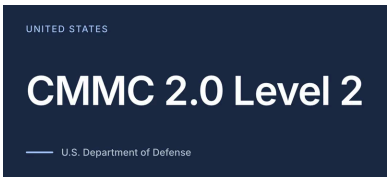
SmartSuite

Framework / Cybersecurity / CMMC

CMMC 2.0 – Level 2

CMMC Level 2 requires contractors handling CUI to meet all 110 NIST SP 800-171 Rev. 2 requirements, shown by a Level 2 (Self) or Level 2 (C3PAO) assessment under 32 CFR 170.



What it is

CMMC Level 2 is the scored level of the CMMC Program for contractors that handle Controlled Unclassified Information (CUI): it requires all 110 security requirements of NIST SP 800-171 Revision 2, proven by a Level 2 (Self) self-assessment or a Level 2 (C3PAO) certification assessment, whichever the contract names (32 CFR 170.14(c)(3), 170.16 and 170.17). The CMMC rule took effect on December 16, 2024, and Level 2 (Self) requirements began to appear in DoD solicitations on November 10, 2025.

At a glance

PUBLISHER
U.S. Department of Defense (DoD)

TYPE
Certification / Assurance Program

VERSION
Level 2: 110 requirements of NIST SP 800-171 Rev. 2 (32 CFR 170.14(c)(3)); CMMC Assessment Guide Level 2 Version 2.13 (September 2024)

EFFECTIVE
December 16, 2024 (32 CFR Part 170); November 10, 2025 (DFARS rule; Level 2 (Self) from Phase 1)

DOMAIN
Cybersecurity

FAMILY
CMMC

REGION
United States

INDUSTRY
Aerospace & Defense

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: dowcio.war.gov/CMMC/About/

Why it matters

- **Contract eligibility** Before award the offeror must hold a Conditional or Final Level 2 (Self) or (C3PAO) status, as the solicitation requires, and have submitted an affirmation in SPRS (170.16(b), 170.17(b)).
- **A threshold with limits** A Conditional status needs at least 80 percent of 110 points, which is 88, and a plan of action restricted to one-point requirements, with one three-point exception (170.21(a)(2)).
- **Three-year validity** A Final Level 2 status is valid for three years from the CMMC Status Date, with an annual affirmation (170.16, 170.17, 170.22).
- **Reuse of earlier DIBCAC work** A perfect-score DCMA DIBCAC High Assessment with no open plan of action, finished before December 16, 2024, counts as Final Level 2 (C3PAO) for three years from that assessment (170.20).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CMMC 2.0 L2

Assessment Scope Register

List each asset by category (CUI, Security Protection, Contractor Risk Managed, Specialized or Out-of-Scope) with its owner and links to the inventory and network diagram (32 CFR 170.19(c)).

110-Requirement Library

Hold each NIST SP 800-171 Rev. 2 requirement as a record with owner, implementation status, assessment objectives and evidence (170.14(c)(3)).

Score and POA&M Tracking

Record each requirement's point value and result, list NOT MET items, and test them against the one-point rule and the six excluded requirements before relying on a Conditional status (170.21(a)(2)).

SSP Version History

Keep the System Security Plan name, date and version that a C3PAO enters into eMASS, with the change history that shows what moved between assessments (170.17(a)(1)(i)).

Closeout and Affirmation Calendar

Track the 180-day closeout deadline, the three-year reassessment date and each annual affirmation in SPRS (170.16, 170.22).

Evidence Retention

Attach artifacts to each requirement and keep them available for six years from the CMMC Status Date (170.16(c), 170.17(c)).

Common framework mappings

CIS Controls v8.1 · CMMC 2.0 · CMMC 2.0 Level 3 · ISO 27001:2022 · NIST CSF 2.0 · NIST SP 800-161 Rev.1 · NIST 800-171 Rev.2 · NIST 800-53 Rev.5

Official resources

CMMC Assessment Guide, Level 2 (Version 2.13)

Assessment objectives and evidence guidance for each Level 2 requirement, September 2024.

dowcio.war.gov/Portals/0/Documents/CMMC/AssessmentGuideL2v2.pdf

CMMC Scoping Guide, Level 2 (Version 2.13)

How to define the Level 2 Assessment Scope, including CUI Assets and Security Protection Assets.

dowcio.war.gov/Portals/0/Documents/CMMC/ScopingGuideL2v2.pdf

CMMC Alignment to NIST Standards

DoD briefing on how CMMC Levels 1 to 3 align to NIST SP 800-171 and 800-172, including Level 2 scoring.

dowcio.war.gov/Portals/0/Documents/CMMC/CMMC-AlignmentNIST-Standards.pdf

Frequently asked questions

Is CMMC Level 2 mandatory for DoD contractors?

Only where a DoD contract includes a Level 2 requirement. The program manager sets Level 2 (Self) or Level 2 (C3PAO) for the procurement based on whether CUI will be handled. Since July 13, 2026 only Level 2 (Self) may be designated while the Phase 2 suspension lasts (32 CFR 170.3(d); Department of War CMMC procedures notice).

What score does Level 2 require?

A Final status needs every one of the 110 requirements MET. A Conditional status needs at least 80 percent of the 110 points, which is 88, with open items limited to one-point requirements and none of six named requirements such as the System Security Plan, closed within 180 days (170.16, 170.21, 170.24).

What is the difference between Level 2 (Self) and Level 2 (C3PAO)?

The requirements are identical. In a Level 2 (Self) the contractor assesses itself and posts the score to SPRS. In a Level 2 (C3PAO) an authorized or accredited C3PAO performs the assessment and posts results to eMASS, and the contractor receives a Certificate of CMMC Status (170.16, 170.17).

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

How long does a Level 2 status last?

A Final Level 2 status is current for three years from the CMMC Status Date, as long as an Affirming Official affirms compliance every year. A Conditional status expires after 180 days unless the plan of action is closed out. Assessment artifacts are kept for six years (170.16, 170.17, 170.22; DFARS 252.204-7021).

Can a cloud provider store CUI for a Level 2 assessment?

Only if it meets the FedRAMP requirements in DFARS 252.204-7012. DoD's CMMC FAQ (Revision 2.4, E-A1) says the provider must be FedRAMP Moderate authorized or meet the equivalency set in the Department's December 2023 FedRAMP Moderate equivalency memo. The provider's services then sit in the contractor's assessment scope (170.19(c)(2)).

License included / downloadable: Yes The CMMC Level 2 requirements, assessment guide and scoping guide are public documents published by the U.S. Department of Defense, and NIST SP 800-171 is free from NIST.

Full framework page and mappings: smartsuite.com/frameworks/cmmc-2-0-l2