Ramish and Prince for Law360: DOD's Cyber Certification Pause May Heighten FCA Risks

By Daniel Ramish, Zachary Prince | July 17, 2026

RELATED PRACTICES Government Contracts

In an article for *Law360*, Haynes Boone Partners **Dan Ramish** and **Zach Prince** examine the U.S. Department of Defense's decision to suspend Phase 2 of the Cybersecurity Maturity Model Certification (CMMC) program and what it means for defense contractors.

While the pause eliminates near-term third-party assessment requirements, Ramish and Prince explain that contractors must still comply with existing cybersecurity obligations under NIST SP 800-171 and continue to certify their compliance through self-assessments. They note that the shift away from third-party verification may actually increase False Claims Act (FCA) risk, as contractors' own representations regarding cybersecurity compliance will face greater scrutiny.

Read the full article below and on the *Law360* website **here**.

DOD's Cyber Certification Pause May Heighten FCA Risks

On July 13, the U.S. Department of Defense released a memorandum and a request for information suspending Phase 2 of the Cybersecurity Maturity Model Certification program that would have required certified third-party assessments.[1] The memoranda explain both why the agency is taking this action and how it intends to implement the suspension.

As DOD Chief Information Officer Kirsten Davies wrote in the memorandum, "the current CMMC program is structurally incompatible with [the Department's] need to rapidly expand the [Defense Industrial Base)]."[2] The memorandum stated that the CMMC program as currently constituted "imposes significant and often prohibitive burdens on the [DIB], particularly the small and non-traditional businesses that are the engine of American innovation."

After years of iterative changes and a previous overhaul of the program, the DOD is once again reconsidering its approach to assuring adequate protection of controlled unclassified information, or CUI, on contractor information systems. A newly established CMMC reform task force is charged with recommending a framework that, in the memorandum's words, "replaces prohibitive, third-party compliance models with scalable, realistic security measures" — suggesting third-party certification may not return in its current form. CMMC 3.0 may be on the horizon.

Contractors must continue to comply with existing cybersecurity requirements during the suspension period. The CMMC Level 2 self-assessment clause will continue to be included in defense contracts involving CUI, requiring implementation of cybersecurity requirements known as NIST SP 800-171, notwithstanding the pause in third-party assessments.

Under CMMC Level 2 (Self), only a limited set of controls remains eligible for plans of action and milestones, or POA&Ms, in lieu of immediate compliance, and even those controls are subject to a 180-day closeout period.

In sum, contractors receive relief from third-party assessments, not from compliance itself or from the risks associated with noncompliance, including contract termination and False Claims Act liability. Indeed, FCA risk may become more pronounced during the suspension because contractors must affirm their conditional or final CMMC Level 2 (Self) status to remain eligible for covered contracts. Any overstatement in those affirmations could expose contractors to significant FCA liability.

CMMC's Verification and Full Compliance Components

The CMMC program was designed to verify that contractors are implementing the full set of NIST SP 800-171 cybersecurity controls. To accomplish that objective, CMMC incorporates two complementary features.

First, for most contractors handling CUI, it replaces the contractor self-attestation framework under Defense Federal Acquisition Regulation Supplement 252.204-7019 and 252.204-7020 with independent third-party assessments to verify implementation of the required controls.

Second, unlike the existing DFARS regime, which permits contractors to rely more broadly on POA&Ms, CMMC requires contractors to achieve full implementation of NIST SP 800-171, permitting POA&Ms only for a narrowly defined subset of controls that must be remediated within 180 days.

In short, CMMC strengthens both the verification mechanism and the expectation of full compliance established under the existing DFARS cybersecurity clauses.

The Phase 2 suspension affects only the first feature. It pauses third-party verification while leaving intact CMMC's more stringent compliance requirements, including the limited availability of POA&Ms.

Security Imperatives Versus Small Business Reality

There is an inherent tension between the need to safeguard CUI from adversaries and the need to avoid imposing undue cost and burdens on the small businesses that make up the majority of the defense industrial base.

Implementing the government-specific cybersecurity requirements of NIST SP 800-171 is challenging and expensive, typically requiring outsourced support, and presents a genuine barrier to entry into the defense market. These burdens have increased as NIST SP 800-171 has evolved. Revision 3 of the standard would be mandated under the proposed Federal Acquisition Regulation CUI rule that is part of a broader overhaul of the FAR.[3]

Meanwhile, the DIB, and particularly small business participation within it, has contracted significantly over the past 15 years.

The CMMC program did not resolve the inherent conflict between the need for heightened cybersecurity and the resource-intensive burden on small businesses. To the contrary, the CMMC rollout may have forced the conflict to come to a head.

As the CMMC program rollout began, there were signs that the DOD may have lacked confidence that the DIB would be able or willing to achieve full compliance. For example, while the CMMC rule at Title 32 of the Code of Federal Regulations, Part 170, contemplated that the CMMC clause would be included in all contracts involving CUI beginning in Phase 1, the corresponding DFARS

implementation gave program offices and requiring activities discretion during the first three years of the rollout to determine whether a solicitation or contract would require a specific CMMC level.

The DOD components have also been urging prime contractors to obtain greater information and assurances from their supply chains regarding subcontractors' ability to comply with the CMMC requirements, compounding inconsistent messaging about the scope and urgency of these obligations. Anecdotal feedback from small businesses and nontraditional defense suppliers indicates that many remain far from full compliance.

At the same time, the DOD is attempting to reimagine government procurement to make government buying faster, with less red tape and more focus on achieving the warfighting mission. Expensive cybersecurity implementation is arguably in tension with this objective as well, and the DOD appears to be wavering on whether CMMC is workable as part of that vision.

The CMMC Phase 2 Pause

CMMC Phase 2, which had been scheduled to begin on Nov. 10, would have marked the point at which designated procurements could require as a condition of contract award CMMC Level 2 assessments completed by a certified third-party assessor organization or, where applicable, CMMC Level 3 assessment completed by the Defense Industrial Base Cybersecurity Assessment Center. In anticipation of that milestone, some program offices had already begun incorporating certain Phase 2 requirements into solicitations and contracts.

According to the DOD guidance, the suspension of CMMC Phase 2 affects solicitations, existing contracts and new awards as follows:

- ***Current solicitations:*** Program managers and requiring activities are directed to amend active solicitations to remove CMMC Level 2 and CMMC Level 3 requirements "as soon as practicable." These will presumably be replaced with CMMC Level 2 (Self).
- ***Existing contracts:*** Contracting Officers are directed to remove CMMC Level 2 and CMMC Level 3 requirements from existing contracts "via modification prior to the exercise of the next option period or during the next scheduled administrative modification." Again, CMMC Level 2 (Self) is the likely substitute in these contracts as well.
- ***New solicitations and contracts:*** The DOD components may designate only CMMC Level 1 or CMMC Level 2 self assessments. Separately, the DOD will continue to enforce baseline compliance through select government-led assessments — presumably Defense Industrial Base Cybersecurity Assessment Center medium or high assessments, already implemented under existing DFARS clauses. Level 2 (Self) is not a ceiling, however; the undersecretary's memorandum states that the Program Managers and requiring activities may require additional cybersecurity protections as commensurate with law and regulation."[4]
- ***Waivers:*** No CMMC waivers will be granted during the review period. Program managers must continue to identify information security requirements for planned contract efforts, but the case-by-case flexibility of the waiver process is suspended along with the phased rollout.

Takeaways for Defense Contractors

Defense contractors may not be subject to third-party verification requirements, at least in the near term, but achieving full compliance with NIST SP 800-171 Rev. 2 controls remains an urgent priority. Contractors should also consider taking steps toward NIST SP 800-171 Rev. 3 in anticipation of its potential adoption.

The DOD's commitment to full compliance has not wavered, and contractors' underlying cybersecurity obligations under DFARS 252.204-7012 and NIST SP 800-171 Rev. 2 remain unchanged. Notwithstanding the pause on third-party assessments, CMMC Level 2 still limits which controls can be deferred through POA&Ms, and requires that any such POA&Ms be closed out within 180 days. Addressing any gaps in implementation of NIST SP 800-171 Rev. 2 controls therefore remains essential to preserving eligibility for defense contracts and subcontracts involving CUI.

A shift back toward self-assessment places even greater weight on the accuracy of contractors' own compliance representations, which is precisely where FCA exposure arises. The U.S. Department of Justice has given no indication that it will relax enforcement of cybersecurity representations and requirements under its Civil Cyber-Fraud Initiative, as demonstrated by a recent series of FCA settlements involving cybersecurity representations.

Contractors should ensure that they have conducted appropriate self-assessments, that their scores are justified and well documented, and that they maintain sufficient evidence of their current system state before affirming.

One implementation detail left unaddressed in the memorandum is how subcontracts and supplier agreements should be modified to remove third-party and Defense Industrial Base Cybersecurity Assessment Center assessment requirements. Contractors should watch for further DOD guidance on this point.

What to Watch

Whether the DOD ultimately returns to third-party certification, adopts a different verification model or moves toward broader reliance on self-attestation remains to be seen. The 60-day review should provide greater clarity regarding the future of the DOD's cybersecurity and CMMC verification requirements.

The DOD is soliciting stakeholder input through its public request for information that seeks views on which current controls deliver meaningful risk reduction, and how commercial capabilities and self-attestation might anchor a reformed framework. These questions telegraph the likely direction of reform. Contractors with views on what should replace the current model should submit comments in response to the request by Aug. 14.

In the meantime, defense contractors performing contracts involving CUI should ensure that they have implemented all required cybersecurity controls under NIST SP 800-171 Rev. 2 or, where permitted, have documented any remaining deficiencies in POA&Ms and are working to remediate them within the required time frame.

Contractors should also ensure that their Supplier Performance Risk System self-assessment scores accurately reflect their current implementation status.

[1] Removing Barriers to DIB Expansion: Immediate Suspension and Strategic Review of Cybersecurity Maturity Model Certification Requirements (July 13, 2026), https://dowcio.war.gov/Portals/0/Documents/Library/CMMC-ReformMemo.pdf; Implementing Department of War Chief Information Officer's Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements (July 13, 2026), https://dowcio.war.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf; Dep't of War, Request for Information: Reforming CMMC and Reducing Compliance Burden for the

Defense Industrial Base (July 13, 2026), https://sam.gov/opp/89ef9bfb0834473791e991c712698d94/view.

[2] Removing Barriers to DIB Expansion: Immediate Suspension and Strategic Review of Cybersecurity Maturity Model Certification Requirements (July 13, 2026), https://dowcio.war.gov/Portals/0/Documents/Library/CMMC-ReformMemo.pdf.

[3] See Federal Acquisition Regulation: Revolutionary Federal Acquisition Regulation Overhaul Parts 1, 2, 4, 33, 39, 40, and 53, 91 Fed. Reg. 37,550 (proposed June 23, 2026).

[4] Implementing Department of War Chief Information Officer's Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements (July 13, 2026), https://dowcio.war.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf.