DEPARTMENT OF WAR SUSPENDS CMMC PHASE II: WHAT YOU NEED TO KNOW

KEVIN BARNETT, KRISTEN BERTCH, AND JON KNIGHT FROM BAKER HOSTETLER

As reported in the last issue of *Modern Casting*, the Department of War (DoW) has announced the immediate suspension of Phase II of the Cybersecurity Maturity Model Certification (CMMC) program and has launched a comprehensive review of the certification framework. Importantly, this is not a suspension of the requirements for protecting Controlled Unclassified Information (CUI) under DFARS 252.204-7012.

Under the announcement, DoW will continue to enforce Phase I requirements, including self-assessments and annual affirmations of compliance, while evaluating whether and how the broader CMMC program should continue.

For defense contractors, the suspension alleviates the near-term burden of obtaining third-party CMMC certifications but leaves in place the existing obligation to self-assess and report compliance. False statements in these reports will continue to expose contractors to liability under the False Claims Act in lawsuits filed by the government and qui tam relators (whistleblowers who file False Claims Act complaints on the government's behalf and can share in the recovery proceeds).

WHAT HAPPENED

After years of false starts, CMMC Phase I became effective in November 2025. Phase I, which mirrors prior DFARS requirements, requires applicable contractors to conduct self-assessments and report compliance scores through the Supplier Performance Risk System (SPRS). It also allows contracting officers to require ad hoc Level 2 Certified Third-Party Assessment Organization (C3PAO) assessments. Phase II, scheduled to begin on Nov. 10, 2026, would have required mandatory Level 2 C3PAO assessments for most defense contractors handling CUI. Small and medium-sized defense contractors raised serious concerns about assessment costs and burden and lobbied the DoW to walk back requirements.

On July 13, DoW announced that it was suspending Phase II and launching a 60-day review of the program. According to DoW, concerns about compliance costs, assessment capacity, and barriers to participation in the defense industrial base contributed to the decision. DoW stated that it will continue to rely on self-assessments and selected government-led assessments while the review is ongoing. DoW has invited comments from industry.

WHAT THE SUSPENSION MEANS

For now, defense contractors will not be required to obtain the third-party certifications that would have been required under Phase II. The DoW has directed that any C3PAO requirements included in pending solicitations be promptly removed through amendments and that any requirements appearing in current contracts be removed through contract modifications. The planned rollout of broader C3PAO assessment requirements has been paused.

However, the suspension should not be mistaken as eliminating contractors' cybersecurity obligations. Contractors that process, store, or transmit Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) remain responsible for meeting existing contractual cybersecurity requirements, such as FAR 52.204-21 and DFARS 252.204-7012. Phase I remains in effect.

WHAT CONTRACTORS MUST STILL DO UNDER PHASE I

If you handle FCI (as most contractors do), you are still subject to CMMC Level 1 requirements, including annual self-assessments against the applicable safeguarding controls and compliance affirmations. If you handle CUI, then you remain responsible for implementing the security requirements associated with CMMC Level 2, which are based on the 110 security controls in NIST SP 800-171. Under Phase 1, organizations generally must:

- Implement and maintain the required NIST SP 800-171 controls.
- Maintain a System Security Plan (SSP) documenting how those controls are implemented.
- Conduct the required self-assessments.
- Submit assessment results through SPRS.
- Make annual affirmations of compliance.
- Ensure applicable subcontractors satisfy flowed-down cybersecurity requirements.

In short, contractors may have gained relief from third-party certification deadlines, but they have not been relieved of their underlying cybersecurity obligations.

FALSE CLAIMS ACT RISK HAS NOT GONE AWAY

The suspension of Phase II may increase the significance of self-assessments because the government will be relying more heavily on contractor representations regarding cybersecurity compliance. The DoW announcement emphasized that it is not suspending contractors' underlying cybersecurity obligations.

The Department of Justice has made cybersecurity enforcement a priority through the Civil Cyber-Fraud Initiative, which focuses on situations where contractors allegedly misrepresent compliance with cybersecurity requirements or fail to

KEY TAKEAWAYS

Phase II relief is limited. Contractors may no longer face an immediate Level 2 certification requirement, but their existing cybersecurity obligations remain in force.

Self-assessments now matter even more. Contractors handling CUI must continue implementing NIST SP 800-171 controls, maintaining accurate documentation, submitting supportable assessments and making defensible compliance affirmations.

Enforcement risk is shifting, not disappearing. With DoW relying more heavily on contractor self-representations, inaccurate compliance statements may create post-award False Claims Act and cyber-fraud enforcement exposure.

adequately protect sensitive government information. While the CMMC framework continues to evolve, existing contract requirements under DFARS 252.204-7012, NIST SP 800-171 and related representations remain enforceable.

CONTINUED RISK AREAS

Contractors should pay particular attention to the following issues:

Overstated SPRS Scores. Companies that submit assessment scores that do not accurately reflect implementation of required controls may face allegations that they knowingly misrepresented their compliance posture.

Unsupported Annual Affirmations. Annual affirmations of compliance should not be viewed as administrative exercises. They should be supported by documented evidence demonstrating control implementation and operational effectiveness. Contractors should be prepared to substantiate their assertions if challenged.

Inaccurate SSPs. SSPs frequently become outdated or fail to accurately describe operational environments. An SSP that materially differs from reality can become evidence supporting allegations that compliance representations were misleading.

Failure To Close Known Gaps. Many organizations maintain Plans of Action and Milestones. Contractors should ensure that known deficiencies are properly documented, tracked, and remediated in accordance with applicable requirements rather than ignored or informally accepted.

Executive Certifications Without Adequate Diligence. As compliance affirmations increasingly become management-level decisions, executives should ensure they have a reasonable basis for representations submitted to the government.

PRACTICAL STEPS FOR CONTRACTORS

DoW's suspension of Phase II creates an opportunity for contractors to reassess their cybersecurity compliance programs before additional certification requirements potentially return.

Organizations should consider:

- Conducting an independent review of their NIST SP 800-171 implementation status.
- Validating SPRS submissions and assessment scores.
- Updating SSPs and associated documentation.
- Reviewing evidence supporting annual affirmations.
- Confirming that CUI is properly identified and scoped.
- Evaluating subcontractor compliance obligations.
- Treating compliance attestations as legal representations rather than purely technical exercises.

BOTTOM LINE

The suspension of CMMC Phase II removes the immediate requirement for contractors to obtain third-party Level 2 certifications. It does not eliminate existing cybersecurity obligations or the requirement to perform self-assessments and make compliance affirmations. Contractors handling CUI remain responsible for implementing NIST SP 800-171 controls, maintaining supporting documentation, and accurately representing their compliance status. It also does not necessarily change the cybersecurity expectation of higher-tiered contractors, which are free to continue to impose obligations on their supply chains.

From an organizational perspective, the principal risk may be shifting from pre-award screening to post-award enforcement. The assessment process would have barred entry for contractors that failed to meet third-party assessment requirements. With DoW's return to a self-assessment framework, more contractors will remain eligible for DoW awards, and false representations will be addressed through post-award enforcement under the False Claims Act and the Department of Justice's cyber-fraud enforcement initiatives. MC

Kevin Barnett is a trusted advisor to government contractors of all sizes, helping companies navigate the complex regulatory scheme imposed on contractors and helping contractors defend their rights through the bid protest and claims processes. He spends an increasing amount of his practice advising contractors on their cybersecurity obligations and the Cybersecurity Maturity Model Certification process.

Kristen Bertch advises clients on current and anticipated regulatory requirements for healthcare entities, as well as entities handling government or other sensitive data, including obligations related to the Cybersecurity Maturity Model Certification (CMMC) Program, FedRAMP, and other cybersecurity standards. With in-depth knowledge of data breach laws, widely recognized security standards, and legally required security practices, she helps clients handling sensitive data.

Jon Knight focuses his practice on technology-related investigations, compliance, and litigation. He is experienced in guiding clients through cybersecurity incident response, data breach litigation, and regulatory enforcement actions, and advises clients on cybersecurity, AI, and privacy governance and transactional issues and conducts pre- and post-acquisition due diligence on privacy and cybersecurity issues.