

# The Bottleneck

*97 Assessment Organizations. 80,000 Contractors that need assessment. Do the Math.*

***As of March 2026, the number of authorized C3PAOs (CMMC Third Party Assessment Organizations) for conducting Level 2 certification stands at approximately 97.*** On the other side of that equation, there are an estimated 80,000 organizations within the Defense Industrial Base that require these certifications to maintain contract eligibility. These figures represent actual data rather than projections or hypothetical scenarios. The result is a structural bottleneck in the CMMC ecosystem's supply and demand, and it is not a temporary constraint that will correct itself with time. This limitation will determine which contractors can compete for defense awards in 2027 and which cannot.

## Throughput Modeling and the 16-Year Gap

***Even under optimal assumptions, available throughput does not match the existing demand.*** If each of the 97 authorized C3PAOs conducted one certification per week, the total annual output for the ecosystem would be roughly 5,000 certifications. Against a demand pool of 80,000 contractors, this level of throughput would require over 16 years to clear the current backlog. While some C3PAOs operate multiple teams to increase capacity, even tripling this estimate does not close the gap within the timeframe required for 2027 contract eligibility.

### C3PAO Capacity: A Simplified Model

Factor	Estimate
Authorized C3PAOs (March 2026)	~97
Contractors Requiring Level 2 Certification	80,000+
Assessments per C3PAO per Year (at 1/week)	~52
Total Annual Ecosystem Throughput	~5,000
Years to Clear Backlog (at current capacity)	<b>16+</b>

*Note: This model assumes one assessment team per C3PAO and does not account for scheduling gaps, remediation cycles, or partial assessments.*

The purpose of this table is to establish that early engagement with a C3PAO is a scheduling reality rather than a competitive advantage. Contractors that delay until Q3 or Q4 of 2026 to begin the process are likely pushing their assessment timeline into 2027, which means missing the window that matters for contract eligibility.

## C3PAO Authorization Growth: Trajectory and Limitations

**The number of authorized C3PAOs has grown steadily, but the growth rate does not fundamentally alter the supply and demand equation.** In November 2021, there were 5 authorized C3PAOs. By December 2023, that number had increased to 48. By late 2024, the count stood at approximately 54. As of March 2026, it has reached 97. This represents an average annual growth rate of roughly 20 to 25 new authorizations per year across the full period.

Projecting this growth rate forward, the ecosystem might reach 120 authorized C3PAOs by the end of 2027 and approximately 145 by the end of 2028. These numbers represent meaningful progress. However, even at 145 C3PAOs operating at full capacity with multiple assessment teams, annual throughput still falls well short of the demand curve. The chart below illustrates this gap using a model that accounts for C3PAO growth, realistic assessment rates, consulting conflicts, and the compounding effect of failed assessments requiring reassessment.

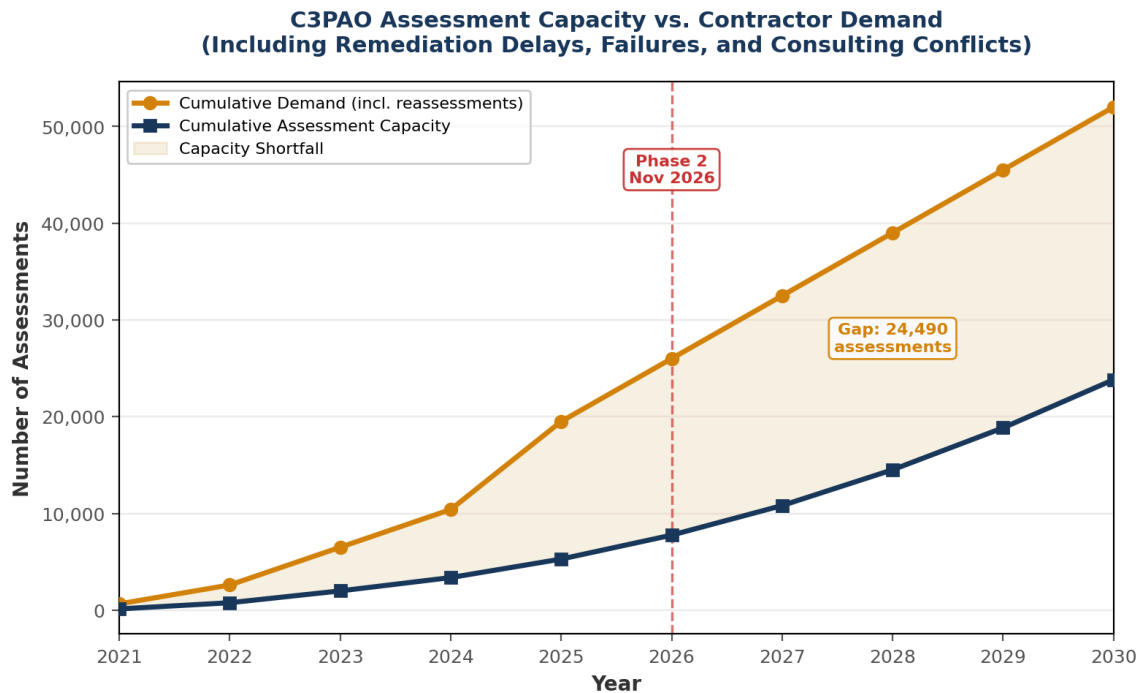


Figure 1: C3PAO Assessment Capacity vs. Contractor Demand (2021-2030 Projection)

### C3PAO Authorization Growth: Historical Data

Date	Authorized C3PAOs	Source
November 2021	5	Cyber AB Marketplace
December 2023	48	Industry Reporting
November 2024	54	Industry Reporting
March 2026	~97	Cyber AB Marketplace

Note: Counts reflect authorized status only. Candidate and applicant C3PAOs are not included.

## The Remediation Timeline: 12 to 18 Months Before Assessment Eligibility

***The bottleneck is not limited to the number of authorized C3PAOs. It extends backward into the remediation timeline that most contractors will require before they are eligible for assessment.*** A significant percentage of DIB contractors have not fully implemented the 110 security requirements defined in NIST SP 800-171 Rev 2. Many organizations have self-reported SPRS scores that reflect partial implementation at best. For these contractors, the path to a C3PAO assessment does not begin with scheduling. It begins with intensive control remediation that will require 12 to 18 months or longer, depending on the size of the environment, the number of deficient controls, and the complexity of the required technical changes.

Consider the practical scope of what remediation involves for a contractor that has not yet implemented foundational controls. Multifactor authentication must be deployed across all privileged and network access points. FIPS validated encryption must be implemented for CUI at rest and in transit. Audit logging must be configured, tested, and operationalized. System security plans must be written, reviewed, and maintained as living documents. A configuration management program must be established and documented. These are engineering projects rather than administrative checkboxes, and they require procurement, deployment, testing, user training, and operational validation. For a midsize contractor with a distributed environment, 12 months is an optimistic timeline and 18 months is more realistic.

The timeline extends further for aerospace and precision manufacturing contractors with operational technology environments. A machine shop running networked CNC equipment presents a remediation challenge that has very little in common with a standard office IT environment. Many CNC controllers operate on legacy platforms that cannot support endpoint protection, cannot be patched on a regular cycle, and were

never designed to exist within a segmented network. Creating a secure boundary around a shop floor requires VLAN segmentation, dedicated firewall rules between the operational network and the corporate network, and in many cases physical separation of systems that have historically shared a flat network. The contractor must determine which shop floor systems process or store CUI, which ones are in scope for assessment, and how to enforce access controls on equipment that may not natively support them. That scoping and segmentation work alone can take months before any of the 110 assessment objectives are addressed. For these organizations, an 18-month remediation timeline is realistic rather than conservative.

What this means in practice is that when modeling the demand side of this equation, it is not sufficient to look at the raw count of 80,000 contractors and assume they are all prepared to schedule assessments. A substantial portion of that population will spend the next 12 to 18 months in active remediation before a C3PAO can consider conducting their assessment. This does not reduce overall demand. It stretches it across a longer timeline, which may actually concentrate demand into a compressed window as contractors complete remediation simultaneously and compete for assessment slots during the same period.

## **Failed Assessments and the Reassessment Burden**

***Not every contractor that schedules a C3PAO assessment will achieve certification on the first attempt, and those that fail consume C3PAO capacity twice.*** A 2025 survey conducted by Alluvionic of authorized C3PAOs actively conducting Level 2 assessments provides concrete data on this issue. Approximately 50 percent of C3PAOs reported delaying or declining engagements due to gaps identified during preaward review. Roughly 80 percent of assessors cited assumed readiness without proper validation as the primary cause of rescheduling. These figures are based on frontline assessment experience rather than projections.

The problem often surfaces before the assessment even reaches the scoring phase. During Phase 1 of the CMMC Assessment Process, the C3PAO assessment team reviews the contractor's System Security Plan, validates the proposed assessment scope, and confirms that the organization's SPRS score aligns with what the documentation actually reflects. When the SSP is incomplete, outdated, or does not accurately describe the environment, or when the reported SPRS score does not match the reality on the ground, the assessment is halted. The C3PAO cannot proceed with an assessment against a security plan that does not represent the system as implemented. The engagement goes on hold, the contractor goes back to remediation, and the C3PAO's scheduling slot is consumed without producing a certification outcome, with no way to recover that lost time for either party.

When a contractor does proceed to a full assessment but receives a score below the 88/110 threshold required for conditional certification, the outcome is the same from a capacity standpoint. The C3PAO time invested in that engagement is not recovered. The assessment consumed the same scheduling window, the same assessor hours, and the same travel and preparation time that a successful assessment would have required. The contractor must then remediate their deficiencies and schedule a reassessment, creating a second demand event against an already constrained C3PAO population.

A conservative estimate of this reassessment burden is 25 to 30 percent. For every 100 assessments conducted, the ecosystem must absorb an additional 25 to 30 reassessments for contractors that did not achieve certification on their first attempt. This additional demand is not reflected in the raw 80,000 contractor count. It compounds on top of it. The effective demand on the C3PAO ecosystem is substantially higher than the surface number suggests.

## **The Consulting Conflict: Capacity Lost to Dual-Role Operations**

***There is an additional structural factor reducing effective C3PAO assessment capacity that is not immediately visible in the authorization numbers.*** Some C3PAOs are providing remediation and readiness consulting to contractors in addition to their assessment function. The CMMC ecosystem permits C3PAOs to operate in this dual capacity, provided they do not assess the same contractor they have consulted for. This restriction exists to preserve assessment independence. However, the practical effect is that every hour a C3PAO allocates to remediation consulting is an hour not spent conducting assessments.

For some C3PAOs, revenue from consulting engagements is more predictable and often more profitable than conducting assessments. A consulting engagement may span several months and generate sustained revenue, whereas an assessment is a discrete event with a defined endpoint. As a result, the economic incentive for some C3PAOs is to allocate a significant portion of their capacity to consulting rather than assessments. This is a rational business decision at the individual firm level, but it reduces the effective assessment throughput of the overall ecosystem.

Additionally, the conflict of interest restriction means that any contractor a C3PAO has consulted for must engage a different C3PAO to conduct their formal assessment. This creates a secondary bottleneck. The contractor has invested time and resources in a readiness engagement with one C3PAO and must now identify, schedule, and engage a completely separate organization for the actual certification. In a market where assessment slots are already constrained, this additional scheduling requirement further

extends timelines. A conservative estimate is that 15 to 20 percent of authorized C3PAOs are allocating a meaningful portion of their capacity to consulting at any given time, effectively removing that capacity from the assessment pool.

## **The Compounding Effect**

***Each of these factors in isolation would be manageable. Combined, they create a compounding capacity deficit that the ecosystem is not structured to absorb.*** Start with 97 authorized C3PAOs. Remove 15 to 20 percent of effective capacity due to consulting conflicts. Factor in a 25 to 30 percent reassessment rate that inflates total demand above the raw contractor count. Layer in the reality that a significant portion of the contractor population requires 12 to 18 months of remediation before they are eligible for assessment. The result is a system where effective capacity meets effective demand at a ratio that is fundamentally mismatched.

The chart above models this scenario. Even with projected C3PAO growth of 20 to 25 new authorizations per year, cumulative assessment capacity does not intersect with cumulative demand at any point within the foreseeable projection window. The gap widens before it narrows, which makes the case for planning with urgency rather than waiting for the market to self-correct.

## **The Phase 2 Trigger and Contract Eligibility**

***Phase 2 of CMMC enforcement begins November 10, 2026.*** This is the date when new DoD solicitations will begin including CMMC Level 2 certification as a condition of award. This does not mean that every contract issued on that date will require certification. It means the requirement begins appearing in new solicitations from that point forward. By November 10, 2027, contractors without certification risk losing eligibility for new awards entirely.

The practical consequence is straightforward: if your organization handles CUI and intends to compete for defense work beyond 2026, you need to be either certified or demonstrably in the certification pipeline before that Phase 2 trigger date. Contractors that treat this as a 2027 problem are the ones most likely to find themselves unable to bid on contracts they have historically depended on.

## **Implications for Readiness Planning**

***The bottleneck does not change your compliance obligations. It changes your timeline.*** The 110 assessment objectives within CMMC Level 2 remain the same

regardless of how many C3PAOs are available to assess against them. What changes is the urgency of completing readiness work before you need to schedule that assessment.

That means gap analysis should be happening now rather than after Phase 2 begins. Enclave architecture should be designed now, while there is still time to iterate and correct course. Your POA&M should reflect realistic timelines rather than emergency deadlines. It is also important to understand that a Conditional Certificate at a score of 88/110 represents a legitimate and planned outcome rather than a consolation prize. The organizations that frame conditional certification as a strategic target rather than a fallback position are the ones that will navigate this bottleneck successfully.

Additionally, contractors should factor the remediation timeline into their planning with clear eyes. If your organization has not yet implemented MFA, FIPS validated encryption, centralized audit logging, or documented configuration management, the remediation work ahead is measured in months rather than weeks. That remediation must be substantially complete before a C3PAO engagement will produce a useful result. Scheduling a C3PAO before your controls are in place does not accelerate the process. It consumes their time, your budget, and a scheduling slot that another contractor could have used.

## **The Bottom Line**

***The math is broken, but your strategy does not have to be.*** Ninety seven C3PAOs cannot serve 80,000 contractors within the timeframe the rule demands. Factor in remediation timelines of 12 to 18 months, a reassessment rate of 25 to 30 percent, and the effective capacity loss from C3PAOs allocating resources to consulting, and the real throughput falls even further short, based on the data that is currently available.

The contractors that understand the bottleneck, begin their remediation now, scope tightly, and target conditional certification at 88/110 will be positioned to bid when it counts. The contractors that wait will find themselves explaining to their leadership why they can no longer compete for the contracts they have always counted on.

Early engagement with the assessment process is less about gaining a competitive edge and more about avoiding the consequences of being too late to schedule one.

*David W. Koran is a CMMC Registered Practitioner and founder of David Koran & Associates, a CMMC readiness consulting firm serving Defense Industrial Base contractors and their legal counsel. He is an Associate Member of the ABA Section of Public Contract Law. He can be reached at [dkoran@davidkoran.com](mailto:dkoran@davidkoran.com)*