CMMC Phase 1 Realities:

Addressing the Technical Documentation and Scoping Gaps Identified by the GAO

David W. Koran

CyberAB Registered Practitioner Advanced

April 2026

The Gap

The GAO published GAO-26-107955 on March 12, 2026. The report found that DoD has not systematically assessed the external factors that could prevent the CMMC program from meeting its goals, including whether there are enough C3PAOs to meet certification demand. While that represents a systemic program risk, the more immediate concern is what contractors are actually bringing to the table when they attempt certification.

Industry survey data quantifies the micro problem. The CyberSheath State of the DIB Report 2025, conducted by Merrill Research and published in October 2025, surveyed 300 defense contractors and found that only 1% reported full readiness for CMMC. The median SPRS score was 60, against a required 110. Only 30% had completed validated medium or high assessments that would confirm their actual security posture. And 17% were still carrying negative SPRS scores. Meanwhile, 69% claimed compliance through self-assessment alone.

Greenberg Traurig reported in October 2025 that third-party assessors estimate 25% of companies seeking certification have experienced false starts due to failed pre-assessments, meaning the assessor was unable to validate the contractor's readiness to advance to the actual certification. The consequences of a failed pre-assessment are not minor. Greenberg Traurig noted that the C3PAO must report an adverse readiness determination in the Enterprise Mission Assurance Support

Service (eMASS), creating a documented record of the contractor's unpreparedness.

The distance between self-reported compliance and verifiable implementation is the gap. It is driven by two specific, correctable technical deficiencies: incomplete System Security Plans and poorly defined asset scoping.

Incomplete System Security Plans

The SSP is the primary document a C3PAO evaluates during a Level 2 certification. Under CMMC practice CA.L2-3.12.4, it must describe system boundaries, the environment of operation, how each of the 110 NIST SP 800-171 controls is implemented, and the relationships with connected systems. The SSP functions as an implementation record, not a policy statement, and a C3PAO will evaluate it as such.

In practice, most SSPs across the DIB do not meet this standard. The National Defense Industrial Association noted in a July 2024 presentation that nearly all SSPs encountered in the field were inadequate to meet requirements. C3PAOs have reported that assessment delays and failures stem most often from incomplete SSPs, unclear control narratives, and insufficient objective evidence, not from missing technology.

The GRC Tool Problem

A significant contributor to SSP inadequacy is organizational misalignment. In many small and mid-sized contractors, CMMC compliance is handed to the IT department as a technology problem. IT, in turn, purchases a Governance, Risk, and Compliance (GRC) platform to manage the effort. The GRC tool provides a structured way to track control status, assign ownership, and store evidence artifacts, but it does not produce a System Security Plan.

ISI Security, in a March 2026 analysis of GRC platform utility for CMMC, stated the problem directly: tools do not create compliance, and without repeatable processes for evidence collection and SSP updates, a GRC platform becomes a repository of

incomplete or outdated artifacts. The distinction between a control inventory and a System Security Plan is critical here. A GRC platform generates a control inventory: a list of requirements, their implementation status, and associated evidence references. That is useful for internal tracking, but it is not what a C3PAO evaluates. The SSP must be a cohesive, narrative document that describes the contractor's specific environment, how each control is implemented within that environment, what technologies and procedures support it, who is responsible for operating and maintaining it, and how the organization demonstrates implementation through verifiable evidence.

The technical shortcomings of many GRC platforms compound this gap. Matthew Titcombe of Peak InfoSec, writing from the perspective of a C3PAO evaluating GRC tools for CMMC assessment support, identified a structural deficiency: most GRC platforms do not evaluate compliance at the NIST SP 800-171A assessment objective level. NIST SP 800-171 contains 110 security requirements, but each requirement is further decomposed into multiple assessment objectives, totaling 320 individual objectives. Compliance is measured first at the assessment objective level and then rolled up to the requirement level. Many GRC tools either do not reach that depth or present objectives as simple task checklists rather than compliance determinations tied to specific systems and evidence artifacts.

The result is a predictable failure pattern. The IT department populates the GRC tool, marks controls as implemented based on the tool's framework mapping, and reports readiness to leadership. Leadership, relying on the GRC status dashboard, signs the SPRS affirmation. When the C3PAO requests the SSP, the organization either exports the GRC data into a document that reads like a spreadsheet with paragraphs, or presents a template SSP that was never customized to reflect the actual environment. In either case, the assessor cannot validate the controls because the document does not describe the system it is supposed to represent. CyberSheath's Rich Baron, SVP of Operations, summarized the pattern in a February 2026 webinar: compliance is not something you buy, and technology enables compliance but does not create it.

CMMC Is Not an IT Project

CyberSheath's legal risk analysis in February 2026 stated it plainly: CMMC compliance is not just an IT project, it is a legal exposure point, and all departments need to understand their roles within the process, including procurement, contracts, IT and security, and legal. ISI Security, in a December 2025 guide for in-house IT departments approaching CMMC, reinforced the same finding: CMMC introduces formal role separation, evidence requirements, and governance expectations that can conflict with day-to-day operational realities.

The controls that depend on non-IT functions illustrate why. Access control policies involve hiring and termination procedures. Physical security controls involve facility management. Incident response plans involve legal notification obligations. Media protection controls involve records management. When the entire effort is delegated to IT and filtered through a GRC tool, the controls that require input from operations, human resources, physical security, and legal counsel are either undocumented or documented generically. The SSP reflects that gap, and the C3PAO is required to identify it.

The Affirmation Consequence

The SPRS affirmation requires a senior executive to attest, under 32 CFR §170.22, that the organization has implemented and will maintain implementation of all applicable CMMC security requirements. An SSP that does not reflect the contractor's actual environment means the affirmation does not reflect reality. Under the False Claims Act (31 U.S.C. §3729), liability attaches not only to actual knowledge of falsity, but to deliberate ignorance and reckless disregard. An executive who signs an affirmation based on a GRC dashboard without verifying that the underlying SSP accurately describes the organization's implementation is operating within that standard.

Poorly Defined Asset Scoping

Scoping determines what the SSP must cover. It is the process of identifying every system, network segment, user, and facility that processes, stores, or transmits CUI,

then classifying each asset as a CUI Asset, Security Protection Asset, Contractor Risk Managed Asset, or Specialized Asset. Each classification carries different control obligations. Inaccurate scoping undermines every element of the compliance program that depends on it.

Two failure modes result. Underscoping excludes CUI-processing systems from the assessment boundary. The C3PAO identifies the gap, and the contractor either fails or must halt for remediation. Overscoping pulls non-CUI systems into the boundary, inflating cost, extending timelines, and multiplying the documentation burden with no corresponding security benefit.

Both failures originate from the same deficiency: the contractor has not performed a data flow analysis. Without tracing how CUI enters the environment, where it moves internally, where it is stored, and how it exits, the assessment boundary is a guess. An SSP built on a guess is incomplete by definition. The organization cannot document what it has not identified.

This compounds in environments that rely on external service providers. If a contractor's email, file storage, or endpoint management is handled by an MSP or cloud provider, the SSP must document which controls are inherited, which are shared, and which remain the contractor's responsibility. Without that analysis, the SSP contains gaps the assessor is required to flag.

Contract Eligibility and Legal Exposure

Since November 10, 2025, contracting officers are required to verify that an offeror has a current CMMC status in SPRS at the required level before making a contract award. Without a current status, the contracting officer cannot make the award. The technical deficiencies described above therefore function as procurement disqualifiers, not compliance technicalities.

The legal exposure compounds the procurement risk. The DOJ's Civil Cyber-Fraud Initiative settled seven cybersecurity-related False Claims Act cases in 2025, recovering more than $52 million across cybersecurity FCA settlements during fiscal year 2025. The cases demonstrate the breadth and escalation of enforcement.

In April 2025, Morse Corp agreed to pay $4.6 million to resolve allegations that it submitted a false SPRS score. According to the settlement, the contractor reported a positive cybersecurity assessment score when its actual score was negative 142. It did not correct the score until three months after receiving a DOJ subpoena. In July 2025, Raytheon Company, RTX Corporation, and Nightwing Group agreed to pay $8.4 million to resolve allegations of noncompliance with cybersecurity requirements. The acquiring entity was explicitly named as successor in liability for preacquisition cybersecurity deficiencies, establishing that FCA exposure transfers through acquisition. In September 2025, Georgia Tech Research Corporation paid $875,000 for a false SPRS score and failure to install anti-malware tools on systems handling CUI.

In December 2025, the DOJ announced its first enforcement action targeting the defense supply chain. Swiss Automation Inc., an Illinois precision machining company, agreed to pay $421,234 to resolve allegations that it failed to provide adequate cybersecurity protections for technical drawings supplied to DoD prime contractors. The case originated as a qui tam action filed by Jaime Gomez, a former quality control manager at Swiss Automation, who received $65,291 as his share of the recovery.

Phase 2 introduces a second dataset. When C3PAO assessment results begin populating SPRS alongside self-assessed scores, the government will be able to compare the two. Significant discrepancies between what a contractor claimed and what an independent assessor verified will become measurable triggers for investigation. Deputy Assistant Attorney General Brenna Jenny stated in January 2026 that cyber-fraud cases are not about data breaches but are instead premised on misrepresentations. The contractors with the greatest exposure are those whose recorded claims and actual results do not align, rather than those who simply fail an assessment.

Phase 2 Timeline: Seven Months

Phase 2 begins November 10, 2026. At that point, C3PAO-assessed Level 2 certification will be required in applicable solicitations involving CUI. As of December 2025, the Cyber AB had authorized 92 C3PAOs to conduct Level 2

assessments. The estimated contractor population requiring Level 2 certification is approximately 80,000. Assessment backlogs are already measured in months.

The preparation timeline for Level 2 certification runs 6 to 18 months depending on organizational complexity. That means the effective deadline for starting preparation has already passed for many organizations. Contractors who have not completed their data flow analysis, defined their assessment scope, and built a complete, environment-specific SSP by mid-2026 will not be in a position to engage a C3PAO before Phase 2 solicitations begin appearing.

The sequence is fixed: data flow analysis, scope definition, SSP development, gap analysis against the CMMC Assessment Guide v2.13, remediation of identified gaps, and C3PAO engagement. Skipping steps does not accelerate the process. It defers deficiencies to the assessment, where they are more expensive to resolve and carry procurement consequences.

The data from the GAO, CyberSheath, and Greenberg Traurig all point to the same conclusion. The majority of the defense industrial base is not ready. The two primary reasons, incomplete SSPs and undefined scoping, are technical problems with known solutions. The solution is not purchasing a GRC tool but rather building an accurate, environment-specific SSP informed by a thorough data flow analysis, with input from every function that touches a CMMC control. What that work requires most is lead time, and that resource is narrowing.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced (RPA) and the founder of David Koran & Associates Inc., a CMMC compliance consulting firm serving Defense Industrial Base contractors and their legal counsel. His practice focuses on readiness, enablement, and implementation services for organizations preparing for CMMC Level 2 certification. He is an Associate Member of the ABA Section of Public Contract Law and the author of *The CMMC Decision*. He can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

Government Accountability Office. *Defense Contractor Cybersecurity: DOD Should Address External Factors That Could Impede Program Implementation* (GAO-26-107955). March 12, 2026. https://www.gao.gov/products/gao-26-107955.

CyberSheath / Merrill Research. *State of the DIB Report 2025*. October 2025. https://cybersheath.com/resources/blog/state-of-the-dib-report-2025-only-1-of-contractors-are-ready-for-cmmc/.

Greenberg Traurig LLP. "Preparing for a CMMC Audit: The System Security Plan." October 22, 2025. https://www.gtlaw.com/en/insights/2025/10/preparing-for-a-cmmc-audit-the-system-security-plan.

Department of Defense. 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Final Rule, effective December 16, 2024.

Department of Defense. DFARS 252.204-7021. Effective November 10, 2025.

NIST SP 800-171, Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. February 2020.

Department of Defense. *CMMC Assessment Guide: Level 2*, Version 2.13.

Holland & Knight. "CMMC Affirmation Trap: FCA Exposure for Defense Contractors and Acquirers." January 23, 2026. https://www.hklaw.com/en/insights/publications/2026/01/cmmc-affirmation-trap-fca-exposure.

U.S. Department of Justice. "Illinois Precision Machining Company Agrees to Pay $421,234 to Resolve Alleged False Claims Act Violations." December 5, 2025. https://www.justice.gov/opa/pr/illinois-precision-machining-company-agrees-pay-421234-resolve-alleged-false-claims-act.

U.S. Department of Justice. "Raytheon Companies and Nightwing Group to Pay $8.4M to Resolve False Claims Act Allegations." July 3, 2025.

https://www.justice.gov/opa/pr/raytheon-companies-and-nightwing-group-pay-84m-resolve-false-claims-act-allegations-relating.

Mayer Brown. "False Claims Act Enforcement: Record-Breaking Year Signals Continued Attention to Cybersecurity." March 2026. https://www.mayerbrown.com/en/insights/publications/2026/03/false-claims-act-enforcement-record-breaking-year-signals-continued-attention-to-cybersecurity.

ISI Security. "Do You Really Need a GRC Platform for CMMC?" March 2026. https://isidefense.com/blog/do-you-really-need-a-grc-platform-for-cmmc.

ISI Security. "An In-House IT Department's Guide to Approaching CMMC Compliance." December 23, 2025. https://isidefense.com/blog/an-in-house-it-departments-guide-to-approaching-cmmc-compliance.

Peak InfoSec / Matthew Titcombe. "Why CMMC Related GRC Tools (as far as I know) are missing the target." LinkedIn. https://www.linkedin.com/pulse/why-cmmc-related-grc-tools-far-i-know-missing-target-matthew-titcombe.

CyberSheath. "Navigating the Path to CMMC Compliance: A Buyer's Guide" (webinar recap). February 27, 2026. https://cybersheath.com/resources/blog/navigating-cmmc-compliance/.

CyberSheath. "CMMC 2.0 Legal Risks: Why Compliance Protects Your Business." February 16, 2026. https://cybersheath.com/resources/blog/cmmc-legal-risks-compliance-protects-business/.

National Defense Industrial Association. "CMMC Updates & Building a System Security Plan." Presentation, July 2024. https://www.ndia.org/-/media/sites/ndia/policy/cmmc/webinars/presentations/2024/cmmc-for-july-2024-final.pdf.