wiley

ARTICLE

DoD audit flags weaknesses in cybersecurity certification vetting, heightening compliance risks

Reuters
January 9, 2026

This article was originally published by Reuters *and is available here and as a PDF here.*

An audit by the U.S. Department of Defense Office of Inspector General (DoD OIG) has identified critical weaknesses in the Pentagon's process for authorizing third-party organizations to conduct Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 assessments — controls that defense contractors and suppliers must obtain before winning certain DoD contracts.

The 2025 audit concluded that the DoD did not effectively implement the procedures designed to ensure that CMMC third-party assessment organizations (C3PAOs) meet all eligibility requirements before being authorized to assess contractors' cybersecurity preparedness. That shortcoming, auditors warned, could undermine the confidence in the certification regime that is central to protecting controlled unclassified information (CUI) across the defense industrial base.

With CMMC 2.0 going into effect on Nov. 10, 2025, making Level 2 certification a contractual requirement for handling CUI in certain instances, contractors face heightened risks: Gaps in assessor vetting threaten the credibility of certifications, potentially leading to flawed compliance outcomes, contract delays, or even disqualification from DoD opportunities.

Authors

Diana R. Shaw
Partner
202.719.3379
dshaw@wiley.law

Practice Areas

White Collar Defense & Government Investigations

As the defense industrial base navigates stricter enforcement and increased scrutiny, the integrity and reliability of the CMMC assessment process have become critical factors in both operational readiness and competitive positioning.

CMMC 2.0 and a complex authorization framework

Launched in 2021 and formalized as a DoD program in December 2024, CMMC 2.0 requires contractors handling sensitive information to demonstrate compliance with 110 cybersecurity requirements drawn from federal standards. Contractors seeking to handle CUI deemed critical to national security must obtain a Level 2 assessment — conducted by a C3PAO — before contract award.

To qualify as an authorized C3PAO, organizations must satisfy a set of 12 distinct requirements, ranging from personnel certifications to internal quality controls and formal agreements. The CMMC Accreditation Body (Cyber AB) was contracted by DoD to manage this authorization process.

Gaps in checks, risks in assurance

Auditors who reviewed 11 C3PAOs found robust documentation showing compliance with 10 of the 12 prerequisites. However, the DoD and Cyber AB — the nonprofit entity charged with vetting C3PAOs — failed to verify all requirements before granting authorizations.

Specifically:

- Two C3PAOs were authorized without signing C3PAO Background Agreements and Codes of Professional Conduct.
- Four were approved without confirmation that their quality control leads held requisite certifications.
- In some cases, there was no formal assurance that both a certified assessor and a certified quality control lead were part of the assessment team structure required by policy.

The audit highlighted that the absence of a formal quality-assurance process to validate each prerequisite contributed materially to these lapses, raising questions about the reliability of the authorizations.

Broad implications for the defense industrial base

For prime and subcontractors operating in the defense industrial base, the findings underscore a structural weakness in the cyber compliance ecosystem at a time when such compliance is starting to be contractually mandated. Defense firms preparing for CMMC Level 2 certification rely on confidence that assessment results accurately reflect their cybersecurity posture; unauthorized or inadequately vetted assessors could lead to flawed certifications, contract delays, or lost opportunities.

Industry executives and compliance officers are scrutinizing the audit's implications closely. With CMMC requirements integrated into solicitations and awards, doubts about the integrity of assessment authorizations could complicate compliance strategies and give rise to legal risk. For instance, now that CMMC 2.0 Level 2

certification is a contractual prerequisite, a misrepresentation about compliance or the validity of a certification could trigger False Claims Act liability, and the government investigations, treble damages, and potential whistleblower actions that come with it.

Contractors must ensure not only that their cybersecurity practices are robust, but also that their certifications are obtained through properly vetted assessors, as reliance on flawed or inadequately authorized C3PAOs may be viewed as reckless disregard or false certification under the FCA. This evolving risk landscape demands heightened diligence and documentation at every stage of the compliance and certification process.

Reinforcing the framework: DoD OIG recommendations

DoD OIG issued 10 recommendations aimed at tightening the authorization process. These include directives that the DoD Chief Information Officer and the CMMC Program Management Office establish and implement a quality assurance mechanism ensuring that all 12 requirements are verified before a C3PAO is authorized to perform CMMC Level 2 assessments.

Other recommendations call for contract modifications with the Cyber AB to enforce verification of signed guidance agreements and assessor credentials, and to develop a reauthorization process that includes ongoing verification of C3PAO compliance. The report also emphasizes requirements for C3PAOs to immediately notify DoD leadership of changes that could affect authorization status.

While DoD officials agreed with parts of the audit and accepted several recommendations in principle, DoD OIG noted that open recommendations remain, signaling continued oversight and follow-up.

Contractor community reaction and compliance realities

Defense contractors and compliance experts have increasingly raised concerns about bottlenecks in CMMC assessments and the capacity of C3PAOs to meet demand. With limited authorized C3PAOs available and demand rising, firms in the supply chain are already scheduling assessments months in advance. The audit's spotlight on authorization process gaps amplifies the need for stability and predictability in this critical certification pipeline.

For smaller businesses — which often struggle with cybersecurity resources and documentation — uncertainty around assessor qualifications and the rigor of certifications presents operational risks. A misstep in the authorization or assessment process could mean disqualification from lucrative DoD work, a particularly acute concern as compliance requirements are increasingly contractually enforced rather than advisory.

Why it matters nationally

Beyond contract eligibility, the audit's findings touch on broader national security considerations. CUI often encompasses design details, supply chain data, and program details essential to maintaining U.S. military technological edge.

Ensuring the proper vetting of organizations tasked with validating contractor cybersecurity posture, the OIG warned, is "imperative" to "reduce the vulnerabilities that malicious actors can exploit to compromise DoD contractor systems and networks."

A watershed moment for CMMC integrity

The DoD's effort to strengthen contractor cybersecurity with CMMC 2.0 is among the most consequential compliance reforms in years. But if the mechanisms intended to ensure assessor credibility are themselves found wanting, enforcement may inadvertently erode industry trust and lead to legal or contractual challenges. The audit, and its follow-on oversight, represent a critical inflection point as the DoD transitions from voluntary compliance to a fully enforced certification regime.

For contractors navigating the blurred line between compliance and competitive posture, the message is clear: Certification integrity matters as much as certification attainment — and the ecosystem that delivers that integrity must be as robust and reliable as the systems it is intended to secure.