COMPLIANCE POSTURE BRIEF

CMMC after the suspension: what software vendors *still owe*

What the 13 July 2026 memo paused, the obligations it left standing, and the one architectural decision that prices everything downstream.

PREPARED FOR

Software vendors evaluating or already inside defense work.

SCOPE

CMMC Levels 1 and 2, and the clause behind them

BASIS

Public federal record only. No self-attested claim shown as verified.

NOT

Legal advice, an assessment, or a certification of any kind

> On 13 July 2026, the CMMC Phase 2 requirement for mandatory certification by an authorized third-party assessment organization was suspended by DoD CIO Memo 26-P-1023. As of 2026-11-04, no rule in the Federal Register has set a replacement date.

What was suspended, and what was not

Two readings of that are common and both wrong. It is not the end of CMMC, and it is not permission to stop.

What paused is one step: who confirms your posture. What did not pause is the posture itself. DFARS 252.204-7012 still obliges adequate security by reference to NIST SP 800-171, the separate self-assessment requirement is still in force, and the 72-hour incident reporting obligation is untouched. An applicable Department of War solicitation can still specify a certified assessment, and a prime can still flow the requirement down by contract.

> So the arithmetic did not improve — it got harder to see. You had a date to plan against; now you have the same obligations and no date, and the gate arrives with a solicitation or a prime's questionnaire instead of on a calendar everybody shares.

The two assessment paths

At Level 2, a contract can be satisfied by self-assessment — you evaluate your own environment, record the result, and a senior official affirms it — or it can require certification by an authorized third-party assessor. Phase 2 would have made the second the default. With the mandate suspended, **the contract is the only thing that decides.**

The requirement set is identical either way; who confirms it is the only variable. A self-assessment runs on your schedule. A certification runs on an assessor's, drawn from a finite population whose calendars will not stay open if the mandate returns.

Which level applies to you

Three tiers, by the sensitivity of the information you handle.

- **Level 1 — basic safeguarding.** Applies where you handle Federal Contract Information: provided by or generated for the government under a contract, and not for public release. Met by an annual self-assessment against a short set of fundamental practices.
- **Level 2 — Controlled Unclassified Information.** Built on the NIST SP 800-171 requirement set. Satisfied by self-assessment or third-party certification, depending on the contract.

- **Level 3 — highest sensitivity.** A government-led assessment adding selected enhanced requirements, for the programs where compromise costs the most.

Most software vendors land at Level 1 or Level 2, and the dividing line is a data question, not a company-size one: is what you touch Federal Contract Information, or CUI?

The 110 requirements, and where the effort actually goes

The CMMC rule keys Level 2 to Revision 2 of NIST SP 800-171 — 110 requirements across fourteen families. A later revision reorganizes the material, so read the revision your solicitation names rather than counting from memory.

The work concentrates in four places.

- **Identity and access.** Multifactor everywhere, least privilege, privileged accounts separated from ordinary ones. Reliably the largest engineering lift.
- **Audit and accountability.** Centralized logging with protected storage, and evidence that a person reviews it — not merely that logs exist.
- **Configuration management.** Baselines, controlled change, drift detection.
- **Evidence.** Not a family of its own, and still the most common reason a competent security program struggles. The gap is rarely the control; it is demonstrating on demand that the control operates as described.

Scoping is the decision that sets the price

The single largest cost driver is how much of your company falls inside the assessment boundary. A vendor that runs CUI through its general corporate environment has scoped its entire business into the assessment. A vendor that built a separate enclave — a distinct environment where CUI lives, with controlled paths in and out — has scoped a fraction of it. The enclave costs engineering effort up front and reliably costs less overall.

For a software company this makes product architecture a compliance decision. A product that can be deployed so the customer's CUI stays in the customer's tenant is in a materially different position from one that ingests CUI into yours — and that is not a decision you can make in the eight weeks before an assessment.

Conditional status is narrower than you think

A conditional outcome — a passing assessment with a plan of action covering a limited set of open requirements — exists, and it is not the safety net vendors read it as. Only requirements worth one point can go on the plan (one encryption case aside), and the plan must be closed

out within 180 days or the conditional status expires. It finishes genuine edge cases; it is not a strategy.

"We are only a subcontractor" is not an exemption

Flowdown does not arrive as a solicitation. It arrives as a questionnaire from a prime's supply-chain team with a short deadline attached — and since the prime's obligation is contractual, the suspension of the program mandate does not remove it. Vendors who already know their posture answer the questionnaire. Vendors who do not lose the subcontract to someone who could.

The clause that has required this all along

CMMC did not invent these obligations — it verifies them, and the suspension of that verification leaves them exactly where they were. DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, has required adequate security by reference to NIST SP 800-171 for the better part of a decade. Two parts catch software vendors specifically.

Cyber incident reporting within 72 hours of discovery

The clock starts at discovery — not at confirmation, and not at the end of an internal investigation. Reporting requires a medium assurance certificate to reach the government's portal, and obtaining one takes time you will not have mid-incident.

The external cloud service requirement

If you use an external cloud service to store, process, or transmit covered defense information, that provider must meet security requirements equivalent to the FedRAMP Moderate baseline. A well-implemented security program on a commercial tier that does not meet that baseline is still non-compliant. Confirm the specific offering and region your federal deployment uses, not the provider's brand.

The affirmation, and why accuracy beats optimism

CMMC requires a senior official to affirm continuing compliance, at each assessment and annually thereafter. That affirmation is a representation to the government, and false representations about cybersecurity compliance have already produced civil enforcement actions against contractors under the False Claims Act. Overstating readiness in marketing copy is a reputational risk; overstating it in an affirmation is a legal one.

Working backwards from your pipeline, not from a date

There is no government date left to work back from. Work back from the first opportunity you intend to bid.

1. NOW
   Decide where CUI lives. Enclave or general environment. Everything downstream is priced by this answer.
2. NEXT
   Write the System Security Plan against the environment you actually have, not the one you intend to have. It is what an assessor works from, and its precision shapes the assessment.
3. THEN
   Close the identity, logging, and configuration gaps — and generate evidence as a by-product of operations, not as a project.
4. BEFORE YOU NEED IT
   Engage an assessor if your target contract requires one. Authorized third-party organizations are a finite population.
5. THROUGHOUT
   Keep the plan of action honest. An unimplemented requirement documented with a date is normal. One that appears nowhere is the finding that turns an assessment into an enforcement question.

What this brief does not tell you

Whether a specific solicitation carries a CMMC requirement, which level it invokes, or which revision it names. Those are contract-specific, and they are the facts that bind you.

Nor whether any particular company holds a certification. A company's own statement that it is compliant is not the same as a government record saying so, and GovExpress renders those two things differently everywhere — verified and self-attested are never merged.

Sources, and how to verify this yourself

Confirm all of it at the source.

- **DoD CIO Memo 26-P-1023, 13 July 2026** — the memorandum that suspended mandatory certification, issued by the Department of War CIO. Read it before acting on any summary, this one included: its scope decides whether your target contract is affected.
- **federalregister.gov** — the CMMC program rule and the acquisition rule that carries it into contracts. Its phased schedule predates the suspension.

- **acquisition.gov** — the current text of DFARS 252.204-7012 and its companion clauses. This is the obligation the suspension did not touch.
- **dodcio.defense.gov** — the Department of War's own CMMC program materials, including scoping and assessment guidance.
- **fedramp.gov** — the baselines the external cloud service requirement points at.

Where this brief and the clause in front of you disagree, the clause wins.

Score your company's federal readiness at govexpress.ai/app/score.

GovExpress is a diagnostic. We are not an assessor, a C3PAO, a 3PAO, or a certification body, and nothing in this brief certifies anything. A C3PAO and a FedRAMP 3PAO are separate accreditations — one is not the other. This document is informational and is not legal advice.

Prepared by GovExpress · govexpress.ai · Version 2.1, 4 November 2026