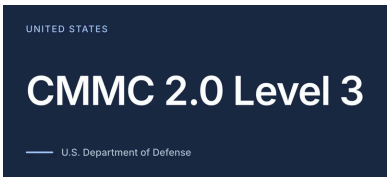
SmartSuite

Framework / Cybersecurity / CMMC

CMMC 2.0 – Level 3 (Expert)

CMMC Level 3 adds 24 NIST SP 800-172 requirements on top of Level 2 and is assessed only by DCMA DIBCAC. The July 2026 suspension bars designating it for now.



What it is

CMMC Level 3 is the highest level of the CMMC Program: it requires a contractor that already holds a Final Level 2 (C3PAO) status to meet 24 enhanced security requirements selected from NIST SP 800-172 (February 2021), and the Defense Contract Management Agency's DIBCAC performs the certification assessment itself (32 CFR 170.14(c)(4) and 170.18). The Part 170 rule took effect on December 16, 2024, and Level 3 could first appear in solicitations in Phase 2, planned for November 10, 2026.

At a glance

PUBLISHER
U.S. Department of Defense (DoD)

TYPE
Certification / Assurance Program

VERSION
Level 3: 24 requirements selected from NIST SP 800-172 (Feb 2021), 32 CFR 170.14(c)(4); CMMC Assessment Guide Level 3 Version 2.13 (September 2024)

EFFECTIVE
December 16, 2024 (32 CFR Part 170); Level 3 contract use planned from Phase 2 (November 10, 2026), suspended July 13, 2026

DOMAIN
Cybersecurity

FAMILY
CMMC

REGION
United States

INDUSTRY
Aerospace & Defense

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Very High

Source: dowcio.war.gov/Portals/0/Documents/CMMC/AssessmentGuideL3.pdf

Why it matters

- **Advanced persistent threat focus** The 24 requirements add a security operations center that runs 24/7, an incident response team deployable within 24 hours, threat hunting and threat-informed risk assessment (IR.L3-3.6.1e, IR.L3-3.6.2e, RA.L3-3.11.2e, RA.L3-3.11.1e).
- **Government-performed assessment** DCMA DIBCAC, not a commercial C3PAO, assesses Level 3 and issues the Certificate of CMMC Status (170.7, 170.18).
- **Level 2 as the foundation** A Final Level 2 (C3PAO) status for the same scope comes first, open Level 2 plan-of-action items must be closed, and Level 3 scoring assumes every Level 2 requirement is already MET (170.18(a), 170.19(e), 170.24(c)(3)).
- **Re-evaluation and appeal** A NOT MET requirement can be re-evaluated for 10 business days after the active assessment if new evidence exists, and an outcome can be appealed to DCMA DIBCAC within 21 days (170.18(c)(2), 170.7(b)).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CMMC 2.0 Level 3

Level 2 Prerequisite Tracker

Record the Final Level 2 (C3PAO) status, its assessment identifier, closed plan-of-action items and the scope that the Level 3 scope must sit inside (32 CFR 170.18(c)(1), 170.19(e)).

24-Requirement Library

Hold each DD.L3-3.x.xe requirement with its DoD parameters, owner, implementation status and evidence (170.14(c)(4)).

SOC and Incident Team Evidence

Attach rosters, on-call schedules and exercise records for IR.L3-3.6.1e and IR.L3-3.6.2e, two of the seven requirements that cannot be placed on a plan of action (170.21(a)(3)).

Annual Testing and Review Calendar

Schedule penetration tests (CA.L3-3.12.1e), security solution reviews (RA.L3-3.11.5e) and supply chain plan updates (RA.L3-3.11.7e), each due at least annually.

Supplier and Cloud Responsibility Matrix

Record each external service provider, its Customer Responsibility Matrix and which of the 24 requirements it inherits, with Third Party Risk Management records for the supplier (170.19(d)(2), 170.18(c)).

Assessment, Closeout and Affirmation Dates

Track the DIBCAC request, the 10-business-day re-evaluation window, the 21-day appeal period, the 180-day closeout, the three-year cycle and both annual affirmations (170.18, 170.22, 170.7(b)).

Common framework mappings

CIS Controls v8.1 | CMMC 2.0 | CMMC 2.0 L2 | 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 3 (Version 2.13)

Assessment objectives for each of the 24 Level 3 requirements, as used by DCMA DIBCAC, September 2024.

dowcio.war.gov/Portals/0/Documents/CMMC/AssessmentGuideL3.pdf

CMMC Scoping Guide, Level 3 (Version 2.13)

How to define the Level 3 Assessment Scope within a Level 2 scope, September 2024.

dowcio.war.gov/Portals/0/Documents/CMMC/ScopingGuideL3.pdf

CMMC Model Overview, Version 2.13

The CMMC model's levels, domains and requirement statements, including the Level 3 list, from the CMMC program office.

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

NIST SP 800-172: Enhanced Security Requirements for Protecting CUI

The NIST supplement to SP 800-171 from which the 24 Level 3 requirements are selected.

csrc.nist.gov/pubs/sp/800/172/final

Frequently asked questions

Who assesses CMMC Level 3?

Only DCMA DIBCAC, on behalf of the DoD. The organization emails a request that cites its Level 2 certification assessment identifier, DIBCAC validates the Level 2 (C3PAO) status and schedules the assessment, and DIBCAC issues the Certificate of CMMC Status (32 CFR 170.7 and 170.18(c)).

What must be in place before a Level 3 assessment?

A Final Level 2 (C3PAO) status for the information systems in the Level 3 scope, with the Level 3 scope equal to or inside the Level 2 scope. Any Level 2 plan-of-action items must be closed before the Level 3 assessment starts (170.18(a), 170.19(e)).

How many requirements does Level 3 have and where do they come from?

Level 3 has 24 requirements selected from NIST SP 800-172 (February 2021), with DoD-defined parameters, in ten domains. Examples are a 24/7 security operations center (IR.L3-3.6.1e), an incident response team deployable within 24 hours (IR.L3-3.6.2e) and annual penetration testing (CA.L3-3.12.1e) (170.14(c)(4)).

Can any Level 3 requirement go on a plan of action?

Some can. A Conditional Level 3 status needs at least 80 percent of the 24 requirements MET and no plan of action for IR.L3-3.6.1e, IR.L3-3.6.2e, RA.L3-3.11.1e, RA.L3-3.11.4e, RA.L3-3.11.6e, RA.L3-3.11.7e or SI.L3-3.14.3e. DIBCAC closes out the plan within 180 days or the status expires (170.21(a)(3), 170.18(a)(1)(ii)).

Is Level 3 required now?

No contract can designate it at present. Part 170 allows Level 3 from Phase 2, planned for November 10, 2026, but on July 13, 2026 the Department of War suspended that transition and told program managers not to designate Level 2 (C3PAO) or Level 3 (DIBCAC) during its review. Existing Level 3 requirements are to be removed by amendment or modification (170.3(e); Department of War CMMC procedures notice).

License included / downloadable: Yes The CMMC Level 3 requirements, assessment guide and scoping guide are public documents published by the U.S. Department of Defense, and NIST SP 800-172 is free from NIST.

Full framework page and mappings: smartsuite.com/frameworks/cmmc-2-0-level-3

© 2026 SmartSuite Inc. All rights reserved.