CMMC 2.0 & NIST SP 800-171.

DFARS has required defense contractors to protect CUI with NIST SP 800-171 since 2017; CMMC adds the proof. The 32 CFR Part 170 program rule took effect December 16, 2024 and the DFARS clause followed on November 10, 2025: **whether the data is FCI or CUI sets the level, and the level sets who must verify it.**

VERIFIES EXISTING RULES | FCI OR CUI SETS THE LEVEL | 110 REQUIREMENTS, REV. 2 | PHASE II SUSPENDED 2026

01 THE MECHANISM

A Verification Layer

DFARS 252.204-7012 has required NIST SP 800-171 on covered systems since December 31, 2017, largely unverified. CMMC adds no safeguards; it makes a self-assessment, C3PAO certificate or government assessment a condition of award. **The controls were owed; CMMC checks them.** [04] [02]

FCI or CUI Sets the Level

Federal Contract Information, not for public release, gets the 15 FAR 52.204-21 safeguards at Level 1. CUI needs the 110 requirements of SP 800-171 Rev. 2 at Level 2; Level 3 adds 24 from SP 800-172. **Scope the data first; the level follows.** [07] [01]

Status Lives in SPRS

Every assessment ends in the Supplier Performance Risk System: a CMMC Status (Conditional or Final), its date, scope, CAGE codes and a CMMC UID. Contracting officers check SPRS before award and each option. **An Affirming Official attests annually.** [01] [05]

02 THE FLOW

How a Contractor Gets There — IMPLEMENT

1. **Scope the boundary:** inventory which systems process, store or transmit FCI or CUI, the security protection assets around them, specialized assets and external service providers; a cloud provider holding covered defense information needs FedRAMP Moderate. [01] [04]
2. **Implement and score:** write the system security plan, meet each requirement against the SP 800-171A objectives and score it: 110 minus 5, 3 or 1 points per unmet item. A POA&M is allowed only at Levels 2 and 3, for one-point items, and only at 80 percent or better. [01]
3. **Assess and affirm:** self-assess (Level 1 yearly, Level 2 every three years) or hire a C3PAO; DCMA DIBCAC assesses Level 3 after a Final Level 2 (C3PAO). Post the result to SPRS, close any POA&M within 180 days, and have the Affirming Official affirm after each assessment and annually. [01]

How the Department Enforces It — AFFIRM

1. **Clause in the contract:** DFARS 252.204-7021 names the required status, Level 1 (Self) through Level 3 (DIBCAC), at award and for the life of the contract; 252.204-7025 gives offerors notice. Contracting officers check SPRS by CMMC UID before award and each option. [05] [03]
2. **Phased rollout:** 32 CFR 170.3 set four one-year phases from November 10, 2025: self-assessments first, Level 2 (C3PAO) as a condition of award from Phase 2, Level 3 in Phase 3, all contracts in Phase 4. Until then program offices pick which contracts carry CMMC. [01] [03]
3. **Suspended, not repealed:** on July 13, 2026 the Department of War suspended the Phase II transition due November 10, 2026 and opened a 60-day reform review. Phase I self-assessments, SPRS scores, affirmations and DFARS 252.204-7012 still apply, enforced against NIST SP 800-171 Rev. 2. [10] [04]

03 SIX ELEMENTS OF THE PROGRAM

ELEMENT	WHAT IT MEANS
Levels	Level 1: FCI, 15 FAR safeguards. Level 2: CUI, the 110 SP 800-171 requirements. Level 3: 24 more from 800-172.
Assessment	Self-assessed at Levels 1 and 2, C3PAO-certified at Level 2, DIBCAC at Level 3; valid three years beyond Level 1.
SPRS	System of record: CMMC Status, status date, scope, CAGE codes and UID, checked by contracting officers at award.
Affirmation	A senior Affirming Official attests in SPRS after every assessment and annually; a status is current only with one.
POA&M	Never at Level 1. At Levels 2 and 3 only at 80 percent or better and for low-weight items, closed within 180 days.
Flowdown	FCI-only subs: Level 1 (Self). CUI subs: Level 2 (Self), or Level 2 (C3PAO) when the prime needs C3PAO or Level 3.

04 FOUR CMMC STATUSES COMPARED

STATUS	THIRD-PARTY ASSESSED?	WHAT IT TAKES
Level 1 (Self)	No	15 FAR 52.204-21 safeguards for FCI, every one MET, no POA&M allowed; self-assess and affirm every year; keep the evidence six years.
Level 2 (Self)	No	110 NIST SP 800-171 Rev. 2 requirements, self-scored; valid three years with annual affirmation; Conditional at 80 percent or better.
Level 2 (C3PAO)	Yes	Same 110 requirements, assessed by an authorized or accredited C3PAO; results flow from eMASS to SPRS; recertify every three years.
Level 3 (DIBCAC)	Yes	Final Level 2 (C3PAO) first, then 24 SP 800-172 requirements assessed by DCMA DIBCAC every three years, with Level 2 kept current too.

CONTINUED ON SHEET 2 →

CMMC 2.0 & NIST SP 800-171. SCOPE · IMPLEMENT · AFFIRM

05 PROGRAM OPERATIONS

Find the CUI before you buy controls. Ask the contracting officer which data is CUI or FCI, mark it, and shrink the enclave that touches it. Security protection assets, specialized assets and external service providers count too, so a provider holding CUI inherits the requirement. [01] [04]

Keep one SSP and one honest score. The system security plan is required and cannot sit on a POA&M. Score against the SP 800-171A objectives, post the Level 2 result to SPRS and refresh it when the system changes; the Basic, Medium and High DoD Assessments of 252.204-7020 run alongside CMMC. [01] [06]

Treat the affirmation as an executive signature. Name the Affirming Official, give them the evidence behind every MET, and calendar the annual affirmation and the 180-day POA&M closeout. Keep artifacts six years from the status date; a lapsed affirmation means the status is not current. [01] [05]

Flow it down and verify it. Before awarding a subcontract involving FCI or CUI, confirm the subcontractor's status in SPRS at the level 32 CFR 170.23 requires (COTS excepted), and keep DFARS 252.204-7012 incident reporting, 72 hours plus 90-day image retention, in every flowdown. [05] [01] [04]

06 CONTROL MAPPING

`DFARS 252.204-7012`

The clause CMMC verifies: implement NIST SP 800-171 on covered contractor systems, report cyber incidents to DIBNet within 72 hours, preserve images for 90 days, hold cloud providers to FedRAMP Moderate or equivalent, and flow it all down. CMMC does not replace it, and the July 2026 suspension left it in force. [04] [10]

`DFARS 252.204-7020 (SPRS)`

Under 252.204-7020 contractors post a NIST SP 800-171 DoD Assessment score, not more than three years old, to SPRS. A Basic assessment is self-generated with Low confidence; Medium and High are government-led. CMMC reuses the scoring method and the system while adding statuses, affirmations and CMMC UIDs. [06] [01]

`NIST SP 800-171 REV. 3`

NIST published Revision 3 on May 14, 2024 with 17 families and organization-defined parameters, and withdrew Revision 2 the same day. CMMC still incorporates Revision 2 in 32 CFR 170.2, and the Department said in July 2026 that Rev. 2 remains the enforced standard; a change would need rulemaking. [09] [01] [10] [02]

`800-53 & DIBCAC HIGH`

SP 800-171 Rev. 2 tailors the moderate baseline of SP 800-53 into 14 families of basic and derived requirements (topic 99 owns 800-53). Under 32 CFR 170.20, a perfect-score DCMA DIBCAC High Assessment with no open POA&M, completed before the rule took effect, counts as Final Level 2 (C3PAO) for three years. [08] [01]

07 WHAT THIS DOES NOT SOLVE

Not New Controls
CMMC adds nothing beyond FAR 52.204-21 and SP 800-171. **It verifies what contracts already demand.** [02] [04]

Not a One-Time Badge
Status is current only with an affirmation under a year old. **Let it lapse and award eligibility lapses.** [05]

Not Federal Systems
Systems a contractor operates for the Government are excluded. **Only contractor systems with FCI or CUI.** [01]

Not Settled in 2026
Phase II is suspended pending a reform task force. **Phase I, SPRS and DFARS 7012 still bind today.** [10]

08 MYTHS VS. REALITY

MYTH	REALITY
"CMMC finally makes us implement NIST SP 800-171."	DFARS 252.204-7012 required it **not later than December 31, 2017**; CMMC checks whether you actually did. [04]
"Revision 3 is what CMMC assesses now."	NIST withdrew Rev. 2 in 2024, but **32 CFR 170 still incorporates Rev. 2 and its 110 requirements**. [08] [01]
"The Phase II suspension ended CMMC."	It paused the C3PAO default and future milestones; **Phase I self-assessments, affirmations and 7012 remain**. [10]
"A POA&M lets us certify with gaps anywhere."	Never at Level 1; at Level 2 only **one-point items, at 80 percent or better, closed within 180 days**. [01]
"Our prime holds the certificate; subs just sign."	Any subcontractor handling CUI needs **at least Level 2 (Self)**, and Level 2 (C3PAO) whenever the prime does. [01] [05]

09 SPEAK THE PROGRAM — KEY TERMS

FCI
Information provided by or generated for the Government, **not for public release**.

CUI
Information that law, regulation or policy requires safeguarding; **see 32 CFR 2002.4(h)**.

OSA / OSC
Organization Seeking Assessment, or **Seeking Certification** under a C3PAO or DIBCAC.

C3PAO
CMMC Third-Party Assessment Organization, **authorized or accredited** to certify Level 2.

CONDITIONAL STATUS
A passing score with an open POA&M; **it expires at 180 days** unless closed out.

AFFIRMING OFFICIAL
The senior representative who **attests to continuing compliance** in SPRS.