Navigating the CMMC Ecosystem

The Straight Facts for the Management Executive

David W. Koran, RPA

David Koran & Associates Inc.

April 2026

Contents

Summary

The Cybersecurity Maturity Model Certification (CMMC) 2.0 program, codified in 32 CFR Part 170 and enforced through DFARS clause 252.204-7021, establishes a mandatory certification framework for organizations within the Defense Industrial Base (DIB). The program introduces a structured ecosystem of credentialed roles, accredited organizations, and regulatory enforcement mechanisms. For executives responsible for contract eligibility and corporate compliance, understanding how this ecosystem functions is a prerequisite to making informed decisions about the path to certification.

This paper provides a structural overview of the CMMC ecosystem. It identifies the principal entities and their roles, explains the regulatory separation between preparation and assessment, outlines the certification timeline, and describes the practical sequence of activities that leads to a certification determination. The goal is to give defense contractor leadership a clear map of the terrain before committing organizational resources.

The Governing Structure

The CMMC program operates under the authority of the Department of Defense, with the final rule published as 32 CFR Part 170 in October 2024. The program is administered through a layered governance model that involves three principal entities: the DoD itself, the Cyber Accreditation Body (CyberAB), and the Defense Contract Management Agency (DCMA) through its Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

The DoD establishes the requirements, defines the certification levels, and sets the enforcement timeline. The CyberAB, operating under a formal agreement with the DoD, is responsible for accrediting the organizations and individuals that participate in the ecosystem. DIBCAC retains oversight authority over the assessment process and may conduct its own assessments, known as DIBCAC High assessments, for CMMC Level 3.

Understanding this governance model matters because it determines who has authority at each stage of the process. The DoD sets the rules. The CyberAB credentials the participants. The C3PAO conducts the assessment. The DoD renders the final certification status. No single entity controls the entire process, and this distribution of authority is intentional.

The Ecosystem Participants

The CMMC ecosystem includes several distinct categories of participants, each with a defined role and scope of authority. Executives evaluating their organization's path to certification should understand who these participants are, what they do, and where the boundaries of their authority lie.

The Organization Seeking Certification

The Organization Seeking Certification (OSC) is the defense contractor or subcontractor that must achieve CMMC certification to satisfy contract requirements. The OSC is responsible for implementing the required security controls, maintaining the supporting documentation, and presenting its environment for assessment. The OSC selects its own path to certification, chooses its service providers, and bears the ultimate responsibility for the compliance posture of its information systems.

Registered Practitioners and Registered Practitioner Advanced

Registered Practitioners (RPs) and Registered Practitioner Advanced (RPAs) are individuals credentialed by the CyberAB to provide implementation consulting and readiness services to OSCs. Their work falls on the enablement side of the ecosystem. This includes technical scoping, gap analysis, policy and procedure development, security control implementation guidance, evidence preparation, and readiness evaluation.

The RP credential represents foundational competence in CMMC requirements and assessment methodology. The RPA credential represents a higher tier of demonstrated technical proficiency. RPAs have passed additional examinations and have demonstrated the ability to work across the full scope of NIST SP 800-171 Rev 2 controls in complex environments. The distinction is relevant because more complex contractor environments, those with hybrid cloud deployments, legacy operational technology, or multiple facility scopes, typically benefit from the deeper technical judgment the RPA credential represents.

The critical limitation to understand is that RPs and RPAs do not issue certifications. They prepare organizations for the certification process. Their role ends where the formal assessment begins.

Registered Provider Organizations

Registered Provider Organizations (RPOs) are companies authorized by the CyberAB to deliver CMMC consulting services. To obtain the RPO designation, an organization must employ at least one credentialed RP or RPA and sign the CyberAB Code of Professional Conduct agreement. The RPO credential is an organizational designation that signals the company has met these requirements.

It is important to note, however, that the RPO is not a prerequisite for practitioner work. An individual holding an RP or RPA credential may operate independently, contracting directly with an OSC without affiliation to an RPO. The CyberAB recognizes both models: practitioners working as members of a Registered Provider Organization, and practitioners contracted as individuals. When evaluating enablement options, OSCs may engage either an RPO or an independent practitioner, depending on the scope of support required and the organization's preference.

C3PAOs and Certified CMMC Assessors

CMMC Third-Party Assessment Organizations (C3PAOs) are accredited by the CyberAB to conduct formal CMMC Level 2 certification assessments. C3PAOs

employ Certified CMMC Assessors (CCAs) and Certified CMMC Professionals (CCPs) who perform the on-site and remote evaluation of the OSC's security controls, evidence, and operational practices.

The C3PAO assessment is the formal audit. The assessment team reviews the OSC's System Security Plan (SSP), evaluates the implementation of all 110 NIST SP 800-171 Rev 2 security requirements, examines the supporting evidence, and conducts interviews with personnel responsible for the controls. The C3PAO then submits its findings to the DoD through the eMASS system, and the DoD renders the certification determination.

The assessment is typically bounded in duration, often spanning one to three weeks of active assessment activity. The DoD projects the cost of a Level 2 certification assessment at $105,000 to $118,000 per the economic analysis in 32 CFR Part 170. A detailed discussion of total program costs appears in the economics section of this paper.

DIBCAC

The Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) operates within DCMA and retains a direct role in the assessment process. DIBCAC conducts the assessments required for CMMC Level 3 (the highest level) and has oversight authority over the C3PAO assessment process for Level 2. DIBCAC may also conduct assessments in response to specific concerns or as part of its quality assurance function.

Ecosystem Role Summary

The following table summarizes the principal entities, their functions, and where they operate within the enablement or assessment side of the ecosystem.

Entity	Function	Side of Ecosystem
OSC	Implements controls, maintains	Subject of certification

	documentation, presents for assessment	
RP / RPA	Gap analysis, implementation guidance, evidence preparation, readiness review	Enablement
RPO	Organizational credential for companies employing RPs/RPAs; not required for individual practitioners	Enablement
C3PAO	Conducts formal Level 2 certification assessment; submits findings to DoD	Assessment
CCA / CCP	Assessors employed by C3PAOs who evaluate controls and evidence	Assessment
CyberAB	Accredits C3PAOs, credentials practitioners, maintains ecosystem integrity	Governance
DIBCAC	Conducts Level 3 assessments, provides quality oversight of Level 2 process	Assessment / Oversight
DoD	Establishes requirements, sets enforcement timeline, renders final certification status	Governance / Authority

Determining Your Required CMMC Level

Before engaging with the ecosystem, an executive must determine which CMMC level applies to the organization. The answer depends on the type of information the organization handles in the performance of its DoD contracts, not on company size, contract value, or the executive's preference.

CMMC Level 1 applies to organizations that process, store, or transmit only Federal Contract Information (FCI). FCI is information provided by or generated for the government under contract that is not intended for public release. Level 1 requires implementation of the 15 basic safeguarding requirements defined in FAR 52.204-21 and is satisfied through an annual self-assessment. No C3PAO assessment is required at Level 1.

CMMC Level 2 applies to organizations that process, store, or transmit Controlled Unclassified Information (CUI). CUI is information the government creates or possesses, or that an entity creates or possesses on behalf of the government, that requires safeguarding or dissemination controls under law, regulation, or government-wide policy. Level 2 requires implementation of all 110 security requirements in NIST SP 800-171 Rev 2. The assessment type, whether self-assessment or C3PAO certification assessment, is specified in the solicitation or contract. For most contracts involving CUI, the DoD will require a C3PAO certification assessment beginning under Phase 2.

CMMC Level 3 applies to organizations that handle the most sensitive categories of CUI and support the DoD's most critical programs. Level 3 requires compliance with all Level 2 requirements plus 24 additional security requirements from NIST SP 800-172. Level 3 assessments are conducted by DIBCAC, not by C3PAOs. The DoD estimates that fewer than one percent of organizations requiring CMMC certification will be subject to Level 3.

The required CMMC level will be specified in the solicitation through DFARS 252.204-7021. For subcontractors, the required level will appear in the subcontract terms flowed down by the prime contractor. Executives who are uncertain about which level applies to their organization should examine the CUI categories identified in the National Archives CUI Registry that are relevant to their contract work and consult with their contracting officer or legal counsel.

The Structural Separation Between Enablement and Assessment

The CMMC ecosystem was designed with an intentional separation between the entities that help organizations prepare for certification and the entities that conduct the formal assessment. This separation is codified in 32 CFR Part 170 and reinforced by the CyberAB's Code of Professional Conduct. It is the organizing principle of the ecosystem, and it has practical consequences that executives must understand.

The rule is straightforward: an organization or individual that provides enablement services to an OSC cannot serve as the assessor for that same organization. A C3PAO cannot consult with an OSC on control implementation and then assess that same OSC for certification. An individual who has served as an RP or RPA for a contractor cannot participate in that contractor's assessment as a CCA.

This separation serves three purposes. First, it ensures that the certification determination is rendered by a party with no financial or professional interest in the outcome of the preparation work. An assessor who also provided the consulting has an inherent incentive to find the organization compliant, because a noncompliant finding reflects on the quality of the assessor's own earlier work. The structural separation eliminates that dynamic entirely.

Second, the separation gives the OSC the benefit of an independent evaluation. If the enablement work was thorough, the assessment confirms it. If gaps remain, the assessment identifies them. In either case, the OSC receives an objective determination that it can rely on.

Third, the separation sustains the credibility of the certification itself. The DoD relies on CMMC certifications as a basis for contract award decisions. If the same entity could both prepare and certify an organization, the reliability of the certification would be diminished. The structural separation ensures that a CMMC Level 2 certification carries the evidentiary weight the DoD intends.

For executives, the practical implication is that the path to certification involves at least two separate engagements with two separate entities: one for preparation and one for assessment. These engagements should be planned as sequential phases of a single compliance effort, not as disconnected events.

The Certification Timeline

The CMMC program is being implemented in four phases, each expanding the scope of contract solicitations that will include the CMMC requirement.

Phase 1: November 10, 2025

The 32 CFR Part 170 final rule became effective on December 16, 2024, establishing the regulatory framework. Phase 1 enforcement began on November 10, 2025, when the revised DFARS clause 252.204-7021 took effect and contracting officers began including CMMC requirements in applicable solicitations and contracts. Phase 1 introduced CMMC Level 1 self-assessment and CMMC Level 2 self-assessment requirements, with the DoD retaining discretion to require Level 2 C3PAO certification assessments during this phase as well.

Phase 2: November 10, 2026

Phase 2 is the inflection point. Beginning November 10, 2026, the DoD will include CMMC Level 2 certification assessment requirements (the C3PAO assessment) in applicable solicitations and contracts involving Controlled Unclassified Information (CUI). This is the date after which a contractor that has not achieved CMMC Level 2 certification will be ineligible for award on solicitations that include the requirement.

Phase 3: Approximately 2028

Phase 3 extends the CMMC Level 2 certification requirement to all applicable solicitations and contracts, including option periods on existing contracts. Phase 3 also introduces CMMC Level 3 requirements (DIBCAC assessment) for contracts involving the most sensitive CUI categories.

Phase 4: Full Implementation

Phase 4 completes the rollout by including CMMC requirements in all applicable DoD solicitations and contracts across all levels.

The practical significance of this timeline is that Phase 2 creates the first mandatory gate for Level 2 C3PAO certification. Organizations that handle CUI and depend on DoD contract revenue should treat November 10, 2026 as the date by which they must have achieved certification or be at immediate risk of contract ineligibility.

Subcontractor Flowdown Requirements

CMMC requirements do not apply only to prime contractors. Under DFARS 252.204-7021, prime contractors are required to flow CMMC requirements down to their subcontractors when those subcontractors will process, store, or transmit Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) in the performance of the subcontract. The required CMMC level for the subcontractor is determined by the type of information the subcontractor will handle, not by the prime contractor's level.

This flowdown obligation has two significant implications. For executives at subtier companies, the CMMC requirement may not appear in a DoD solicitation at all. It will appear in the subcontract terms imposed by the prime. A subcontractor that has not achieved the required CMMC level will be ineligible for award by the prime, regardless of the subcontractor's technical qualifications or pricing. The practical effect is the same as a direct DoD contract requirement: no certification means no work.

For executives at prime contractor organizations, the obligation is to verify subcontractor CMMC compliance before awarding and during administration of subcontracts that involve FCI or CUI. Prime contractors cannot simply include the CMMC clause in the subcontract and assume compliance. They must confirm that the subcontractor holds the required CMMC status in SPRS. A prime contractor that awards a subcontract to a noncompliant subcontractor places its own contract performance and compliance posture at risk.

The flowdown requirement amplifies the timeline pressure across the entire supply chain. If a prime contractor achieves certification but its critical subcontractors do not, the prime may be unable to execute the contract as proposed. Executives at both the prime and subtier levels should be coordinating on CMMC readiness as a supply chain management function, not solely as an internal compliance matter.

The Economics of Certification

The cost of CMMC Level 2 certification is distributed across several categories, and the total varies significantly based on the organization's size, the complexity of its environment, and its starting compliance posture. Executives should plan for the full cost envelope, not just the assessment fee.

The C3PAO Assessment

The DoD's published cost estimate for a Level 2 C3PAO certification assessment, as detailed in the economic analysis accompanying 32 CFR Part 170, projects a cost of $105,000 to $118,000. That figure includes the triennial assessment and two annual affirmations. C3PAOs set their own fees, and actual costs may vary based on the scope and complexity of the OSC's environment, the number of facilities, and the duration of the assessment engagement.

Implementation and Remediation

For most organizations, the largest cost component is not the assessment itself but the implementation work that precedes it. Remediation costs depend on how many of the 110 security requirements are already in place and how much work is needed to close the gaps. Organizations that have been actively maintaining compliance with NIST SP 800-171 Rev 2 under DFARS 252.204-7012 may find their remediation costs are modest. Organizations that have deferred compliance investments may face costs ranging from tens of thousands of dollars for targeted control implementation to several hundred thousand dollars or more for

organizations requiring infrastructure upgrades, CUI enclave buildouts, or significant tooling changes.

Cost categories within implementation typically include security tool procurement and licensing, infrastructure upgrades (network segmentation, endpoint protection, SIEM deployment), policy and procedure development, personnel training, and the labor cost of configuring and operationalizing the controls. Organizations with complex or distributed environments, multiple facilities, hybrid cloud deployments, or legacy operational technology should expect higher implementation costs than organizations with a single-site, standardized IT environment.

Enablement Consulting

Enablement consulting costs, whether engaged through an RPO or an independent RP or RPA, depend on the scope and duration of the engagement. These costs should be evaluated in the context of the assessment they are designed to support. The purpose of enablement is to ensure that the organization enters the C3PAO assessment in a position to succeed. An assessment that results in findings of noncompliance may require remediation and reassessment, and the cost of that second cycle, in both direct C3PAO fees and operational disruption, typically exceeds the cost of thorough preparation.

Common Cost Drivers and Avoidable Mistakes

Several factors consistently drive costs higher than they need to be. Over-scoping the CUI boundary is one of the most common. An organization that includes systems in the assessment scope that do not actually process, store, or transmit CUI will pay for controls, evidence, and assessment time that were never required. Accurate scoping, performed early in the process, is the single most effective cost control measure.

Reliance on a cloud service provider that does not meet FedRAMP Moderate or equivalency requirements is another frequent cost driver. Organizations that

discover this gap late in the process face the cost of migrating to a compliant provider, reconfiguring their environment, and rebuilding their evidence package, all under timeline pressure. Verifying ESP compliance at the outset of the project avoids this.

Deferred compliance is itself a cost driver. Organizations that have been contractually required to implement NIST SP 800-171 Rev 2 since 2017 under DFARS 252.204-7012 but have not done so face the accumulated cost of years of deferred investment, compressed into a timeline that no longer permits phased implementation. The DoD's position, as reflected in the 32 CFR Part 170 economic analysis, is that the security control implementation costs are not new costs attributable to CMMC, because they were already required. The assessment cost is the only new cost the program introduces. For organizations that have deferred implementation, the practical reality is that all of those costs must now be incurred simultaneously.

The Revenue Context

The total cost of the certification effort, across implementation, enablement, and assessment, should be measured against the contract revenue it protects. For organizations whose business depends on DoD contracts requiring CUI handling, CMMC Level 2 certification is a condition of continued eligibility. The cost of certification is a known, plannable investment. The cost of ineligibility is the loss of the revenue that those contracts represent. For most DIB contractors, the former is materially smaller than the latter.

The Path to Certification: Practical Sequence

Achieving CMMC Level 2 certification is not a single event. It is a sequence of activities that typically spans twelve to eighteen months for organizations that have not already implemented the full scope of NIST SP 800-171 Rev 2 controls. Executives should understand the phases of this process and the approximate time each requires.

The following table presents a representative timeline for an organization beginning the certification process with meaningful gaps in its current compliance posture. Organizations with a more mature security baseline may compress certain phases. Organizations with complex or distributed environments may require additional time.

Phase	Approximate Duration	Key Activities
Scoping and Gap Analysis	Months 1 through 2	Define CUI boundary; identify systems, networks, personnel, and facilities in scope; evaluate current posture against all 110 NIST SP 800-171 Rev 2 requirements; document gaps
Remediation and Implementation	Months 3 through 12	Procure and configure security tools; draft and approve policies and procedures; implement technical controls; train personnel; establish operational practices
Evidence Preparation	Months 10 through 14	Build and organize evidence repository; map artifacts to assessment objectives; verify documentation completeness; collect operational records demonstrating control effectiveness
Readiness Review	Months 13 through 15	Conduct simulated assessment against CMMC Assessment Guide methodology; identify remaining deficiencies; remediate findings; verify assessment readiness
C3PAO Scheduling	Months 8 through 12	Select C3PAO from CyberAB Marketplace; negotiate scope and schedule; secure assessment window (begin early due to assessor availability constraints)
C3PAO Assessment	Months 15 through 17	Formal assessment of all 110 controls; evidence review; personnel interviews;

		C3PAO submits findings to DoD through eMASS
Certification Determination	Months 17 through 18	DoD reviews C3PAO report and renders certification status; organization receives certification, conditional status with remediation window, or finding of noncompliance

Note that several phases overlap. Evidence preparation begins during implementation as controls produce operational records. C3PAO scheduling should begin well before the readiness review is complete, because assessment windows may be booked three to six months in advance. The timeline above reflects these parallel activities.

Scoping and Gap Analysis

The process begins with defining the scope of the certification boundary. This means identifying which systems, networks, personnel, and facilities process, store, or transmit CUI. Scoping is the most consequential decision in the entire process, because it determines the size and complexity of the environment that must satisfy all 110 security requirements. A scope that is too broad creates unnecessary cost. A scope that is too narrow risks excluding systems that handle CUI, which will result in findings during assessment. Following the scoping decision, a gap analysis evaluates the organization's current posture against all 110 requirements, producing a clear picture of what is implemented, what is partially implemented, and what is missing.

Remediation and Implementation

The gap analysis drives the implementation plan. This phase involves procuring and configuring security tools, drafting policies and procedures, implementing technical controls, training personnel, and establishing the operational practices

each control requires. Implementation timelines vary based on the size and complexity of the environment, but six to twelve months is a reasonable expectation for organizations with meaningful gaps. Common areas of significant remediation include audit and accountability (AU), identification and authentication (IA), and system and communications protection (SC).

Evidence Preparation and Readiness Review

The C3PAO assessment is evidence-based. Assessors evaluate compliance by reviewing documented policies, system configurations, operational records, and supporting artifacts. Before scheduling the assessment, the organization should conduct a readiness review that simulates the assessment process. This review verifies that controls are functioning as intended, that the evidence package is complete, and that any remaining deficiencies are identified and remediated before the formal assessment begins.

The C3PAO Assessment

The formal assessment is conducted by a C3PAO accredited by the CyberAB. The assessment team evaluates the OSC's implementation of all 110 controls, reviews the evidence, conducts interviews, and submits its findings to the DoD. The DoD renders the certification determination based on the C3PAO's report. If the assessment identifies deficiencies, the OSC may receive a conditional certification with a defined remediation window, or the assessment may result in a finding of noncompliance that requires a reassessment after remediation is complete.

External Service Providers and FedRAMP Moderate Equivalency

Many defense contractors rely on cloud service providers (CSPs) or managed service providers to host, process, or transmit CUI. These External Service Providers (ESPs) fall within the CMMC assessment scope and must meet specific requirements. Under DFARS 252.204-7012, any cloud service provider used to

process, store, or transmit CUI must meet security requirements equivalent to those established by the FedRAMP Moderate baseline.

This requirement can be satisfied in one of three ways: the CSP holds a FedRAMP Moderate authorization, the CSP meets the DoD's FedRAMP Moderate Equivalency requirements as defined in the December 2023 DoD memorandum, or the CSP itself holds a CMMC Level 2 certification for the services in scope. During the C3PAO assessment, the assessment team will evaluate whether the OSC's ESPs meet these requirements. If an ESP does not meet the applicable standard, the controls that depend on that provider may be scored as NOT MET.

This is a scoping and cost factor that catches many organizations off guard. Executives should inventory all ESPs that touch CUI, verify their FedRAMP or equivalency status, and factor any necessary provider changes or migrations into the implementation timeline. A provider migration in the middle of the assessment preparation process can add months to the timeline and significant cost to the project.

Assessment Capacity: The Supply Constraint

The CMMC program's enforcement timeline assumes that the assessment ecosystem will have sufficient capacity to certify the organizations that require it. The current data suggests that this assumption should not be taken for granted. Executives should understand the supply side arithmetic, because assessment scheduling is not fully within the OSC's control.

As of the January 2026 CyberAB Town Hall, the ecosystem included 97 authorized C3PAOs and 688 Certified CMMC Assessors. The number of Lead CCAs, who are required to lead each assessment team, stood at 425. The CyberAB expected to cross 100 authorized C3PAOs in the near term, and four non-U.S. C3PAOs were reported to be moving through the authorization process. ISACA assumed responsibility for CMMC professional credentialing (CCP, CCA, Lead CCA) in April 2026, and these numbers continue to grow as new applications are processed.

On the demand side, the DoD estimates that approximately 80,000 contractors will require CMMC Level 2 certification. Not all of these organizations will require certification simultaneously, and the phased enforcement timeline distributes the demand across several years. However, the Phase 2 trigger on November 10, 2026 will create a concentration of demand from organizations that have deferred action and are now operating under deadline pressure.

The practical math is instructive. If each C3PAO can conduct an average of 20 to 30 assessments per year (a reasonable estimate given assessment duration, travel, reporting, and QA requirements), the current pool of 97 C3PAOs can process roughly 1,900 to 2,900 assessments annually. Against a demand pool of 80,000 organizations, the assessment infrastructure would require decades to clear the backlog at current capacity. The ecosystem will grow, and not all 80,000 organizations will pursue certification on the same timeline, but the structural imbalance between supply and demand is a material factor in planning.

For executives, the implication is direct. Assessment scheduling is a constrained resource, and organizations that begin the scheduling process later will face longer wait times. Many C3PAOs are reporting booking windows of three to six months or more. An organization that completes its implementation and readiness review but cannot secure an assessment window before the Phase 2 enforcement date will still be ineligible for contract award, regardless of its actual compliance posture. Beginning the C3PAO selection and scheduling process early in the implementation timeline, rather than waiting until readiness is confirmed, is a risk mitigation measure that costs nothing but protects the organization against a scheduling bottleneck it cannot control.

The Assessment Process in Detail

The formal CMMC Level 2 certification assessment follows a structured methodology defined in the CMMC Assessment Process (CAP). The CAP establishes the procedures that C3PAOs and their assessment teams must follow, the quality assurance requirements that govern the process, and the reporting mechanism

through which results are submitted to the Department of Defense. Executives should understand this process in detail, because it defines what the organization will experience during the assessment and what determines the outcome.

Preliminary Activities

Before the formal assessment begins, several administrative and contractual activities must be completed. The OSC initiates the process by contacting an accredited C3PAO from the CyberAB Marketplace. The C3PAO and the OSC negotiate the scope of the assessment, the schedule, the assessment team composition, and the terms of engagement. The OSC must have a valid Commercial and Government Entity (CAGE) code, as the assessment cannot proceed without one. A single assessment may cover more than one CAGE code if the OSC's certification boundary spans multiple entities.

The C3PAO is responsible for identifying and mitigating any conflicts of interest among the members of the assessment team before commencing the assessment. This responsibility cannot be delegated to the Lead CCA or the OSC. Any conflict between a member of the assessment team and the OSC must be sufficiently mitigated or avoided before the assessment proceeds.

Phase 1: Pre-Assessment and Planning

Phase 1 encompasses the collection and documentation of pre-assessment information. The C3PAO generates a Pre-Assessment Form that captures the OSC's CAGE code, System Security Plan (SSP) title, OSC contact information, assessment team details, planned assessment dates, and a readiness determination. This information is required for DoD program management and oversight purposes.

The C3PAO may use the official Pre-Assessment Form available on the CMMC eMASS website or any tool that generates pre-assessment data in the required JSON file format compliant with the CMMC eMASS data standard. Once the Pre-Assessment Form is complete, a C3PAO Quality Assurance (QA) individual conducts

a review of the form. The QA individual must be a CCA and cannot be a member of the assessment team for which they are performing the QA role.

After the QA review, the QA individual uploads the Pre-Assessment Form into the CMMC instantiation of eMASS. Phase 1 concludes upon completion of this upload. If the Lead CCA determines during Phase 1 that the OSC is not prepared to undergo the assessment, the Lead CCA will inform the OSC's Affirming Official of the decision in writing and suspend the assessment. Under no circumstances will the C3PAO offer advice on improving the OSC's preparedness, as the Code of Professional Conduct prohibits C3PAOs from providing advisory services to assessment clients.

Phase 2: The Assessment

Phase 2 is the evaluative core of the process. The assessment team, led by the Lead CCA, conducts a systematic evaluation of the OSC's implementation of all 110 NIST SP 800-171 Rev 2 security requirements. The assessment methodology includes three categories of evidence gathering: examination of documentation and artifacts, interviews with personnel responsible for implementing and operating the controls, and observation of security practices and system configurations.

The assessment team evaluates each security requirement against the assessment objectives defined in the CMMC Assessment Guide. For each requirement, the team determines whether the control is MET or NOT MET based on the evidence presented. The assessment team hosts a Daily Checkpoint Meeting with the OSC point of contact at the end of each assessment day to summarize progress, identify challenges, and discuss items requiring coordination.

The assessment team does not provide guidance, recommendations, or implementation assistance to the OSC during the assessment. The C3PAO's role is strictly evaluative. This restriction reinforces the structural separation between enablement and assessment that governs the entire ecosystem.

Phase 3: Reporting and Submission to eMASS

Phase 3 begins after all evaluative activity in Phase 2 is complete. The assessment team compiles the assessment results and composes them in the format required for upload into the CMMC instantiation of the Enterprise Mission Assurance Support Service (eMASS). eMASS is the DoD's system of record for managing cybersecurity authorization and assessment data across defense programs.

The CMMC instantiation of eMASS serves as the central repository for all CMMC assessment data. It is the mechanism through which C3PAO assessment results are transmitted to the DoD and ultimately reflected in the Supplier Performance Risk System (SPRS). SPRS is the system that contracting officers query to verify a contractor's CMMC status before making contract award decisions. The linkage between eMASS and SPRS means that the assessment results entered by the C3PAO directly determine the contractor's eligibility status in the DoD's procurement systems.

Before the results are uploaded, the C3PAO QA individual conducts a quality assurance review of the compiled assessment report. This review ensures that the results are complete, consistent, and compliant with the CMMC eMASS data standard. After the QA review, the QA individual uploads the results into eMASS. The C3PAO follows the procedures set forth in the DoD CMMC eMASS Concept of Operations for C3PAOs.

The Limited Practice Deficiency Correction Program

One mechanism within the CAP that executives should understand is the Limited Practice Deficiency Correction Program. During the assessment, the assessment team may determine that a security requirement has been implemented but that the supporting documentation is outdated, incomplete, or recorded incorrectly. In these cases, the deficiency is not a failure of implementation but a gap in the evidence supporting it.

The Limited Practice Deficiency Correction Program allows the OSC to correct these types of deficiencies without triggering a POA&M. The program applies to 52 of the 110 Level 2 practices, specifically the lower-weighted requirements as defined in

the CMMC Scoring Methodology. It does not apply to the higher-weighted requirements. The OSC has five business days from the Final Findings Briefing to provide corrected evidence. The C3PAO reviews the new evidence, and if the correction is sufficient, the score for that practice changes to MET. If the evidence remains insufficient, the score stays at NOT MET and the Lead CCA recommends moving the deficiency to a POA&M.

This correction window is narrow and applies only to documentation and evidence deficiencies, not to controls that have not been implemented. It is not a second chance to build what was missing. It is an opportunity to correct the record where the underlying control is in place but the evidence did not adequately demonstrate it during the assessment. Organizations that maintain well-organized, current evidence throughout the implementation process are less likely to need this correction window, but its existence reflects the practical reality that documentation gaps can occur even in otherwise well-prepared environments.

Assessment Outcomes

The assessment process produces one of three outcomes. The first is a Final CMMC Level 2 certification, issued when the OSC has demonstrated compliance with all 110 security requirements. A Final certification is valid for three years, during which the organization must submit annual affirmations of continued compliance.

The second outcome is a Conditional CMMC Level 2 certification. This status may be issued when the OSC has not met all 110 requirements but has achieved a minimum score and met all requirements that are not eligible for a Plan of Action and Milestones (POA&M). Under conditional status, the OSC must remediate all unmet requirements documented in the POA&M and complete a closeout assessment within 180 days of the conditional status date. The closeout assessment verifies that the previously unmet requirements have been fully implemented. If the closeout assessment confirms compliance, the conditional status converts to a Final certification. If one or more requirements remain NOT MET, or if the closeout assessment is not finalized in eMASS within 180 days, the conditional status is terminated and the organization must begin the assessment process again.

The third outcome is a finding that the OSC does not meet the requirements for certification. In this case, no certification is issued, and the organization must remediate the identified deficiencies and schedule a new assessment to attempt certification.

DoD Oversight and Quality Assurance

The DoD maintains oversight of the assessment process through several mechanisms. DIBCAC has authority to observe C3PAO assessments, review assessment results, and conduct its own assessments when warranted. The CyberAB monitors C3PAO performance and compliance with the Code of Professional Conduct. The eMASS system provides the DoD with a centralized view of assessment activity, certification status, and annual affirmation compliance across the entire Defense Industrial Base.

This layered oversight structure ensures that the certification process produces reliable results. The C3PAO conducts the assessment. The QA individual within the C3PAO verifies the quality of the work. DIBCAC and the CyberAB provide external oversight. The DoD retains final authority over certification status through its control of the eMASS and SPRS systems. At each layer, the process is designed to ensure that a CMMC Level 2 certification represents a genuine and verified compliance posture.

SPRS Score Integrity and the False Claims Act

The introduction of mandatory C3PAO assessments under CMMC creates a condition that did not exist under the prior self-assessment regime: the DoD will now hold two independent data points for the same contractor. The first is the SPRS score the contractor self-reported under DFARS 252.204-7019. The second is the C3PAO assessment result submitted through eMASS. When both records exist in the DoD's systems, any material discrepancy between them becomes visible to the government.

This matters because the Department of Justice (DOJ) has established, through enforcement action, that inaccurate SPRS score submissions can constitute violations of the False Claims Act (FCA), 31 U.S.C. Section 3729. The FCA does not require proof of intent to defraud. Under the statute, liability attaches to claims submitted with actual knowledge of their falsity, deliberate ignorance of the truth, or reckless disregard of the truth. An executive who signs an annual affirmation of compliance without verifying the accuracy of the organization's SPRS score may be exposed to FCA liability under the reckless disregard standard.

Recent Enforcement Actions

The DOJ settled seven cybersecurity-related FCA cases in 2025, establishing a clear enforcement pattern. In one of the most instructive cases, a defense contractor had submitted a self-assessed SPRS score of 104, near the maximum of 110. A subsequent independent evaluation determined the contractor's actual score to be negative 142. The contractor paid $4.6 million to resolve the allegations. The case originated as a qui tam action filed by a whistleblower, who received over $850,000 from the settlement.

In a separate 2025 settlement, a defense contractor and its affiliates paid $8.4 million to resolve allegations that they failed to meet cybersecurity obligations while certifying compliance. Notably, the acquiring company in that transaction was named as successor in liability for the target's preacquisition cybersecurity failures, extending FCA exposure to the M&A context. In yet another case, both a contractor and its private equity owner were held liable for DFARS cybersecurity violations, demonstrating that FCA exposure is not limited to the operating entity.

The DOJ also announced its first FCA settlement targeting the defense supply chain when a precision machining subcontractor paid approximately $421,000 to resolve allegations of inadequate cybersecurity protections for technical drawings supplied to prime contractors. That case, too, originated as a qui tam action filed by a former employee.

The Structural Exposure

The CMMC program creates a structural condition in which SPRS score discrepancies will become routine findings rather than exceptional discoveries. Under the prior regime, the self-assessed SPRS score was the only data point. The government had limited visibility into whether the reported score reflected the contractor's actual posture. Under CMMC, the C3PAO assessment provides an independent, evidence-based determination that is entered into eMASS and reflected in SPRS. If the C3PAO-verified score differs materially from the contractor's previously submitted self-assessment, the discrepancy is documented in the DoD's own systems.

The DOJ's Civil Cyber-Fraud Initiative, launched in 2021, was specifically designed to use the False Claims Act as an enforcement mechanism for cybersecurity compliance in government contracting. The combination of the Initiative's mandate, the qui tam provisions that incentivize whistleblower reporting, and the dual-record visibility that CMMC creates means that SPRS score accuracy is no longer a matter of administrative diligence alone. It is a legal exposure that requires executive attention.

Implications for Executives

The executive who signs the annual affirmation of compliance in SPRS is personally accountable for the accuracy of that affirmation. Under 32 CFR Part 170.22, the Affirming Official must attest that the organization has implemented and will maintain implementation of all applicable CMMC security requirements. This affirmation is required upon achieving CMMC status, annually thereafter, and at POA&M closeout.

For organizations that have not revisited their SPRS score since it was first submitted, the risk is straightforward. If the self-assessed score was based on assumptions, incomplete analysis, or aspirational compliance rather than verified implementation, the C3PAO assessment will surface those discrepancies. At that point, the government holds documented evidence of the gap between what was claimed and what was verified. A lower but accurate SPRS score, updated to reflect

the organization's actual posture, is a materially safer position than an inflated score that cannot withstand independent verification.

The Certification Lifecycle

Achieving CMMC Level 2 certification is not the end of the compliance obligation. It is the beginning of a recurring cycle that extends for the duration of the organization's participation in DoD contracts requiring CUI protection. Executives should understand the post-certification requirements before entering the assessment process, because the operational and financial commitments extend well beyond the initial certification event.

Certification Validity and Triennial Reassessment

A Final CMMC Level 2 certification is valid for three years from the CMMC Status Date. Before the certification expires, the organization must complete a new C3PAO assessment to maintain its certified status. The triennial reassessment follows the same CAP methodology as the initial assessment. Organizations should begin planning for reassessment well in advance of the expiration date, accounting for the same C3PAO scheduling constraints that apply to initial assessments.

Annual Affirmation of Compliance

Between triennial assessments, the organization must submit an annual affirmation of continuous compliance in SPRS. Under 32 CFR Part 170.22, the Affirming Official, a senior executive of the organization, must attest that the organization has implemented and will maintain implementation of all applicable CMMC security requirements. This affirmation is required annually following the CMMC Status Date and carries the same False Claims Act exposure discussed in the preceding section. The affirmation is not a formality. It is a legally binding representation to the DoD.

Continuous Compliance

The CMMC program assumes that the security posture verified during the assessment is maintained throughout the certification period. Controls must remain operational, policies must remain current, personnel must continue to receive required training, and the evidence of ongoing compliance must be maintained. If the organization's environment changes materially, through infrastructure upgrades, cloud migrations, facility changes, or organizational restructuring, the impact on the certification boundary must be evaluated and the SSP must be updated to reflect the current state.

Organizations that treat certification as a point-in-time event and allow controls to degrade between assessments face two risks. First, the annual affirmation becomes inaccurate, creating FCA exposure. Second, the triennial reassessment is more likely to surface findings of noncompliance, requiring remediation and potentially a conditional certification or failure. The organizations that manage CMMC most effectively treat compliance as a continuous operational function, not a periodic project.

Risk Prioritization for the Executive

This paper has identified several categories of risk associated with the CMMC program. Executives managing competing priorities and limited resources benefit from understanding not just what the risks are, but the order in which they are most likely to affect the organization. The following prioritization reflects the sequence in which consequences typically materialize and the relative severity of each.

First Order: Loss of Contract Eligibility

The most immediate and consequential risk is the inability to compete for or retain DoD contracts. After Phase 2 enforcement begins on November 10, 2026, a contracting officer will not award a contract, exercise an option, or extend a period of performance if the offeror or contractor does not hold the required CMMC status in SPRS. For organizations whose revenue depends on DoD work involving CUI, the

loss of eligibility translates directly to loss of revenue. This risk is binary: the organization either holds the required certification or it does not. There is no provisional status that permits continued performance while the certification is pending, apart from the conditional certification pathway that requires an assessment score of at least 80 percent and remediation within 180 days.

Second Order: False Claims Act Exposure

The second most significant risk is legal and financial liability under the False Claims Act. As discussed in this paper, the DOJ has established through multiple enforcement actions that inaccurate SPRS score submissions, false affirmations of compliance, and misrepresentations of cybersecurity posture can result in settlements ranging from hundreds of thousands to millions of dollars. This risk is compounded by the qui tam provisions that incentivize whistleblower reporting. FCA exposure exists independently of whether the organization ultimately achieves certification. An organization that achieves certification but previously submitted an inflated SPRS score still carries the risk of enforcement action for the period in which the inaccurate score was on record.

Third Order: Supply Chain Disruption

For prime contractors, the failure of critical subcontractors to achieve CMMC certification creates execution risk. If a subcontractor that handles CUI cannot demonstrate the required CMMC status, the prime cannot award or continue the subcontract. This may require the prime to identify and qualify alternative suppliers under time pressure, potentially disrupting production schedules, delivery timelines, and contract performance. For subtier companies, the reciprocal risk is loss of position in established supply chains as primes shift work to certified competitors.

Fourth Order: Assessment Failure and Delay

An assessment that results in a finding of noncompliance or a conditional certification creates direct cost and schedule impact. The organization must

remediate the identified deficiencies and either complete a closeout assessment within 180 days (for conditional status) or schedule an entirely new assessment (for a noncompliance finding). The cost of reassessment, the operational disruption of a second assessment cycle, and the delay in achieving certification all compound the original investment. This risk is most effectively mitigated through thorough preparation during the enablement phase, which is the purpose of the readiness review that precedes the formal assessment.

Conclusion

The CMMC ecosystem is a structured regulatory environment with clearly defined roles, authorities, and boundaries. The separation between enablement and assessment is the central organizing principle of that structure, and understanding it is essential to making sound decisions about the path to certification.

For defense contractor executives, the key takeaways are these. The ecosystem has two sides, and they do not overlap. The enablement side, served by RPs, RPAs, and RPOs, helps organizations prepare. The assessment side, served by C3PAOs and their assessors, conducts the formal certification evaluation. No entity may perform both functions for the same organization. The required CMMC level is determined by the type of information the organization handles, and the requirement flows down through the supply chain from prime to subcontractor.

The Phase 2 enforcement date of November 10, 2026 creates a concrete deadline for CMMC Level 2 certification. The process of achieving certification typically spans twelve to eighteen months. The combination of implementation timelines, ESP compliance requirements, and C3PAO scheduling constraints means that organizations beginning the process today are operating within a reasonable but finite window.

The assessment process itself follows a rigorous, multi-phase methodology that culminates in the submission of results to the DoD through eMASS and their reflection in SPRS. Contracting officers will query SPRS to verify certification status before making award decisions. The accuracy of the organization's SPRS score is

not merely an administrative matter; the DOJ has established through enforcement action that inaccurate score submissions carry False Claims Act liability.

Certification is not a destination. It is the beginning of a recurring compliance cycle that includes triennial reassessment, annual affirmations, and continuous maintenance of the security posture that the assessment verified. The organizations that approach CMMC as an ongoing operational function, rather than a one-time project, will be best positioned to maintain certification and the contract eligibility it protects.

The ecosystem was designed to produce a credible, objective certification that the Department of Defense can rely upon in contract award decisions. Executives who understand the full scope of that ecosystem, from level determination through certification lifecycle, are better positioned to allocate resources, select the right partners, and manage the process on a timeline that protects their organization's competitive position in the defense industrial base.

About the Author

David W. Koran, RPA, is the Managing Partner of David Koran & Associates Inc., a CMMC compliance consulting firm serving Defense Industrial Base contractors and their legal counsel. He is a CyberAB Registered Practitioner Advanced, an Associate Member of the ABA Section of Public Contract Law, and the author of The CMMC Decision. He brings more than 30 years of IT and cybersecurity experience to his work with organizations navigating the CMMC certification process.