PRESCIENT SECURITY

CMMC Program Update

CMMC after July 13, 2026

What changed, what remains, and what organizations should do now

INTERIM BRIEF | JULY 16, 2026

Key takeaway

The Department paused the planned expansion of mandatory Level 2 C3PAO and Level 3 procurement requirements. It did not eliminate the obligation to protect FCI and CUI, rescind 32 CFR Part 170, or remove applicable NIST SP 800-171 and DFARS safeguarding duties.

PAUSED

- November 2026 Phase II transition
- New Level 2 C3PAO procurement designations
- New Level 3 procurement designations
- Pending and future rollout milestones

STILL ACTIVE

- Phase I self-assessment requirements
- NIST SP 800-171 Rev. 2 baseline
- DFARS safeguarding and incident reporting
- Applicable SPRS records and affirmations

UNDER REVIEW

- Future independent-assessment model
- Replacement implementation dates
- Cost, capacity, and automation approach
- Long-term treatment of certification requirements

Important distinction:

The July 13 actions only affect how DoW program offices apply CMMC requirements in procurements while the review is underway. The memoranda do not prohibit organizations from voluntarily pursuing a Level 2 C3PAO assessment.

Please note

This document is for planning purposes only. Organizations should check the requirements in each solicitation, contract, subcontract, or prime contractor direction before changing their compliance or assessment strategy.

CMMC comparison matrix

Interim status based on public guidance available as of July 16, 2026

Reading note: "What changed" describes the July 13 policy action. "What customers should do now" identifies the interim posture and does not replace a solicitation amendment, contract modification, or legal review.

Area	Original plan before July 13, 2026	What changed	What customers should do now
Implementation timeline	Phase I started on November 10, 2025. The plan was to add more CMMC requirements over four phases. Phase II was planned for November 10, 2026, with full rollout by November 2028. [3][6]	The November 2026 Phase change and later rollout dates are paused during a 60-day review. [1][2]	Phase I is still active. The government has not announced a new date for Phase II or later phases. [3]
Level 1: FCI	Organizations that need Level 1 complete a self-assessment each year and confirm they meet the requirements. [4]	No announced change.	If your contract requires Level 1, continue the self-assessment and annual confirmation. [3][4]
Level 2: Self-Assessment	DoW could require a Level 2 self-assessment for some contracts that involve CUI. The assessment is repeated every three years, with confirmation at the time of assessment and each year after that. [4]	During the pause, DoW programs may not require Level 2 C3PAO assessments. Active solicitations must be updated, and affected existing contracts should be modified. [2]	If your solicitation, contract, or subcontract requires Level 2 self-assessment, complete it, keep your SPRS record updated, and submit required confirmations. [2][4]
Level 2: C3PAO certification	Phase II was expected to make third-party Level 2 certification more common for higher-priority CUI contracts. It could have been required to win or keep certain work. [4][5]	While the suspension is in effect, DoW program managers and requiring activities may not require Level 2 C3PAO assessments. Active solicitations must be amended, and affected existing contracts must be modified. [2]	Level 2 C3PAO certification is not being added as a mandatory DoW procurement requirement during the paused rollout. The rules and assessment process still exist. [2][4]
Level 3: DIBCAC	Level 3 requirements were planned for the highest-priority programs in later phases. [4]	During the pause, DoW programs may not require Level 3 assessments. [2]	There is no new Level 3 requirement or new rollout date right now. Some government-led assessments may still continue during the review. [1][2]
Solicitations and contracts	New solicitations and contracts were expected to include the required CMMC level and assessment type more often as the rollout expanded. [5][6]	Active solicitations with Level 2 C3PAO or Level 3 requirements must be updated. Existing contracts and agreements should remove those requirements before the next option period or during the next scheduled administrative update. [2]	Check the actual amendment, contract update, subcontract, or direction from your prime contractor. Do not assume your requirement changed until the document is updated.
NIST SP 800-171 and DFARS safeguarding	Contractors handling covered defense information were required to implement NIST SP 800-171 Rev. 2 and comply with DFARS 252.204-7012. [4][5]	No change.	NIST SP 800-171 Rev. 2, safeguarding, cyber incident reporting, and related contractual responsibilities remain in effect. [1][2]
SPRS and affirmations	Assessment results and confirmations were recorded in SPRS. Level 1 is annual. Level 2 self-assessment and certification generally follow a three-year assessment cycle with annual confirmations. [4]	No announced change to the underlying SPRS or affirmation rules.	Keep SPRS submissions, assessment records, and annual confirmations up to date. If you already have a status, continue maintaining it unless official guidance says otherwise. [4]
Plans of action and milestones	Limited POA&Ms were allowed for some Level 2 findings, with closeout required within 180 days. Level 1 POA&Ms were not allowed. [4]	No announced change to the POA&M provisions in 32 CFR Part 170.	The limited POA&M and 180-day closeout rules still apply when a conditional status is used. [4]
Existing CMMC statuses	Final Level 2 C3PAO status generally remained current for three years, as long as the organization submitted annual confirmations and stayed compliant. [4][5]	The July 13 memoranda did not announce that existing statuses were cancelled or invalidated.	32 CFR Part 170 is still in effect. Keep meeting the conditions of your existing status and watch for official guidance on how it will be treated in future procurements. [4]
Reason for the review	CMMC was designed to help make sure organizations protect FCI and CUI across the defense supply chain. [4][6]	DoW pointed to cost, limited third-party assessment capacity, complex timelines, acquisition concerns, and barriers for small and non-traditional businesses. A 60-day reform task force was directed. [1][7]	The future assessment and assurance model is under review. No final replacement framework or implementation schedule has been announced.
What organizations should do	Prepare for the assessment type that may apply to future contracts and keep meeting the cybersecurity requirements in current contracts.	Organizations now face uncertainty regarding when mandatory third-party certification may return and what form it may take.	Continue implementing NIST SP 800-171, preserve evidence, keep applicable SPRS data and affirmations current, verify opportunity-specific requirements, and make risk-based decisions rather than abandoning readiness. [2][4]

Recommended actions

Maintain cyber readiness while the Department completes its review

What to do now

- Keep implementing and sustaining the controls required by NIST SP 800-171 and current contracts.
- Preserve objective-specific evidence, configuration records, and assessment files.
- Keep applicable SPRS entries and annual affirmations current.
- Review each solicitation, contract modification, and subcontract flowdown before changing course.
- Continue readiness planning based on business risk, customer expectations, and the cost of losing momentum.

What you should watch

- The future role and scope of independent third-party assessments.
- Replacement dates for Phase II and later implementation milestones.
- How existing CMMC statuses will be treated in future procurements.
- Whether the Department adopts new risk tiers, automation, reciprocity, or alternative assurance mechanisms.
- Additional instructions for contracting officers, primes, C3PAOs, and organizations seeking assessment.

Prescient Security's perspective

Prescient Security has supported assessments across multiple federal and industry frameworks and has helped organizations navigate program reviews, regulatory transitions, and modernization efforts. While the Department evaluates the future CMMC assessment model, our focus remains helping customers build sustainable cybersecurity capabilities that satisfy current contractual obligations and prepare them for future assurance requirements.

How Prescient Security can support organizations during the review

1. CMMC and NIST SP 800-171 readiness, mock assessments, and evidence review.
2. Independent certification assessments where appropriate and permitted under current program rules.
3. Contract- and opportunity-specific scoping to distinguish tive obligations from anticipated future requirements.
4. Cross-framework strategy for FedRAMP, GovRAMP, FISMA, CJIS, NIST CSF, and related assurance programs.
5. Planning to keep security controls and evidence ready as requirements change.

Primary sources:

[1] Department of War CIO, "*Removing Barriers to Defense Industrial Base Expansion: Immediate Suspension and Strategic Review of CMMC Requirements*," July 13, 2026.

[2] Under Secretary of War for Acquisition and Sustainment, "*Implementing Suspension of CMMC Phase II Requirements*," July 13, 2026.

[3] Department of War CIO, *CMMC program page and current implementation status*.

[4] 32 CFR Part 170, *Subpart D, Key Elements of the CMMC Program*.

[5] DFARS 252.204-7021, *Contractor Compliance With CMMC Level Requirements*.

[6] Federal Register, 90 FR 43560, *Final DFARS rule effective November 10, 2025*.

[7] Department of War, "*Forging the Arsenal of Freedom: Department Suspends CMMC Phase II Requirements*," July 13, 2026.