SCALE LLP

CLIENT ALERT

Department of War Suspends CMMC Phase II

What Dual-Use and Defense Tech Companies Need to Know

Introduction

On July 13, 2026, the Department of War (DoW) announced it is immediately suspending Phase II of the Cybersecurity Maturity Model Certification (CMMC) program, which had been set to take effect November 10, 2026. Third-party assessments and future CMMC milestones across DoW solicitations and contracts are paused.

DoW's Chief Information Officer, Kirsten Davies, said the move responds to "prohibitive compliance costs and bureaucratic burdens" that, according to the Small Business Administration, are pushing innovative companies, including plenty of dual-use and non-traditional defense tech firms, out of the Defense Industrial Base.

DoW launched a 60-day review of the whole CMMC program, aimed at speeding up capability delivery and easing the load on small and mid-size businesses. For companies in the dual-use or defense tech space, this is welcome news, but with an important caveat. The rule is temporarily paused, not repealed, raising immediate questions about existing contracts, certification plans, and subcontractor obligations.

What's Suspended & What Isn't

- The suspension halts CMMC Phase II specifically. That means the third-party assessment requirements under DFARS 252.204-7021 are halted while the review is underway.
- CMMC Phase I self-assessments stay in place, and so do DFARS 252.204-7019 and 252.204-7020 (self-assessment scoring and Supplier Performance Risk System (SPRS) posting), NIST SP 800-171 Rev 2, and DFARS 252.204-7012, which still requires companies and subcontractors to safeguard covered defense information and report cyber incidents within 72 hours.

Existing Contracts & Active Procurements

The DoW has told program managers and contracting officers to amend or modify solicitations and contracts that still contain CMMC Phase II requirements, as soon as possible. But until a contract is actually modified, the CMMC is still binding. Organizations should not assume relief is automatic, and should confirm the impact in writing with the contracting officer.

Mid-Certification?

Companies in mid-certification should continue Phase I self-assessment and SPRS posting, keeping NIST 800-171 documentation current, and staying assessment ready. A prime contractor may still require CMMC certification or a specific SPRS score as a matter of contract, regardless of the federal updates.

For Subcontractors & Suppliers

DFARS 252.204-7012 still flows down regardless of what happens with CMMC Phase II, prime contractors may still condition subcontract awards on cybersecurity performance.

This is a Suspension – Not a Repeal

The CMMC Phase II suspension is tied to the 60-day review, and DoW has not yet announced a replacement security model or timeline. Expect CMMC Phase II, or some reformed version of it, to return in some form.

Recommendation: Stay the Course

We recommend maintaining cyber security diligence. The Department of Justice has made clear it will keep using the False Claims Act, under its Civil Cyber-Fraud Initiative, to go after noncompliance with DFARS 252.204-7012 and DFARS 252.204-7020, and that scrutiny could extend to inaccurate CMMC Phase I self-assessments too.

Companies still face risk for weak cybersecurity, and those that keep investing in their cybersecurity posture now will be best positioned to win contracts once CMMC Phase II, or its successor, is back in force.

How this plays out depends on contract(s) and where an organization may sit in the supply chain. Scale LLP will proactively monitor the results of this 60-day review.

Scale LLP's Dual Use & Emerging Defense Technology Team

Our Dual Use & Emerging Defense Technology team partners with companies developing next-generation technologies for both commercial and defense markets. We provide strategic counsel on government contracting, regulatory compliance, corporate transactions, intellectual property, and national security matters, helping clients innovate, scale, and seize opportunities in a rapidly evolving sector.

Tim Furin
Partner
tfurin@scalefirm.com

Karey Marren
Counsel
kmarren@scalefirm.com

Laura Mayo
Counsel
lmayo@scalefirm.com

Contact us for more info at (415) 735-5933

Connect with our team to evaluate how the CMMC Phase II suspension may affect your contracts, compliance obligations, and cybersecurity strategy.