part 170 (Federal Register)

The final rule of October 15, 2024 that established the CMMC Program, as published in the Federal Register.

govinfo.gov/content/pkg/FR-2024-10-15/pdf/2024-22905.pdf

Frequently asked questions

Who has to meet CMMC?

Contractors and subcontractors at every tier whose information systems process, store or transmit FCI or CUI under a DoD contract that carries DFARS clause 252.204-7021, except contracts solely for commercially available off-the-shelf items. The program manager picks the level and assessment type for each procurement, and the prime flows the right level down to each subcontractor (32 CFR 170.3 and 170.23; DFARS 204.7504).

What are the CMMC levels and how many requirements does each have?

Level 1 has 15 requirements from FAR 52.204-21 and protects FCI. Level 2 has the 110 requirements of NIST SP 800-171 Rev. 2 and protects CUI. Level 3 adds 24 requirements selected from NIST SP 800-172 for CUI (32 CFR 170.14).

Where does CMMC stand after the July 2026 suspension?

Phase 1 began on November 10, 2025 and its Level 1 and Level 2 self-assessment requirements remain in place. On July 13, 2026 the Department of War suspended the Phase 2 transition planned for November 10, 2026 and began a program review. Program managers may designate only Level 1 (Self) or Level 2 (Self) until further guidance, and DFARS 252.204-7012 still applies.

 · © 2026 SmartSuite Inc. All rights reserved.

Which CMMC statuses are self-assessments and which are certifications?

Level 1 (Self) and Level 2 (Self) are performed by the contractor, with results and an affirmation entered in SPRS. Level 2 (C3PAO) is a certification assessment by an authorized or accredited C3PAO, and Level 3 (DIBCAC) is performed by DCMA DIBCAC after a Final Level 2 (C3PAO) for the same scope (32 CFR 170.15 to 170.18).

How does CMMC relate to DFARS 252.204-7012 and NIST SP 800-171?

DFARS 252.204-7012 requires contractors to protect covered defense information with NIST SP 800-171, and it stays in effect alongside CMMC. Level 2 uses the same 110 requirements of Revision 2, so a CMMC status verifies what the clause already requires. The July 2026 suspension did not remove the clause (32 CFR 170.14(c)(3)).

License included / downloadable: Yes The CMMC rule, model overview and assessment guides are public documents published by the U.S. Department of Defense and are free to read on its CMMC site and in the Federal Register.

Full framework page and mappings: smartsuite.com/frameworks/cmmc-2-0-cybersecurity-maturity-model-certification