Government Contracts and Privacy & Cybersecurity Update

July 2026

DOW Suspends CMMC Program Phase 2; Contractor Obligations Remain

The Department of War (DOW) has suspended the upcoming phase of its Cybersecurity Maturity Model Certification (CMMC) program designed to increase cybersecurity standards and compliance for the defense industrial base. In a memorandum issued on July 13, DOW announced the suspension of Phase 2 of the CMMC program, scheduled to begin this November, while the agency examines whether the program aligns with its priorities. Although the memorandum pauses implementation of Phase 2 requirements, it makes clear that contractors must continue to adhere to CMMC Phase 1 requirements, including Levels 1 and 2 self-assessments.

DOW issued regulations implementing the CMMC 2.0 framework in September 2025, which established three levels of cybersecurity requirements. Contractors at CMMC Level 1 and some at Level 2 must conduct a self-assessment of compliance with specified cybersecurity standards. Most contractors at Level 2 must engage a third party to conduct a compliance assessment. For contractors at CMMC Level 3, DOW would certify compliance with applicable cybersecurity requirements. Phase 1 of CMMC 2.0, which began in November 2025, requires contractors at Levels 1 and 2 to submit their self-assessments to DOW reflecting their certification to compliance with applicable cybersecurity standards. Under Phase 2, contractors were to complete third-party assessments of cybersecurity compliance.

In its July 13 memorandum, DOW suspends the November 2026 transition deadline for Phase 2, noting that although the CMMC program is intended to enhance security, it has imposed "significant and often prohibitive burdens" on the defense industrial base, particularly small businesses and non-traditional contractors. In addition, the memorandum states that all pending and future CMMC implementation milestones for DOW solicitations and contracts are held in abeyance until further notice. It further notes that DOW activities and personnel shall only include the CMMC Level 1 or 2 self-assessment requirements in procurement documents, and that all other cybersecurity clauses in contracts remain in force.

The memorandum establishes a "CMMC Reform Task Force" to conduct a complete review of the CMMC program over a 60-day period. The task force is responsible for redesigning the agency's approach to cybersecurity compliance by the defense industrial base supply chain to adhere to the DOW secretary's acquisition priorities. The memorandum notes that the task force's recommendations should focus on "a reformed cybersecurity and operational resilience framework that prioritizes speed to capability, lower barriers for small, medium, and non-traditional businesses, and replaces prohibitive, third-party models with scalable, realistic security measures."

Although many contractors may be relieved by this development, it does not mean that the government's goal of improving cybersecurity in the defense industrial base is entirely on hold. While DOW's memorandum suspends the next phase of CMMC 2.0, contractors must continue to follow applicable cybersecurity standards. The memorandum notes that DOW will maintain enforcement of baseline compliance with NIST SP 800-171 Rev. 2 requirements through contractor self-assessments and select government-led assessments. It also states that

contractors must continue to adhere to the requirements for cybersecurity compliance set forth in DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

Implications for Contractors

While DOW's July 13 memorandum halts implementation of the upcoming phase of CMMC 2.0 while the agency considers the program, contractors should be aware of ongoing cybersecurity compliance obligations and the implications for compliance failures.

- *Existing compliance requirements remain in force*. The memorandum makes clear that although implementation of CMMC Phase 2 is suspended, the requirements of Phase 1 continue to apply to contractors. As a result, contractors must follow Phase 1 requirements for CMMC Levels 1 and 2 self-assessments. Further, as noted in the memorandum, the requirements of DFARS 252.204-7012 remain in force, so contractors must ensure that they meet NIST SP 800-171 requirements.
- *Penalties for false certifications*. Because the memorandum underscores continued compliance obligations with DFARS 252.204-7012, contractors should not relax their vigilance with respect to NIST SP 800-171 compliance. Under its Cyber-Fraud Initiative, the Department of Justice seeks to investigate and prosecute contractors under the False Claims Act for noncompliance with applicable cybersecurity standards.

Our Government Contracts and Privacy & Cybersecurity groups will continue to monitor developments related to the implementation of the CMMC 2.0 program and can assist with questions regarding the implications of DOW's memorandum.

FOR MORE INFORMATION

For more information, please contact:

Francis E. (Chip) Purcell, Jr.
202.263.4118
Chip.Purcell@ThompsonHine.com

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Edward T. DeLisle
202.973.2725
Edward.DeLisle@ThompsonHine.com

Jamar T. King
937.443.6852
Jamar.King@ThompsonHine.com

Ryan S. Spiegel
202.973.2742
Ryan.Spiegel@ThompsonHine.com

Joseph R. Berger
202.263.4193
Joseph.Berger@ThompsonHine.com

Kathryn Pettit
610.304.0987
Kathryn.Pettit@ThompsonHine.com

Andrés M. Vera
202.973.2795
Andres.Vera@ThompsonHine.com

Amaiya Johnson
202.973.2762
Amaiya.Johnson@ThompsonHine.com