Shumaker

MAY 8, 2026 | PUBLICATION

What Business Leaders Need to Know About Cybersecurity Certification and Enforcement in 2025–2026

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The Department of Defense has fundamentally reshaped the cybersecurity landscape for federal contractors. With the Cybersecurity Maturity Model Certification (CMMC) program now embedded in contract clauses effective November 10, 2025, and False Claims Act enforcement tripling in a single fiscal year, cybersecurity is no longer a technical concern delegated to IT departments. It is a business eligibility requirement with direct implications for revenue, contract awards, and legal exposure.

This article provides an executive-level overview of what has changed, what is at stake, and what actions organizations should prioritize.

Program Origins and Evolution

CMMC traces its origins to Executive Order 13556 (November 2010), which established the Controlled Unclassified Information (CUI) Program. Prior to this Order, over 100 different markings existed across federal agencies—creating confusion and failing to adequately protect sensitive information. The CUI Program standardized how the executive branch handles information requiring safeguarding.

In 2019, DoD announced development of CMMC to move beyond the self-attestation model. The Office of the Under Secretary of Defense for Acquisition and Sustainment conceived the program to secure the Defense Industrial Base against evolving threats. An interim rule published in September 2020 established a five-year phase-in and outlined the framework's core features: tiered practices, required assessments, and contract-based implementation. Following approximately 750 public comments and an internal review, DoD announced a revised CMMC Program in November 2021 with streamlined requirements and reduced compliance barriers.

The current program rests on three pillars: a tiered model requiring progressively advanced cybersecurity based on information sensitivity; an assessment requirement allowing DoD to verify compliance; and phased implementation adding requirements incrementally over three years. DoD estimates approximately 8,350 entities will require Level 2 third-party certification, with assessment capacity ramping from 135 certifications in year one to over 4,400 by year four.

The Regulatory Shift: From Self-Attestation to Mandatory Certification

For years, federal contractors could self-certify compliance with cybersecurity requirements under NIST SP 800-171. That model has ended. Under the finalized CMMC framework, contractors handling Controlled Unclassified Information (CUI) must now obtain third-party certification from Certified Third-Party Assessment Organizations (C3PAOs). Certification status must be maintained throughout contract performance, and non-certified contractors are ineligible for contract award.

The CMMC framework establishes three certification levels. Level 1 applies to contractors handling only Federal Contract Information (FCI), requires 15 basic cybersecurity practices, and permits annual self-assessment. Level 2 applies to contractors handling CUI, requires alignment with approximately 110 NIST SP 800-171 controls, and typically mandates third-party certification. Level 3 addresses highly sensitive programs and requires government-led assessments. Most construction, manufacturing, and supply chain contractors supporting federal projects will fall into Level 1 or Level 2.

The Department of Defense is implementing these requirements in phases. Phase 1 began November 10, 2025, with CMMC clauses appearing in solicitations and contracts and self-assessments required at Levels 1 and 2. Phase 2 begins November 10, 2026, when third-party certification becomes mandatory for many Level 2 contracts. Full implementation across all applicable DoD contracts is expected by 2028.

The Enforcement Reality: False Claims Act Exposure Is No Longer Theoretical

The regulatory expansion is arriving alongside an aggressive enforcement surge. In fiscal year 2025, the Department of Justice secured more than $52 million across nine cybersecurity-related False Claims Act settlements—representing cyber recoveries that have more than tripled over the past two fiscal years. Since the Civil Cyber-Fraud Initiative launched in October 2021, the DOJ has settled at least fifteen civil cyber-fraud cases, with 60 percent of those resolved in FY 2025 alone.

The enforcement theory is straightforward and does not require a data breach. The DOJ's position is that cyber-fraud cases are "not about data breaches" but are "premised on misrepresentations"—the gap between what an organization certifies about its cybersecurity posture and what it actually does. The bar for liability sits at the point of the misrepresentation, not at the point of compromise.

Recent settlements illustrate the breadth of conduct now triggering enforcement:

Defendant	Settlement Amount	Key Allegations

Health Net Federal Services/Centene Corporation	$11.2 million	Failed to scan for vulnerabilities, ignored third-party and internal audit findings, fell short on patch management and access controls in TRICARE administration contract
Illumina Inc.	$9.8 million	Sold federal agencies genomic sequencing systems with software vulnerabilities for seven years, failed to resource product security function, falsely represented compliance with NIST and ISO standards
Raytheon/RTX Corporation/ Nightwing Group	$8.4 million	Used noncompliant internal system across 29 DoD contracts and subcontracts; settlement included successor liability for acquiring entity
MORSECORP Inc.	$4.6 million	Scored -142 on cybersecurity self-assessment, did not correct the record until three months after receiving federal subpoena
Swiss Automation Inc.	$421,234	Failed to protect technical drawings of parts delivered to DoD prime contractors—first settlement reaching defense supply chain subcontractor tier
Aero Turbine Inc./Gallant Capital Partners	$1.75 million	Failed to implement NIST SP 800-171 controls, shared protected defense information with external company in Egypt; first settlement including private equity sponsor as defendant

Key Business Implications

Cybersecurity Is Now a Bid Requirement. CMMC requirements are written directly into DFARS contract clauses, making compliance a prerequisite for contract award rather than a post-award obligation. Organizations that cannot demonstrate the required certification level will be disqualified from competition.

Flow-Down Obligations Extend Throughout the Supply Chain. Prime contractors must ensure subcontractors meet the appropriate CMMC level. For manufacturing and construction firms, this means fabricators,

suppliers, and IT vendors can create compliance risk. The Swiss Automation settlement demonstrates that enforcement has reached the subcontractor tier of the defense supply chain.

Private Equity Sponsors Inherit Compliance Exposure. The Aero Turbine settlement established that PE sponsors acquiring companies with government contracts inherit not just revenue but compliance obligations and enforcement exposure. Self-disclosure and cooperation reduced the damages multiplier but did not eliminate liability.

Whistleblowers Are Driving Enforcement. Qui tam relators, insiders who file suit on behalf of the government, have been the engine behind most cyber-fraud cases. In FY 2025, whistleblower-filed FCA lawsuits outnumbered DOJ-initiated cases by more than three to one, and the 1,297 qui tam actions filed that year set a single-year record. The employees closest to cybersecurity compliance gaps are the employees most likely to report them, with federal law providing financial incentives of 15 to 30 percent of any recovery.

Conditional Certification Offers Limited Flexibility. The final rule permits conditional CMMC certification for contractors at Levels 2 and 3 who are actively resolving Plans of Action and Milestones (POAMs). Conditional status may last up to 180 days. This allows companies to compete for and receive awards while completing remediation, but it is not a substitute for substantive preparation.

Why This Demands Executive Attention

Many construction, manufacturing, and supply chain companies do not view themselves as technology organizations. Their operational environments were not built for compliance. They rely heavily on third-party vendors and legacy systems. Yet these organizations frequently store project specifications, facility data, or infrastructure plans that constitute CUI, and they interface with federal agencies or defense primes.

The result is a compliance gap that creates both legal and commercial risk. Organizations that misclassify data (e.g., failing to identify where CUI or FCI resides across systems), may never apply the required cybersecurity controls. That classification failure cascades into a compliance failure, which becomes an FCA predicate when the organization certifies compliance it has not achieved.

The question Deputy Assistant Attorney General Jenny posed applies to every organization in the defense industrial base: if the DOJ subpoenaed your cybersecurity compliance records tomorrow, would the documentation match the certifications you have already submitted?

Recommended Actions

Determine your required CMMC level. Assess what data your organization handles (FCI versus CUI) and what contracts or bids are approaching. Most contractors will fall into Level 1 or Level 2.

Conduct an independent gap assessment. Benchmark your current posture against NIST SP 800-171 requirements. Focus particular attention on access controls, logging and monitoring, incident response, and vendor management. Do not rely solely on internal self-scoring.

Develop a realistic remediation plan. Prioritize high-risk gaps and formalize a Plan of Action and Milestones. Many organizations require 9 to 12 months to achieve certification readiness.

Engage assessors early. The pool of certified C3PAOs is limited, and demand is high. Delay in scheduling assessments can result in inability to certify in time for contract competitions.

Integrate legal and technical strategy. CMMC compliance is not solely an IT implementation project. It

encompasses contract compliance, risk allocation, representation and warranty exposure, and False Claims Act risk. Legal counsel should be involved in assessing current certifications, establishing voluntary self-disclosure protocols, and evaluating vendor and subcontractor flow-down obligations.

Extend due diligence to the supply chain. Prime contractors bear responsibility for subcontractor compliance. Evaluate your vendors' cybersecurity posture and incorporate appropriate contractual controls.

Conclusion

The shift underway is significant. CMMC requirements become enforceable in contracts starting November 2025, with third-party certification mandatory for many contractors by November 2026. Non-compliance results in loss of eligibility for federal contracts. Requirements flow down to subcontractors. And the DOJ's enforcement posture has moved cyber compliance from a regulatory concern to an active litigation risk.

For business leaders, the framing should be clear: this is not a compliance burden to minimize, it is a business eligibility requirement that separates qualified contractors from disqualified ones. Organizations that invest in genuine readiness will be positioned both to pass CMMC audits and to withstand the DOJ's misrepresentation standard. Organizations that treat certification as a paperwork exercise are building the fact patterns for the next round of settlements.

If you have questions or would like more information, please contact Jade Davis.

Shumaker