CENTER FOR COMPETITIVE STATECRAFT AND STRATEGIC POLICY

CMMC Level 2 Readiness Risk in the U.S. Defense Industrial Base

Evidence, Drivers, and a 90-Day Remediation Path

Author	Collin George, CISSP
Date	March 2026
Contact	cgeorge@collinbgeorge.com
ORCID	0009-0007-8162-6839
Status	Unclassified // Open Source // Independent Analysis

1. Executive Summary

This assessment examines the risk that small and mid-sized firms in the U.S. Defense Industrial Base will fail to achieve CMMC Level 2 certification within the enforcement timeline established by the DFARS acquisition rule effective November 10, 2025. Key Judgments are derived from public reporting, regulatory filings, NIST framework analysis, and industry survey data.

1 **HIGH CONFIDENCE**
Available evidence is consistent with the judgment that a non-trivial proportion of small and mid-sized defense contractors may not achieve CMMC Level 2 readiness without structured external remediation. One industry survey (Merrill Research/CyberSheath, October 2024) reported that approximately 4% of respondents described themselves as fully prepared, and the average self-reported SPRS score among respondents stood at -12 against a required threshold of 88 for conditional certification.

2 **HIGH CONFIDENCE**
The primary failure drivers appear to be documentation deficiency (incomplete or absent System Security Plans), control implementation gaps (particularly in access control, audit logging, and media protection), and audit preparation failure (inability to produce demonstrable evidence of control implementation). Available evidence suggests these are structural rather than episodic.

3 **HIGH CONFIDENCE**
The gap between self-reported compliance and actual assessment readiness is assessed as significant. NIST SP 800-171 controls have been contractually required since 2017 via DFARS 252.204-7012, yet public reporting through 2025 indicates persistent non-compliance across the DIB. Public reporting indicated that approximately 270 organizations had received final CMMC Level 2 certification by August 2025, against an addressable population exceeding 220,000 firms.

4 **MODERATE CONFIDENCE**
The enforcement timeline creates compounding pressure. Phase 2 (mandatory C3PAO assessment for applicable Level 2 contracts) is projected to begin in November 2026. Typical remediation timelines of 12–18 months and C3PAO scheduling backlogs of 3–6 months suggest that contractors who have not initiated gap assessment by mid-2026 face elevated risk of contract ineligibility during the 2026–2027 contract cycle. Enforcement tempo may vary by contracting office.

5 **HIGH CONFIDENCE**
Non-compliance consequences extend beyond contract loss. The False Claims Act creates potential civil liability for contractors who submit inaccurate SPRS self-assessments. Prime contractor supply chain pressure is accelerating independently of government enforcement, with major primes already requiring subcontractors to demonstrate CMMC readiness as a condition of inclusion in bids.

6 **MODERATE CONFIDENCE**
A structured 90-day readiness engagement — encompassing gap assessment, documentation development, control remediation, and evidence preparation — is consistent

with the minimum viable approach to achieve assessment readiness for organizations starting from a moderate baseline (SPRS score of 40–80). Organizations with scores below 40 or with significant infrastructure deficiencies are likely to require longer remediation timelines.

7 ASSESSMENT LIMITATION

Several material unknowns constrain the precision of this assessment: true baseline readiness rates across the full DIB population, C3PAO capacity relative to demand, enforcement variability across contracting offices, and the degree to which prime contractor pressure will substitute for or accelerate government enforcement. These unknowns are addressed in Section 7.

2. Scope and Methodology

2.1 Sources

This assessment draws on the following source categories:

- NIST Special Publication 800-171 Revision 2 (primary control framework for CMMC Level 2) [Tier 1]
- CMMC Final Rule (32 CFR, published October 15, 2024) and DFARS acquisition rule (48 CFR, effective November 10, 2025) [Tier 1]
- SPRS portal documentation and scoring methodology (Defense Logistics Agency) [Tier 1]
- Industry survey data: CyberSheath/Merrill Research, October 2024 [Tier 2 — commissioned study; sample methodology not fully disclosed]
- Public reporting from C3PAO organizations, compliance consulting firms, and defense trade press through March 2026 [Tier 2/3]
- Congressional Research Service reports on the Defense Industrial Base (IF10548, R47751) [Tier 1]
- Department of Defense Office of Small Business Programs data [Tier 1]

2.2 Methodology

This assessment uses observational analysis (reported readiness metrics), inferential analysis (extrapolation from available data to broader DIB population), and framework analysis (mapping observed deficiency patterns against NIST SP 800-171 control families). All inferential conclusions are explicitly labeled. No classified, proprietary, or non-public assessment data was used.

2.3 Limitations of the Public Record

This assessment is subject to several material limitations:

- No access to aggregated SPRS score data across the full DIB population. The -12 average score cited is drawn from a single industry survey and should be interpreted as indicative rather than definitive.

- No access to C3PAO assessment results, pass/fail rates, or common deficiency findings.
- Enforcement tempo and contracting officer discretion in applying CMMC requirements may vary significantly.
- Industry survey data may reflect selection bias (firms engaging with compliance vendors may be more or less prepared than non-respondents).

Where evidence is insufficient to support a judgment, the assessment identifies the gap rather than filling it with inference.

3. Observed Conditions in the Defense Industrial Base

The following observations are descriptive. Analytical conclusions are reserved for Section 4.

3.1 Readiness Metrics

An October 2024 industry survey conducted by Merrill Research and commissioned by CyberSheath reported that the average SPRS score among respondents was -12. The survey sample size and methodology were not fully disclosed in public reporting; the figure should be interpreted as indicative rather than definitive. The SPRS scoring range extends from -203 (no controls implemented) to +110 (full compliance). A minimum score of 88 is required for conditional CMMC Level 2 certification.

The same survey reported that approximately 4% of respondents described themselves as fully prepared for CMMC certification.

By August 2025, public reporting indicated that approximately 270 organizations had received final CMMC Level 2 certification through C3PAO assessment, against an addressable DIB population exceeding 220,000 firms. This figure had likely increased by the time of this assessment, but no comprehensive public count was available as of March 2026.

3.2 Documentation Deficiencies

Public reporting from C3PAO organizations and compliance consultants consistently identifies documentation as the most common deficiency category:

- System Security Plans (SSPs) that are absent, incomplete, or based on generic templates not tailored to the organization’s actual system boundaries and control implementations
- Plans of Action and Milestones (POA&Ms) that lack specificity, ownership assignments, or realistic completion timelines
- CUI boundary documentation that does not accurately map where Controlled Unclassified Information is stored, processed, and transmitted
- Evidence artifacts that are not collected, organized, or indexed in a manner suitable for C3PAO review

3.3 Control Implementation Gaps

Reported control implementation gaps cluster in several NIST SP 800-171 control families:

- Access Control (3.1.x): Role-based access not implemented, over-permissive privilege assignments, shared account usage
- Audit and Accountability (3.3.x): Audit logging not enabled across all CUI-touching systems, no centralized log aggregation, audit records not reviewed
- Configuration Management (3.4.x): Baseline configurations not established, unauthorized software present, change management informal or absent
- Identification and Authentication (3.5.x): Multi-factor authentication not implemented for all remote and privileged access
- Media Protection (3.8.x): Removable media controls not implemented, CUI not encrypted on portable devices
- System and Communications Protection (3.13.x): CUI not encrypted in transit, network segmentation insufficient

3.4 Audit Preparation Gaps

Compliance practitioners report a distinct deficiency category: organizations that have partially implemented controls but cannot demonstrate implementation to a C3PAO assessor:

- Controls technically in place but not documented in the SSP
- Evidence that exists but is not organized or retrievable within assessment timelines
- Staff who implement controls operationally but cannot describe them in assessment interviews
- No mock assessment conducted prior to engaging a C3PAO

4. Assessment: Failure Drivers

Each analytical statement below is accompanied by its evidence basis, identified limitations, and confidence level.

4.1 Under-Resourced IT Environments

Available evidence suggests that many small defense contractors (50–500 employees) operate IT environments managed by limited generalist staff whose primary responsibilities are operational. These staff typically lack specialized training in NIST SP 800-171 control implementation, assessment methodology, or compliance documentation standards.

Evidence basis:

Congressional Research Service reporting identifies small businesses as comprising 73% of the DIB [Tier 1 — CRS IF10548]. Public reporting from compliance consultants describes SMB IT teams as lacking CMMC-specific expertise [Tier 2/3]. The average SPRS score of -12 is consistent with environments where controls are largely unimplemented.

Limitation:

This assessment infers IT staffing patterns from industry-wide reporting. Individual firm capabilities may vary significantly. (Moderate confidence)

4.2 Misinterpretation of NIST SP 800-171 Controls

Public reporting is consistent with the judgment that a non-trivial proportion of DIB contractors misinterpret NIST SP 800-171 control requirements, either by applying controls at insufficient depth, conflating compliance with general cybersecurity hygiene, or assuming that commercial product certifications satisfy contractor-level control responsibilities.

Evidence basis:

Compliance practitioners report that organizations frequently conflate the use of a GCC High-licensed Microsoft 365 environment with full control implementation, when the platform satisfies only a subset of the 110 controls [Tier 2/3 — practitioner reporting].

Limitation:

The prevalence of this misinterpretation across the full DIB population cannot be established from available evidence. (Moderate confidence)

4.3 Absence of Integrated Compliance Ownership

Available evidence suggests that many SMB defense contractors lack a single individual or function with clear ownership of CMMC compliance. Responsibility is typically distributed informally across IT, operations, and executive leadership, with no formal accountability structure or progress reporting cadence.

This condition appears to contribute to delayed remediation timelines, incomplete evidence collection, and inconsistent prioritization of compliance activities relative to operational demands. (Moderate confidence)

4.4 False Claims Act Exposure

An additional risk factor identified in public reporting is the potential for False Claims Act liability arising from inaccurate SPRS self-assessments. Under the CMMC framework, a senior official must submit an annual affirmation of compliance. Organizations that submit inflated SPRS scores face potential civil liability under 31 U.S.C. §3729–3733.

Limited public reporting indicates that enforcement interest in this vector may be increasing. (Low confidence — limited enforcement data available as of March 2026)

5. Common Failure Modes and Required Evidence

The following table maps observed failure patterns against evidence required for C3PAO assessment. Patterns reflect those most frequently cited in public practitioner reporting.

Control Family	Common Failure Mode	Required Evidence	Priority	Assessment Impact

Access Control (3.1)	Over-permissive roles; shared accounts; no access matrix	Access matrix; least-privilege evidence; account audit logs	Critical (5-pt)	Likely assessment failure if unremediated
Audit & Accountability (3.3)	No centralized logging; logs not reviewed or retained	SIEM output; review cadence; retention policy; alert config	Critical (5-pt)	Likely assessment failure if unremediated
Configuration Mgmt (3.4)	No baselines; unauthorized software; informal change mgmt	Baseline configs; software inventory; change mgmt logs	High (3-pt)	Conditional finding; POA&M required
ID & Auth (3.5)	No MFA for remote/privileged access; weak password enforcement	MFA config evidence; password policy enforcement screenshots	Critical (5-pt)	Likely assessment failure if unremediated
Media Protection (3.8)	No removable media controls; CUI unencrypted on portables	Media policy; encryption evidence; sanitization logs	High (3-pt)	Conditional finding; POA&M required
Sys & Comm Protection (3.13)	CUI unencrypted in transit; insufficient segmentation	Network diagrams; encryption verification; firewall rules	Critical (5-pt)	Likely assessment failure if unremediated
SSP / POA&M (Cross-cutting)	SSP absent or generic; POA&M lacks specificity	Tailored SSP; POA&M with owners, milestones, dates	Mandatory	Assessment cannot proceed without SSP

5.5 Assessment Failure Conditions

Based on the CMMC assessment methodology and publicly available C3PAO guidance, the following conditions are assessed as likely to result in assessment failure or conditional denial if present at the time of C3PAO engagement:

- Absent System Security Plan: A C3PAO assessment cannot proceed without a current, tailored SSP. Organizations that present for assessment without a completed SSP face immediate procedural failure.
- No multi-factor authentication on remote or privileged access: MFA is a critical (5-point) control. Absence of MFA is consistently identified in practitioner reporting as a high-probability failure point.

- No centralized audit logging or evidence of log review: Without centralized logging and documented review procedures, organizations cannot demonstrate compliance with Audit and Accountability controls.
- Evidence not collected or not retrievable: Controls that are technically implemented but cannot be demonstrated through organized, indexed evidence artifacts are treated as not implemented for scoring purposes.
- CUI boundary not defined or documented: If the organization cannot articulate where CUI resides, how it flows, and what systems touch it, the assessment scope cannot be established.
- SPRS score below 88 with no viable POA&M path: Conditional certification requires a minimum score of 88. Organizations significantly below 88 may not have a viable path to conditional certification without substantial remediation.

The presence of any single condition above is sufficient to produce an assessment outcome below the certification threshold. The presence of multiple conditions simultaneously is consistent with a high probability of assessment failure. (High confidence)

6. Structured 90-Day Readiness Model

The following model describes a structured remediation path from gap assessment to C3PAO assessment readiness. Designed for organizations with a moderate baseline (estimated SPRS 40–80) and functional IT infrastructure. Organizations with lower baselines, significant infrastructure deficiencies, or complex multi-site environments are likely to require extended timelines.

This model describes the analytical structure of a readiness engagement. It does not constitute a guarantee of assessment outcome.

6.1 Phase 1: Gap Assessment and Baseline (Days 0–30)

1. Map all 110 NIST SP 800-171 Rev 2 controls against current systems, policies, and procedures using a structured control assessment workbook (e.g., NIST SP 800-171A assessment procedures)
2. Identify all non-inherited controls requiring organizational implementation
3. Document the CUI boundary: where CUI is received, stored, processed, transmitted, and disposed of; produce network diagrams (e.g., Visio, draw.io) showing all CUI data flows and system interconnections
4. Produce a gap matrix scoring each control as Implemented, Partially Implemented, Not Implemented, or Not Applicable
5. Calculate current SPRS score from the gap matrix
6. Draft or review the System Security Plan (SSP) to reflect the actual system boundary and control implementations
7. Identify ITAR-controlled data flows where applicable and assess handling controls against export control requirements

Deliverables:

Gap assessment matrix, SPRS score calculation, SSP baseline draft, CUI boundary diagram, remediation priority ranking.

6.2 Phase 2: Control Remediation and Policy Alignment (Days 30–60)

1. Remediate critical (5-point) controls first, then high (3-point), then standard (1-point). Critical controls account for approximately 55 of the total 110 SPRS points.
2. Implement access control matrices with documented role-based assignments and least-privilege enforcement
3. Deploy or configure centralized audit logging across all CUI-touching systems (e.g., Microsoft Sentinel, Splunk, Elastic SIEM, or equivalent with log ingestion from all endpoints, servers, and network devices in the CUI boundary)
4. Establish MFA for all remote and privileged access paths (e.g., Microsoft Entra ID Conditional Access, Duo Security, or equivalent phishing-resistant MFA for all VPN, RDP, cloud admin, and privileged local access)
5. Document baseline configurations per system type (e.g., CIS Benchmarks for Windows Server, workstations, network devices) and implement technical change management using ticketing systems with approval workflows
6. Draft or update policies for media protection, incident response, personnel security, and physical access
7. Build POA&M for any controls that cannot be fully remediated within the 60-day window, with named owners, milestones, and 180-day completion targets

Deliverables:

Updated SSP reflecting remediated controls, completed POA&M, updated SPRS score, policy documentation package.

6.3 Phase 3: Evidence Collection, Testing, and Assessment Preparation (Days 60–90)

1. Collect and organize evidence artifacts for each implemented control in a structure aligned with C3PAO assessment methodology
2. Index evidence by control number with cross-references to SSP sections
3. Conduct internal tabletop exercise simulating C3PAO assessment interview questions
4. Test technical controls: run authenticated vulnerability scans (e.g., Tenable Nessus, Qualys), verify MFA enforcement on all required access paths, confirm FIPS 140-2 validated encryption on CUI at rest and in transit, validate SIEM log ingestion completeness
5. Conduct mock assessment or pre-assessment review against all 110 controls
6. Remediate findings from mock assessment
7. Engage C3PAO for scheduling (current wait times reported at 3–6 months; early engagement reduces timeline risk)

Deliverables:

Complete evidence package indexed by control, mock assessment results, final SSP, final POA&M, C3PAO scheduling confirmation.

7. Key Unknowns

The following unknowns constrain the precision of this assessment. They are documented in the interest of analytical transparency.

- True baseline readiness rates: No comprehensive, independently validated data exists on SPRS score distribution across the full 220,000+ firm DIB population. The true proportion of firms at risk of assessment failure is not known with precision.
- C3PAO capacity: The number of authorized C3PAOs and their assessment throughput capacity relative to demand is not fully characterized in public reporting.
- Enforcement variability: The degree to which individual DoD contracting officers will exercise discretion in applying CMMC requirements is not established.
- Prime contractor pressure dynamics: The extent to which major primes are independently enforcing CMMC readiness requirements on subcontractors is reported anecdotally but not systematically quantified.
- Small business exit rates: Analysts have projected 15–20% DIB contraction. The actual exit rate is not yet observable and will depend on enforcement tempo, compliance costs, and available support resources.
- False Claims Act enforcement activity: The frequency and scale of FCA enforcement actions related to SPRS score accuracy is not established in public reporting as of March 2026.

8. Conclusion

Available public evidence is consistent with the judgment that a non-trivial proportion of small and mid-sized DIB firms may not achieve CMMC Level 2 readiness without structured remediation, primarily due to deficiencies in documentation, control implementation fidelity, and audit preparation discipline.

The enforcement timeline — with C3PAO assessments projected to become mandatory for applicable contracts beginning November 2026 — creates a narrowing window for remediation. Organizations that have not initiated structured gap assessment by mid-2026 face elevated risk of contract ineligibility during the 2026–2027 contract cycle.

The risk is structural, not episodic. The underlying NIST SP 800-171 controls have been contractually required since 2017. The persistent readiness gap observed across the DIB suggests that the transition from self-attestation to third-party validation will produce a significant population of firms unable to demonstrate compliance under assessment conditions.

Organizations seeking to reduce assessment risk require structured evaluation of current control posture, documentation completeness, and evidence readiness prior to engaging with a

C3PAO. The 90-day model described in Section 6 represents the minimum viable approach for organizations starting from a moderate baseline.

This assessment does not evaluate individual contractor readiness and should not be interpreted as a determination of compliance status for any specific entity.

Organizations seeking structured readiness diagnostics may contact: cgeorge@collinbgeorge.com

9. Scope and Disclaimer

This document is independent open-source policy research produced by Collin George in a personal capacity. It does not reflect the views or positions of any institution. All analysis is based entirely on publicly available information. No classified or controlled information was used.

This document does not constitute legal advice, operational guidance, or a recommendation to any government authority. Where regulatory interpretation or legal determinations are required, coordination with qualified legal counsel is recommended. No guarantee of assessment outcome is expressed or implied.

END OF DOCUMENT

Collin George • CISSP • collinbgeorge.com • ORCID: 0009-0007-8162-6839
UNCLASSIFIED // OPEN SOURCE // INDEPENDENT ANALYSIS