COALFIRE FEDERAL

CMMC Defense Industrial Base Threat and Assurance Report

Executive Analysis from a Leading C3PAO

Q3 2026 Report

Prepared by Coalfire Federal for Prime Contractors, Subcontractors, Executives, CISOs, Compliance Leaders, and Supply Chain Risk Owners

Contents

Section I: Threat Landscape and Assessment Intelligence

Section II: The Readiness Playbook

Section One

Threat Landscape and Assessment Intelligence

01 Executive Summary

The Defense Industrial Base is facing a convergence of cyber espionage, supply chain exploitation, ransomware, identity compromise, cloud misconfiguration, and rapidly increasing AI-enabled social engineering. **At the same time, the regulatory landscape has shifted.** The Department of War's suspension of CMMC Phase II on July 13, 2026, changes the immediate path to third-party certification. It does not change the threat environment, the contractual obligation to safeguard covered defense information, or the responsibility contractors assume when they represent that cybersecurity requirements have been met. During the interim period, Phase I self-assessment requirements remain in place, and the Department has stated that it will enforce NIST SP 800-171 Rev. 2 through self-assessments and selected government-led assessments. That places greater weight on the accuracy of contractor-generated scores, documentation, and compliance representations. Organizations must be able to support what they report with evidence that reflects actual operations.

From the perspective of Coalfire Federal, a leading C3PAO, the organizations best positioned to manage this risk are those that operationalize cybersecurity and independently test whether their internal view is accurate. They do not treat System Security Plans, POA&Ms, access reviews, incident response, supplier oversight, and evidence collection as paperwork. They run these activities as normal business operations and can demonstrate that they work consistently.

Taken together, this data points to four conclusions for executive decision-makers:

The primary DIB risk is no longer only external intrusion. It is the inability to validate cybersecurity maturity across thousands of suppliers at speed.

Self-assessment preserves flexibility, but it also concentrates responsibility inside the organization. The contractor owns the claim and the consequences if that claim is unsupported.

Identity, third-party access, cloud services, remote administration, CUI sprawl, and poor evidence management remain the dominant assessment and threat exposure areas.

Prime contractors need scalable supplier readiness models. Subcontractors need access to trusted, practical resources that can move them from confusion to certification.

This gap is driving demand for coordinated ecosystems that connect primes and suppliers to a curated network of partners across advisory, cloud, MSP/MSSP, GRC, training, legal, insurance, technology, and assessment support.

Executive Metric	Current Planning Estimate	Executive Implication
Final Level 2 certifications	1,600	Certification velocity must accelerate dramatically.
Estimated Level 2 population	80,000	Most of the DIB remains uncertified and will require support.
Certified percentage	2%	The supply chain is underprepared for scaled enforcement.
Organizations struggling in Phase I	10% to 15%	Scope and evidence readiness are blocking progress.
Highest risk control themes	MFA, CUI boundary, SSP accuracy, supplier risk	Foundational discipline matters more than tool count.

Data as of May 2026

02

Strategic Context for the Defense Industrial Base

> CMMC changes the operating environment because it forces organizations to prove that cybersecurity requirements are implemented.

The DIB includes thousands of organizations that support weapons systems, aerospace, shipbuilding, software, space, advanced manufacturing, engineering, logistics, and critical mission support. Many of these companies handle Federal Contract Information and Controlled Unclassified Information. Adversaries target this ecosystem because they can gain insight into United States defense priorities, military technology, production dependencies, research pipelines, and operational readiness.

On July 13, 2026, the Department of War suspended the transition to CMMC Phase II and pending future implementation milestones while launching a 60-day review. The Department retained all Phase I self-assessment requirements and reaffirmed that contractors and subcontractors remain contractually obligated to safeguard covered defense information under DFARS 252.204-7012.

This changes the immediate business case for third-party assessment. Certification may not be mandated for every organization on the prior timeline, but independent verification remains one of the clearest ways to test whether cybersecurity claims are accurate, evidence is defensible, and documented controls operate as described.

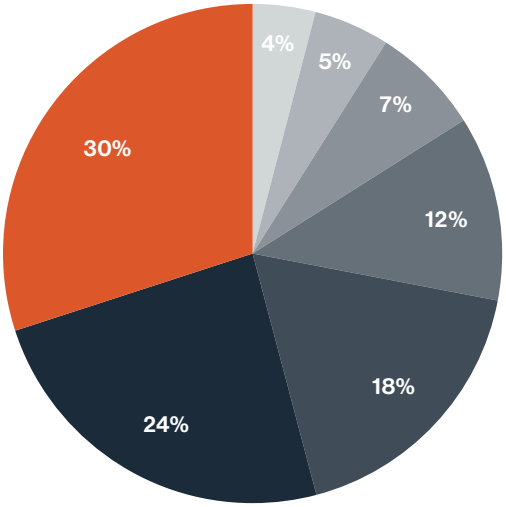
The verification requirement changed. The obligation, threat, and accountability did not.

Strategic Driver	What It Means	Risk to Executives
CMMC Phase II suspension	Third-party certification is no longer expanding on the previously announced timeline, while Phase I self-assessments remain in place.	Organizations may mistake the pause for reduced accountability and rely on compliance claims that have not been independently validated.
CUI supply chain flow down	Primes must understand which suppliers receive, process, store, or transmit CUI.	Supplier gaps can create program delays and cyber exposure.
Nation state targeting	Foreign cyber actors pursue defense IP and program intelligence.	Smaller suppliers may become the path into larger programs.
AI-enabled attacks	Phishing, impersonation, and reconnaissance are becoming faster and more convincing.	Traditional awareness training is insufficient by itself.

03

Threat Vector Distribution

Estimated DIB Threat Vector Distribution



Credential theft / identity abuse	30%
Phishing / Business Email Compromise (BEC)	24%
Supply chain compromise	18%
Ransomware / extortion	12%
Insider threat	7%
Vulnerability exploitation	5%
Other	4%

Figure 1. Estimated distribution of primary threat vectors affecting DIB organizations.

The chart below provides a directional estimate of the most relevant attack vectors affecting DIB organizations. It blends public cyber reporting, C3PAO readiness observations, and the practical attack paths most often encountered across defense contractors.

The key message for executives is that attackers are not relying on one technique. They combine stolen credentials, social engineering, vulnerable systems, supplier access, and ransomware pressure to create multi-stage compromise paths. **None of these attack methods became less effective when Phase II was suspended.**

Threat Vector	Estimated Share	Why It Matters
Credential theft / identity abuse	30%	Legitimate credentials allow attackers to bypass traditional perimeter controls and blend into normal activity.
Phishing / Business Email Compromise (BEC)	24%	AI-generated messages and impersonation make business email compromise harder to detect.
Supply chain compromise	18%	Trusted vendors can become access paths into prime contractor environments.
Ransomware / extortion	12%	Data theft and business disruption create operational and contractual risk.
Insider threat	7%	Insiders can expose CUI intentionally or through negligence.
Vulnerability exploitation	5%	Unpatched external systems remain attractive entry points.
Other	4%	Includes misconfiguration, lost devices, and physical security gaps.

Vulnerability exploitation is now a leading breach entry point, while credential abuse, phishing, and pretexting remain major identity-centered risks. For DIB organizations, this means the executive control agenda must include both identity hardening and vulnerability management. MFA alone is not enough if internet-facing systems remain unpatched, and patching alone is not enough if privileged identities remain weak.

Board-Level Takeaway

Cyber risk remains material regardless of certification timing.

Operational Takeaway

Security teams need continuous asset visibility, credential governance, and rapid remediation workflows.

CMMC / Assurance Takeaway

Access control, identification and authentication, configuration management, audit logging, incident response, and risk assessment must operate together.

04

Top Vulnerabilities Observed During CMMC Readiness

The most common readiness issues are rarely exotic. They are usually foundational control weaknesses that were partially implemented, inconsistently executed, poorly documented, or excluded from scope without sufficient justification. These issues matter even without an immediate certification mandate because they affect both security outcomes and the credibility of self-assessment results.

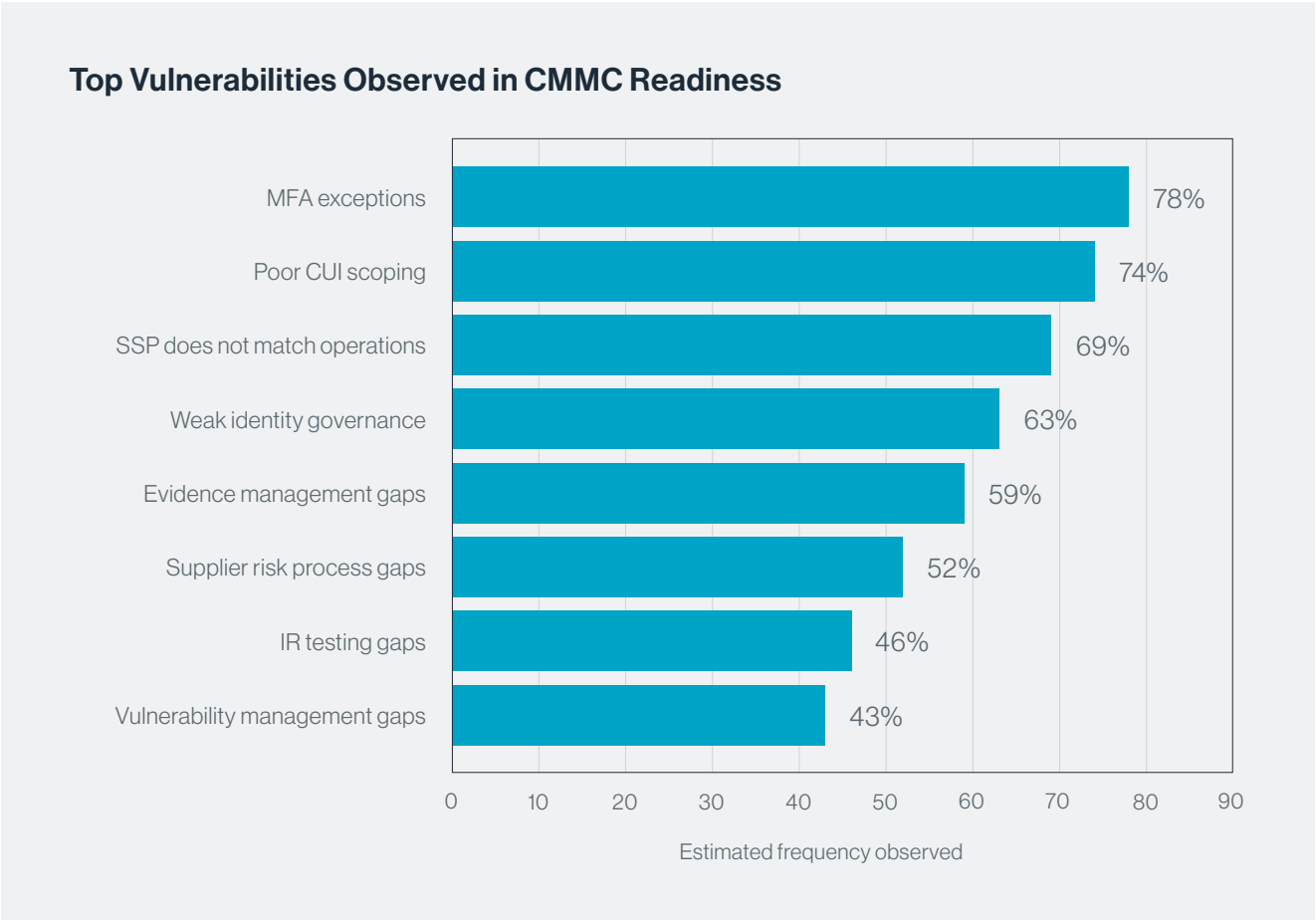


Figure 2. Estimated frequency of common readiness and assessment weaknesses observed in DIB environments.

MFA exceptions

Organizations frequently enable MFA for standard users but leave gaps for administrators, VPN, remote access tools, privileged access management, legacy systems, or third-party portals. These exceptions become the attacker path of least resistance and are difficult to defend during assessment interviews.

Poor CUI scoping

Many organizations cannot clearly show where CUI is stored, processed, or transmitted. Poor scoping either expands the assessment boundary unnecessarily or leaves critical systems out of scope. Both outcomes create risk.

SSP does not match operations

The SSP often describes a desired future state instead of the current operating environment. Assessors look for alignment between the SSP, policies, procedures, interviews, technical evidence, and daily practice.

Weak identity governance

Common issues include dormant accounts, shared administrator access, excessive privileges, missing access reviews, weak Joiner-Mover-Leaver processes, and inconsistent account disablement.

Evidence management gaps

Organizations may perform security activities but fail to retain evidence. Lack of screenshots, tickets, logs, approvals, access reviews, scan results, and meeting records can make implemented controls difficult to prove.

Supplier risk process gaps

Many organizations lack a formal process to identify suppliers that handle CUI, validate their cybersecurity posture, document risk decisions, and monitor changes over time.

Incident response testing gaps

Plans exist, but tabletop exercises, lessons learned, escalation procedures, and external reporting workflows are often immature or untested.

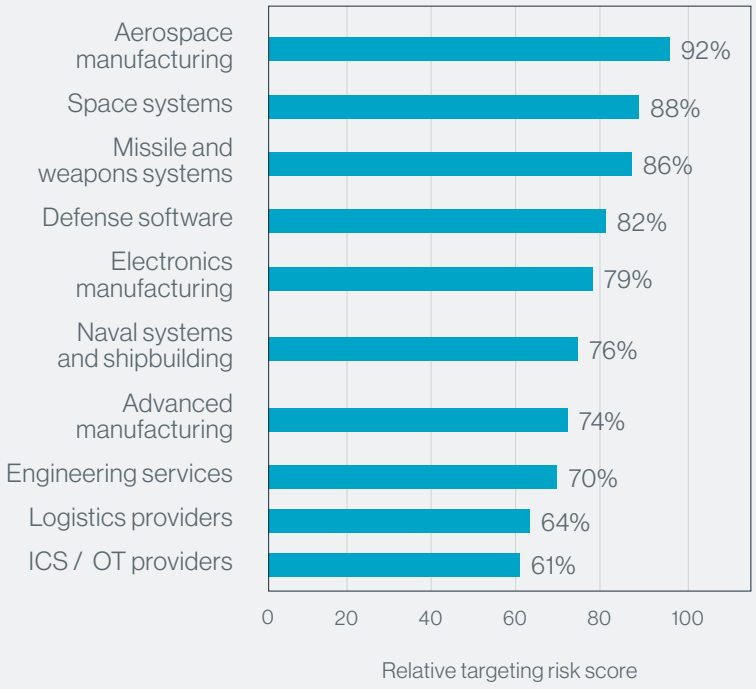
Vulnerability management gaps

Scanning is inconsistent, authenticated scanning is missing, remediation SLAs are not enforced, and exceptions are not risk accepted by leadership.

05

Most Targeted Sectors in the DIB

Most Targeted DIB Sectors



Adversaries prioritize sectors where stolen information can provide military, economic, or geopolitical advantage. Targeting is especially intense where organizations possess engineering data, design drawings, export controlled technical data, weapons system information, advanced manufacturing processes, mission software, satellite communications, or sensitive program schedules.

Small and mid-sized subcontractors remain especially exposed because they often receive sensitive information from primes but do not always have mature security operations, dedicated compliance teams, or established evidence management practices. From a national security perspective, a small supplier with high-value CUI can represent a risk equivalent to a major prime contractor system.

Figure 3. Directional targeting risk score by DIB sector.

Sector	Typical CUI or Sensitive Data	Common Threat Activity
Aerospace manufacturing	Technical drawings, production data, propulsion research	Espionage, supplier compromise, IP theft
Space systems	Satellite design, ground systems, mission operations	Nation-state reconnaissance, cloud attacks, third-party access abuse
Missile and weapons systems	Design files, test data, components, telemetry	Advanced persistent threat activity and long-term collection
Defense software	Source code, DevSecOps pipelines, vulnerability data	Credential theft, repository compromise, CI/CD attacks
Electronics manufacturing	Circuit designs, chips, boards, embedded systems	Counterfeit risk, IP theft, supplier compromise
Naval systems and shipbuilding	Vessel designs, maintenance data, system integration	Espionage, ransomware, supplier targeting
Logistics providers	Movement data, readiness data, supplier records	BEC, ransomware, identity compromise

06

The Independent Assurance Gap

CMMC Level 2 Certification Gap (June 2026)

Comparison of Final Level 2 certifications versus estimated organizations requiring certification.

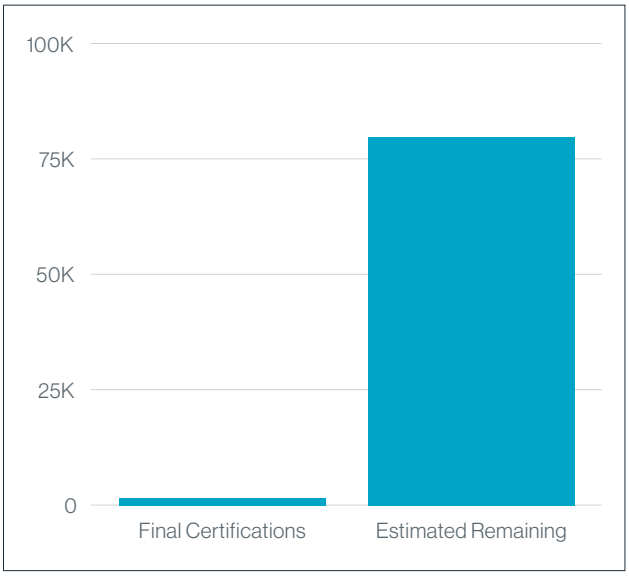


Figure 4. Certified versus estimated remaining CMMC Level 2 population using an 80,000-organization planning estimate.

The CMMC certification gap remains one of the largest strategic challenges facing the Defense Industrial Base. While the number of certified organizations continues to grow, only approximately 2% of the estimated 80,000 organizations expected to require CMMC Level 2 certification have achieved certification. More than 78,400 organizations remain uncertified, creating significant demand for advisory services, managed security providers, governance platforms, evidence automation solutions, and C3PAO assessment capacity.

These figures should be used as planning estimates, not as a definitive count of the final CMMC universe.

The important executive takeaway is that the market is still in the early stages of certification scaling. Demand for qualified advisors, MSPs, MSSPs, cloud providers, GRC platforms, evidence automation, and C3PAO assessment capacity will increase as more contracts require certification.

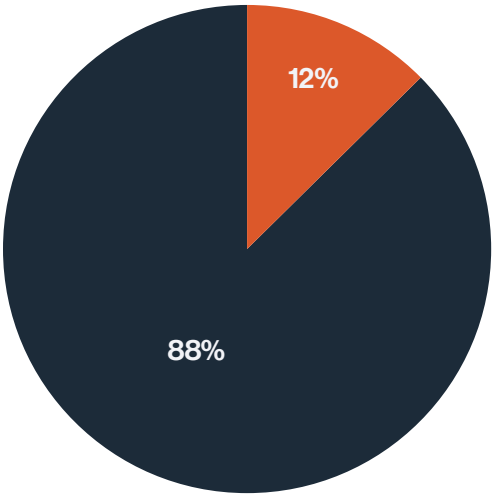
- **Prime contractor implication:** Supplier cyber risk cannot be managed through unverified questionnaires and scores alone. Independent assurance can strengthen supplier segmentation and risk decisions.
- **Subcontractor implication:** An independently validated control environment can provide stronger evidence to primes, customers, boards, insurers, investors, and acquisition partners.
- **Legal and contracts implication:** Contractors remain responsible for the accuracy of representations connected to federal contracts. Verification can reduce the risk of relying on unsupported internal assumptions.
- **C3PAO implication:** Mock and formal third-party assessments can test implementation, evidence, scope, and interview consistency even when certification is not immediately required
- **Readiness implication:** Organizations that maintain defensible evidence and validated control operation will be better positioned for government-led assessments and any future verification model.

07

Self-Assessment Risk and Verification Drivers

A recurring readiness trend is that a meaningful percentage of organizations struggle before reaching deeper evidence and interview review. A practical planning estimate is that 10% to 15% do not move cleanly through early assessment activities without significant corrective work. The leading blockers are usually scope, CUI understanding, missing documentation, and lack of evidence.

Under a self-assessment model, those same weaknesses may remain undiscovered while the organization continues making contractual, customer, or internal representations about its cybersecurity posture. Independent verification creates a structured challenge process before a discrepancy becomes a government finding, customer dispute, cyber incident, whistleblower allegation, or False Claims Act matter.



Phase I Assessment Readiness Outcome

Advance through Phase I	88%
Do not advance cleanly	12%

Figure 5. Estimated Phase I readiness outcome across organizations entering assessment preparation.

Phase 1 Blocker	Observed Pattern	Executive Response
Undefined assessment boundary	Organization cannot clearly identify in-scope systems, users, locations, and external service providers.	Require a CUI data flow and boundary validation workshop before assessment scheduling.
CUI uncertainty	Teams disagree on what information is CUI and where it resides.	Establish a CUI governance function with legal, contracts, program, IT, and security participation.
Incomplete SSP	SSP lacks system details, inheritance, diagrams, external dependencies, or accurate implementation statements.	Treat the SSP as an operational record, not a compliance document.
Insufficient evidence	Controls may exist, but proof is missing or inconsistent.	Create a centralized evidence repository with owners, cadence, and retention expectations.
Process inconsistency	Interviews do not align with policy language or documented procedures.	Run internal mock interviews and reconcile gaps before formal assessment.

08
Key C3PAO Insights

The following insights reflect an assessment-oriented view of what separates mature organizations from organizations that struggle. These are not simply technical observations. They are governance and operating model observations that determine whether cybersecurity practices are sustainable and whether leadership can confidently stand behind the organization's compliance representations.

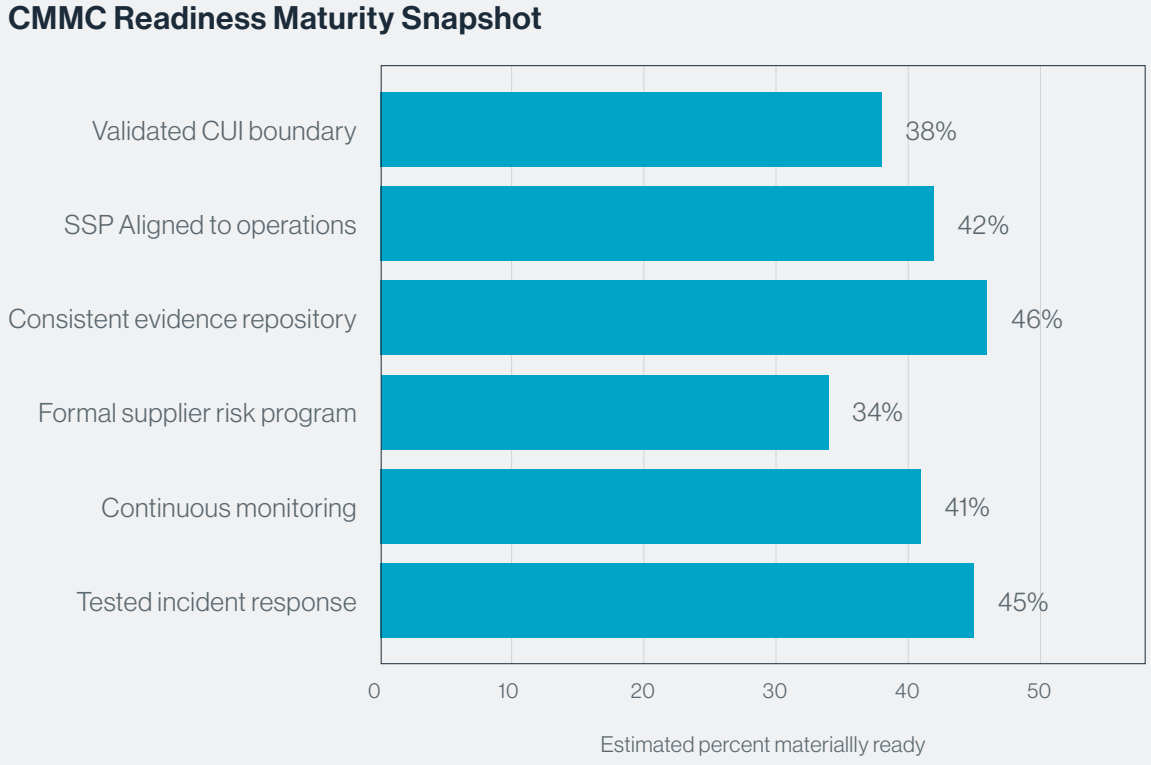


Figure 6. Estimated maturity snapshot across common readiness domains.

Cybersecurity must be operated, not narrated

Independent assurance tests the claim

A self-assessment records the organization's conclusion. An independent assessment challenges that conclusion against evidence, interviews, and operating reality. That distinction becomes more important when third-party certification is optional rather than automatic.

CUI scoping is the foundation of assessment success

When the CUI boundary is unclear, everything becomes harder. Asset inventory, access control, logging, incident response, encryption, external service provider review, and evidence collection all depend on scope clarity.

Evidence management is now a core business process

Organizations need a repeatable evidence process with control owners, collection cadence, quality review, retention rules, and executive oversight. Evidence should be created through normal operations rather than reconstructed after scrutiny begins.

Supplier risk is becoming a prime contractor board issue

Primes cannot protect CUI if they do not understand where it flows across the supplier ecosystem. Supplier cyber maturity, CUI access, flow-down obligations, independent assurance, and escalation paths must be managed centrally.

Technology does not equal maturity

Many organizations have EDR, SIEM, GRC tools, MFA, and vulnerability scanners but still lack effective procedures, accountability, and evidence. Security maturity depends on implementation, not only technology purchases.

> Cybersecurity must be operated, not narrated.

09

Artificial Intelligence and the Future of DIB Cybersecurity

Artificial intelligence will reshape both sides of the DIB cybersecurity equation. Defenders will use AI to automate evidence collection, identify control drift, summarize logs, analyze supplier risk, generate dashboards, and improve security operations. Adversaries will use AI to automate reconnaissance, generate convincing phishing content, impersonate executives, accelerate vulnerability research, and scale social engineering.

The suspension of Phase II does not slow that trajectory. In fact, a longer period of self-assessment may increase the importance of continuous validation because static documentation and annual internal reviews will become less reliable as environments and attack techniques change.

Estimated Growth of AI Enabled Cyber Pressure

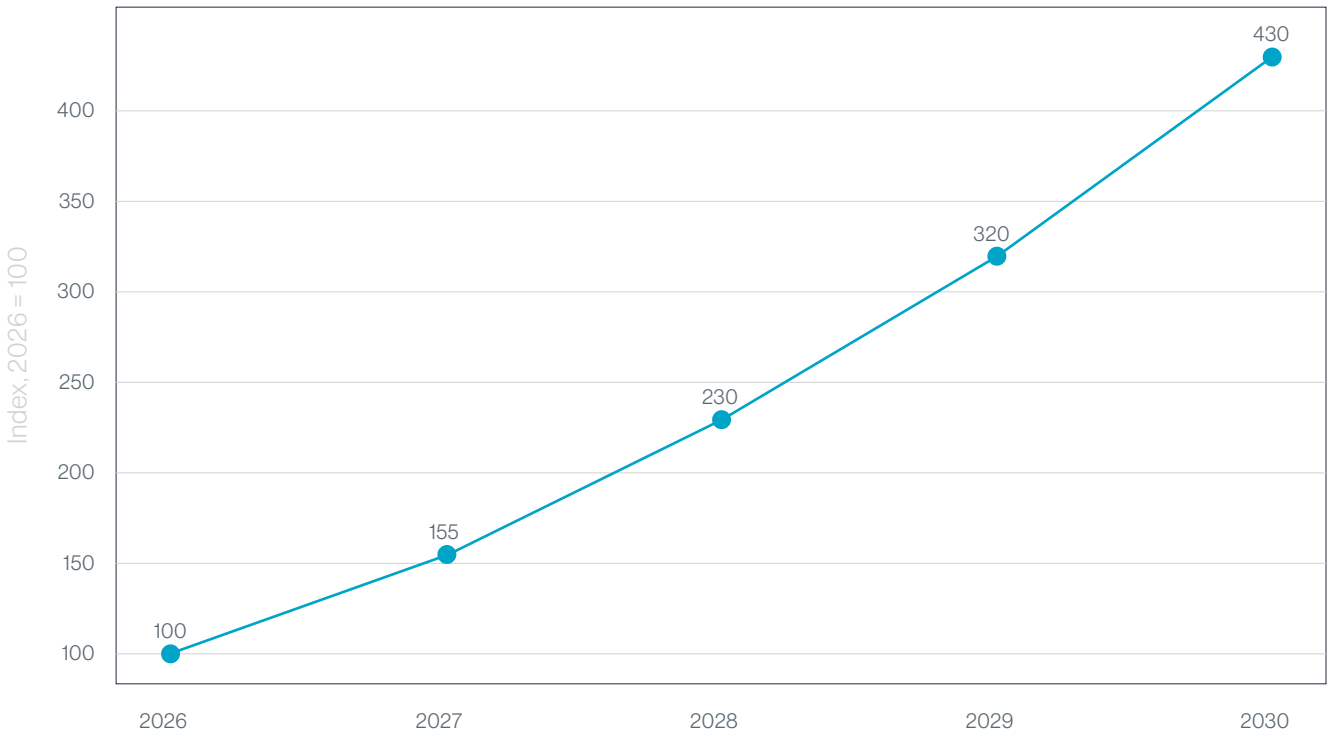


Figure 7. Directional projection of AI-enabled cyber pressure, indexed to 2026.

AI Defensive Use Case	CMMC Value	Executive Caution
Automated evidence collection	Reduces manual evidence burden and improves consistency.	Evidence still requires human validation and ownership.
Continuous control monitoring	Detects drift between documented controls and live operations.	Monitoring must be tuned to the actual CUI boundary.
SSP and policy assistance	Improves drafting speed and crosswalk mapping.	AI-generated documentation must reflect real operations.
Supplier risk scoring	Helps primes triage supplier readiness and criticality.	Scores must not replace supplier engagement and due diligence.
SOC copilot functions	Improves alert triage and investigation speed.	AI outputs need auditability and analyst review.

AI Threat Use Case	Likely DIB Impact	Mitigation Priority
AI phishing and pretexting	More convincing messages to finance, contracts, executives, and program managers.	Stronger identity controls, callback procedures, and user reporting.
Deepfake executive impersonation	Fraudulent payment, data release, or access requests.	Out-of-band verification and executive awareness.
Automated reconnaissance	Faster discovery of exposed services, people, suppliers, and contract data.	Reduce public exposure and improve attack surface management.
Malware and exploit acceleration	More variants and faster weaponization.	Patch velocity, EDR, network segmentation, and detection engineering.

Key Takeaways

AI should be governed as both a productivity enhancer and a data protection risk.

CUI should not be entered into public AI tools unless the tool, contract, and environment are approved for that use.

Organizations should document AI usage policies, approved tools, data handling rules, and monitoring expectations.

Future CMMC readiness will increasingly depend on continuous evidence and control monitoring rather than static documentation.

> CUI should not be entered into public AI tools unless the tool, contract, and environment are approved for that use.

10 Executive Recommendations

Executives should treat CMMC as a risk-management, contractual-integrity, and customer-assurance program. The following recommendations represent the highest-impact actions for organizations handling CUI.

01 | Enforce MFA Across All Systems Without Exception

Identity has become the primary attack vector across the Defense Industrial Base. Attackers increasingly rely on stolen credentials rather than malware to gain access. Every account with access to CUI or administrative privileges should require multifactor authentication.

Priority Actions

- Eliminate MFA exceptions wherever possible.
- Require MFA for cloud consoles, VPNs, privileged accounts, and third-party access.
- Implement privileged access management for administrators.
- Identify legacy systems that cannot support MFA and isolate them through segmentation.
- Monitor authentication logs for abnormal behavior.

Expected Outcome

Reduced risk of credential compromise and improved resilience against phishing and account takeover attacks.

02 | Validate and Minimize CUI Boundaries

Poor scoping increases cost, complexity, security exposure, and the likelihood that internal assessments omit relevant systems or users.

Priority Actions

- Perform CUI discovery exercises.
- Document CUI flows throughout the organization.
- Reduce unnecessary CUI storage locations.
- Segment systems containing CUI from corporate networks.
- Review suppliers and external parties receiving CUI.

Expected Outcome

Smaller assessment scope, lower cost, reduced attack surface, and more efficient assessments.

03 | Build a Supplier Risk Management Program

Supply chain maturity has become one of the largest risks facing prime contractors. Organizations must move beyond spreadsheets and develop repeatable supplier governance processes.

Priority Actions

- Maintain a supplier inventory.
- Identify which suppliers receive CUI.
- Collect and validate cybersecurity evidence.
- Include cybersecurity obligations in contracts.
- Establish escalation procedures for critical suppliers.

Expected Outcome

Improved supply chain resilience and reduced inherited cyber risk.

04 | Shift from Point-in-Time Compliance to Continuous Monitoring

Threat actors operate continuously, while many only when a contract or assessment creates pressure.

Priority Actions

- Deploy SIEM or MDR capabilities.
- Monitor endpoints and identities continuously.
- Conduct vulnerability scanning regularly.
- Centralize cloud logging and alerting.
- Perform periodic tabletop exercises.

Expected Outcome

Improved detection capability, reduced dwell time, and stronger operational resilience.

05 | Make Documentation an Operational Asset

Documentation should support operations, not merely satisfy assessors. Many organizations create policies for assessment purposes that do not reflect actual business practices.

Priority Actions

- Keep SSPs aligned with the current environment.
- Update network diagrams and inventories regularly.
- Maintain evidence throughout the year.
- Ensure procedures are executable by personnel.
- Conduct internal reviews before assessments.

Expected Outcome

Greater consistency, fewer assessment findings, and reduced audit preparation effort.

Executive Perspective

Organizations that achieve successful CMMC certification consistently demonstrate five characteristics:

01 **Identity-first security.**

02 **Clearly defined CUI boundaries.**

03 **Formal supplier risk management.**

04 **Continuous monitoring and detection.**

05 **Documentation that reflects operational reality.**

From the perspective of a C3PAO, organizations that institutionalize these capabilities are not only more likely to achieve certification efficiently but are also better positioned to defend sensitive information and sustain cybersecurity maturity over time.

Section Two

The Readiness Playbook

11 Why CPAN Is Critical for Prime Contractors and Subcontractors

The Phase II suspension increases flexibility, but it also creates a more fragmented assurance environment. Prime contractors must determine which suppliers present material CUI risk, what evidence is sufficient, and when independent verification is warranted. Subcontractors must navigate contractual obligations, technical implementation, customer requests, and changing government expectations without a single mandatory certification trigger.

The CMMC Partner Assurance Network (CPAN) provides a coordinated ecosystem of trusted providers across advisory, cloud, MSP/MSSP, GRC, training, legal, insurance, technology, and independent assessment support. The objective is not to route every organization toward the same service. It is to connect each organization to the capabilities required to protect CUI and produce defensible assurance.

Prime Contractor Challenge	How CPAN Helps	Expected Outcome
Limited visibility into supplier readiness	Connects suppliers to trusted partner categories and readiness resources.	Improved supplier action and reduced uncertainty.
Thousands of suppliers to support	Creates a scalable marketplace-style path rather than one-off referrals.	Lower operational burden on prime teams.
Reliance on unverified supplier claims	Offers access to independent assessment and validation resources.	Greater confidence in supplier representations.
Inconsistent supplier maturity	Supports suppliers at different stages of the CMMC journey.	Faster movement from awareness to remediation.
Contract performance risk	Helps suppliers prepare before certification becomes a contract blocker.	Reduced delays and supply chain disruption.

Subcontractor Need	CPAN Partner Category	Value to Supplier
Understand requirements	Advisory and training	Translate CMMC into an actionable roadmap.
Build secure environment	Cloud service providers and system integrators	Create a controlled boundary for CUI.
Operate security controls	MSP, MSSP, MDR, tool vendors	Support monitoring, response, and daily operations.
Manage evidence	GRC and continuous monitoring platforms	Improve readiness and reduce assessment friction.
Validate cybersecurity claims	C3PAO and compliance support	Prepare for formal assessment activities.
Manage legal and financial risk	Legal and insurance partners	Address contract, liability, and risk transfer issues.

Executive conclusion

CPAN matters because it turns CMMC from a fragmented supplier problem into an organized ecosystem response. It strengthens prime contractor supply chains, gives subcontractors practical paths to readiness, and supports the broader national security objective of protecting CUI across every tier of the DIB.

12

90-Day Executive Action Plan

Executives should move immediately from awareness to action. The following 90-day plan provides a practical path for primes and subcontractors.

Timeframe	Executive Action	Deliverable
Days 1 to 15	Appoint executive sponsor and CMMC program owner. Confirm CUI stakeholders across contracts, legal, IT, security, HR, supply chain, and operations.	CMMC governance charter and accountable owner list.
Days 16 to 30	Map CUI flows, identify in-scope systems, validate external service providers, and define preliminary assessment boundary.	CUI flow diagram, asset inventory, boundary memo.
Days 31 to 45	Review MFA coverage, privileged access, vulnerability management, logging, incident response, and supplier access.	Top risk register and remediation priorities.
Days 46 to 60	Update SSP, POA&M, policies, procedures, and evidence repository structure.	Defensible documentation and evidence baseline.
Days 61 to 75	Conduct mock interviews, evidence review, access review, incident response tabletop, and supplier risk review.	Independent assurance or mock-assessment validation report.
Days 76 to 90	Resolve critical gaps, create certification timeline, and align with advisors or assessment partners as needed.	Executive assurance briefing and assessment roadmap.

Prime contractors should run a parallel supplier readiness workstream during the same period. The supplier workstream should segment suppliers by CUI exposure, program criticality, certification status, known gaps, and potential CPAN support pathways.

13

Board-Level Message Map

Achieving CMMC compliance requires more than implementing cybersecurity controls. It demands coordinated action across the organization, with clear ownership, accountability, and alignment among executive leadership, security teams, legal counsel, supply chain stakeholders, and program managers. Each group plays a distinct role in reducing risk, maintaining eligibility for defense contracts, and supporting certification success.

The following messages can help communicate the importance of CMMC and drive action across key audiences.

Audience	Message	Call to Action
CEO / COO	The certification timeline changed, but cyber, contractual, and reputational exposure did not.	Fund a cross-functional cybersecurity assurance program.
CISO / CIO	Identity, logging, vulnerability management, and evidence consistency are priorities.	Validate control operation inside the CUI boundary.
General Counsel	CUI obligations, flow downs, supplier risk, and false claims exposure require governance.	Review contracts, supplier language, and certification representations.
Supply Chain	Supplier cyber readiness affects contract performance.	Segment suppliers and route them to trusted resources.
Program Managers	CUI handling must be understood at the program level.	Map CUI flows and supplier access by program.
Subcontractors	Waiting creates cost and contract risk.	Start scope, gap assessment, and evidence planning now.

14 Closing Statement

The Defense Industrial Base has entered a period of regulatory uncertainty, not reduced cyber risk. The Department of War suspended CMMC Phase II and initiated a review of the program, but it retained Phase I self-assessments, selected government-led assessments, and the contractual obligation to safeguard covered defense information.

For many organizations, third-party certification is no longer an immediate need-to-have. Independent verification, however, remains a strategically valuable way to determine whether cybersecurity claims can withstand scrutiny. It can surface gaps among the SSP, SPRS score, technical environment, policies, interviews, and evidence before those gaps are identified by a prime contractor, government assessor, customer, whistleblower, incident investigator, or enforcement agency.

This matters because cybersecurity representations carry real consequences. The Department of Justice continues to use the False Claims Act in matters involving government contractors' cybersecurity obligations. The Act can impose treble damages and inflation-linked per-claim penalties when a party knowingly submits false claims or uses false records material to those claims. Independent assessment is not immunity, but it can provide leadership with a stronger factual basis for the decisions and representations made on behalf of the company.

Prime contractors will continue managing cyber risk across their supply chains. Customers will continue asking suppliers to demonstrate that sensitive information is protected. Threat actors will continue targeting credentials, cloud systems, engineering data, and trusted supplier relationships. None of those pressures depends on the timing of CMMC Phase II.

From the perspective of a leading C3PAO, the organizations that will be best positioned are not those that simply wait for the next mandate. They are the organizations that operate cybersecurity as a business discipline, maintain evidence as part of normal operations, and seek objective assurance where the risk justifies it.

Validate What Your Organization Is Claiming

CMMC Phase II may be paused, but the responsibility to protect CUI and support your cybersecurity representations remains. Organizations that complete a C3PAO assessment can objectively validate their cybersecurity posture, identify and remediate gaps before customers find them, and provide greater assurance to prime contractors. As primes increase scrutiny of supplier risk, companies that can demonstrate validated compliance will be in a much stronger competitive position than those relying solely on self-attestation.

Talk to Coalfire Federal about an independent CMMC assessment or mock assessment.

COALFIRE FEDERAL

About Coalfire Federal

For 20 years, Coalfire Federal has provided cybersecurity services to a wide range of government and commercial organizations, enabling and protecting their mission-specific cyber objectives. Coalfire Federal is the leading FedRAMP 3PAO and an Authorized CMMC C3PAO, and offers a full spectrum of cybersecurity risk management and compliance services.

For Support with your C3PAO Journey,
Contact us at Coalfirefederal.com

References

This report combines public cyber threat intelligence, CMMC ecosystem data, and assessment-oriented observations to provide executive-level guidance. Percentages labeled as "estimated" are directional indicators designed for planning and communication, not formal statistical claims.

Government Sources

1. Department of Defense (DoD) CMMC Program
   - https://dodcio.defense.gov/CMMC/
2. National Institute of Standards and Technology (NIST)
   - NIST SP 800-171 Rev. 2
   - NIST SP 800-172
   - NIST Cybersecurity Framework (CSF) 2.0
   - https://www.nist.gov
3. Defense Counterintelligence and Security Agency (DCSA)
   - https://www.dcsa.mil
4. Cybersecurity and Infrastructure Security Agency (CISA)
   - Known Exploited Vulnerabilities Catalog
   - Secure by Design Guidance
   - Annual Threat Reports
   - https://www.cisa.gov
5. NSA Cybersecurity Advisories
   - https://www.nsa.gov/cybersecurity/
6. FBI IC3 Annual Internet Crime Report
   - https://www.ic3.gov

CMMC Ecosystem Sources

7. Cyber AB Town Hall Presentations
   - Current certification statistics
   - Final and Conditional Certificates
   - Assessment pipeline updates
8. Cyber AB Marketplace Statistics
9. Cyber AB CMMC Assessment Process Documentation
10. Cyber AB Public Dashboard and Town Hall Slides

Threat Intelligence Sources

11. Microsoft Digital Defense Report
12. Google Mandiant M-Trends Report
13. CrowdStrike Global Threat Report
14. Palo Alto Unit 42 Threat Report
15. IBM X-Force Threat Intelligence Index
16. Verizon Data Breach Investigations Report (DBIR)
17. Recorded Future Annual Threat Report
18. Dragos OT/ICS Threat Landscape Report
19. Fortinet Threat Landscape Report
20. Cisco Talos Annual Threat Report

Defense Industrial Base Sources

21. Industrial Base Analysis and Sustainment (IBAS)
22. DoD Industrial Base Reports
23. Defense Industrial Base Sector Coordinating Council
24. CISA Defense Industrial Base Cybersecurity Resources
25. DIB Sector Risk Management Agency Publications

Supply Chain & AI Sources

26. ENISA Threat Landscape Report
27. MITRE ATT&CK Framework
28. OWASP Top 10
29. OpenAI and Microsoft AI Security Research
30. Gartner Cybersecurity Trends
31. Forrester Zero Trust Research