The Inverted Bottleneck

An Examination of CMMC Assessment Capacity, Readiness, and the SPRS Delta

David W. Koran

CyberAB Registered Practitioner Advanced

May 2026

Summary

The narrative that the CMMC ecosystem lacks enough assessors to certify the Defense Industrial Base on time has hardened into conventional wisdom over the past year. Contractors hear it from peers, vendors repeat it in marketing collateral, and trade press carries the claim forward without much examination. The published numbers do not support this narrative.

As of April 2026 the CyberAB ecosystem holds 766 Certified CMMC Assessors and 489 Lead CCAs. Those counts support 255 assessment teams capable of producing more than 12,000 assessments per year if each team conducts a single weekly assessment. Through April 2026 the industry has logged 1,240 Level 2 certifications in total. The current capacity could absorb that entire historical volume in a single month.

The bottleneck is not capacity. It is contractor readiness, compounded by hesitation tied to existing SPRS filings that may not reflect actual implementation. Summit 7 reports that between 25 percent and 40 percent of contractors who sign up for an assessment fail the readiness check before the formal assessment can begin. Those organizations do not fail an assessment in the technical sense, because the formal assessment never starts.

This paper examines the published capacity math, the live pay per click bid data drawn from a CMMC keyword research account in May 2026, the readiness gap that drives the false start phenomenon, the tooling and timeline mistake on the contractor side and the candor gap on the practitioner side that together produce many of those readiness failures, the role of SPRS deltas and False Claims Act exposure in slowing demand, and the second order risk that the shortage narrative will become self fulfilling as practitioners exit the ecosystem before demand arrives.

The Capacity Math

As of April 2026 the CyberAB ecosystem holds 766 Certified CMMC Assessors and 489 Lead CCAs. A CMMC assessment team requires at minimum one Lead, one

additional CCA, and a third CCA performing the quality assurance function. Dividing the assessor pool by three yields 255 possible assessment teams. If each of those teams conducts a single assessment per week, the ecosystem produces 1,020 assessments per month, or 12,240 per year. Through April 2026 the industry has logged 1,240 Level 2 certifications in total. The current capacity could absorb that entire historical volume in a single month.

The DoD's own demand projections appear in Table 8 of the 32 CFR Part 170 final rule. Those projections sit well below current ecosystem capacity at every phase. The Phase 1 estimate covering November 2025 to November 2026 projected 517 Level 2 certifications. Current capacity exceeds that figure by a factor of 24. The Phase 2 estimate projected 2,599 certifications. Current capacity exceeds that by a factor of five. The Phase 3 estimate projected 8,666 certifications, and the ecosystem is approximately two and a half years ahead of the capacity that target requires. Phase 4 steady state projects 16,610 assessments per year, a figure that requires 319 active teams.

The math holds even under far more conservative participation assumptions. A practitioner who looks at the raw assessor count and observes that not every CCA conducts assessments full time can still run the numbers. At 50 percent assessor participation the ecosystem produces 6,144 certifications per year. That figure exceeds the DoD's full Phase 1 estimate by an order of magnitude. At 25 percent participation, which is unrealistic on its face given the visible pool of CCAs actively marketing services, the ecosystem still produces 3,072 certifications per year. That number is more than double the throughput observed today.

The growth rate compounds the picture. The ecosystem is adding approximately 29 new CCAs per month, and ISACA's involvement in CMMC assessor training is expected to accelerate the pipeline. Even if the DoD's projections were understated by 20 or 50 percent, the current growth trajectory absorbs that gap without strain. The ecosystem is not capacity limited today, and it is moving further away from being capacity limited every month.

Market Signals from Pay Per Click and Advertising

Public discussion of CMMC marketing typically references high keyword costs without producing the underlying data. A snapshot drawn from the author's Google Ads research account on May 10, 2026 produces specific figures. Across 112 CMMC related keywords with active competitive bid data, the median top of page high-range bid is $28.36 and the mean is $43.45. Twelve keywords command top of page high-range bids above $100. The highest is $217.32 for "cmmc compliance consultant." The full set of keywords priced above $100 appears below.

Keyword	Top of Page Bid (High Range)
cmmc compliance consultant	$217.32
cmmc consulting services	$191.26
cmmc readiness services	$153.73
cmmc consultant	$153.22
c3pao assessment	$145.26
msp cmmc	$140.09
c3pao cost	$136.70
cmmc c3pao	$131.78
c3pao	$117.99
cmmc readiness assessment	$111.45
cmmc managed services	$104.40
cmmc compliance solution	$100.98

These figures describe a market in which providers are paying meaningful sums for each click on a single search term. The bid levels also reflect a particular experience within the practitioner community. C3PAOs, consultants, MSPs, and tooling vendors that entered the ecosystem expecting steady inbound demand in 2025 and 2026 have not seen that demand arrive at the volume anticipated, and are now competing for contractor attention through paid channels rather than receiving it through referral and inbound pipeline. The bidding visible at $217 for "cmmc compliance consultant" and $191 for "cmmc consulting services" is the visible consequence of that shift. Lifetime engagement value for CMMC work supports the economics of the bidding, and the underlying pattern is one of supply chasing a smaller pool of ready contractors than the original projections suggested. A genuine supply shortage would produce falling acquisition costs as urgency among providers eased, and the bid data shows the opposite pattern.

The pattern is not limited to consultants. "msp cmmc" carries a top of page high-range bid of $140.09, and "cmmc managed services" sits at $104.40. Managed service providers are competing for the same contractor attention as consultants and C3PAOs. The breadth of the bidding indicates that the supply side of the CMMC services market is broadly oversupplied for current demand, not narrowly so.

The same pattern shows in conference activity. CS5 West in San Diego in April 2026 saw a notable absence of major cloud providers from the expo floor, even as GRC vendors made aggressive claims about their CMMC offerings. Cloud providers go where the customers are. Their absence from the dominant CMMC industry event suggests that the customer volume promised by the shortage narrative is not yet visible in their pipelines.

Taken together these signals say something the published assessor counts and DoD projections also say. The supply side of the CMMC market is well staffed and working hard to attract contractors, while the demand side moves slowly. The story the marketplace tells through its purchasing behavior is the story the data confirms.

The Readiness Wall

The actual bottleneck sits on the contractor side. Summit 7 reports that between 25 percent and 40 percent of contractors who sign up for an assessment fail the readiness check before the formal assessment can begin. Those contractors do not fail a CMMC assessment in the technical sense, because the formal assessment never starts.

That outcome traces back to the head start contractors received. NIST SP 800-171 has been a contract requirement for unclassified DoD work since DFARS 252.204-7012 took effect in late 2017. Contractors that took the requirement seriously have spent five or more years implementing it. Contractors that treated the requirement as an attestation exercise are now arriving at the C3PAO door without the substrate the assessment is meant to verify.

Field experience confirms those numbers. Engagements undertaken during 2026 to date show a consistent pattern. Many contractors enter the initial readiness conversation with very few existing controls in place, or with controls that exist only on paper without operational backing. The assessment guide assumes a working set of 110 implemented controls and is not the right starting tool for an organization that has only a handful of those controls in place or none at all. The starting baseline determines the workload, and the workload determines the realistic timeline. A contractor that has been treating NIST SP 800-171 as an attestation exercise rather than as a control implementation effort is not three or four months from assessable but twelve to eighteen months from that point, and often longer if the existing technology environment requires structural change.

A C3PAO readiness check looks at whether an organization has the basic documentary structure and operational practices required to be assessed. Has the contractor scoped its CUI environment correctly? Are the system security plan and policies current and reflective of actual operations? Are the artifacts that demonstrate implementation of each control available and organized? When the answer to those questions is no, the formal assessment cannot proceed under the standards the C3PAO is required to apply.

The result is that the assessor pool sits idle while the contractor goes back to do the implementation work that should have been done over the prior five years. That delay is not visible in the assessor count. It is visible only in the gap between scheduled assessments and completed certifications, and in the slow pace at which new certifications are added to the CyberAB Marketplace each month. Since January 2026 only 25 to 80 Level 2 certifications have been added per month. The capacity to do far more is sitting in place, waiting for ready contractors to arrive.

The Three Month Illusion

A common refrain on the contractor side runs as follows. The company will purchase a GRC platform, sign a remote consulting engagement that operates primarily through video calls, and present itself for assessment within three to four months. The timeline often originates with the CEO, who anchors the projection on contract pressure or budget cycle considerations rather than on the work the standard requires. That timeline does not match the work the assessment will examine.

GRC tooling is a useful aid. It gives a contractor a place to store policies, track artifacts, and run a workflow against the 110 controls in NIST SP 800-171 Revision 2. The tooling does not implement the controls. Implementation is the act of changing how systems are configured, how people perform their work, and how the organization documents and reviews that work over time. The platform records the result of implementation but does not produce the result itself.

A remote engagement that runs entirely through scheduled video calls has a similar limitation. The consultant on the other end of the call can review documents, draft policies, and walk through control language. The consultant cannot directly observe the network, the manufacturing floor, the engineering systems, or the access patterns that the controls are meant to govern. Without that observation, the gap between what is documented and what is actually happening on the ground will not be closed. NIST SP 800-171A asks the assessor to verify operational implementation, not just policy text. A pure remote engagement can produce policy text but cannot on its own produce the operational record that supports the policy.

The realistic timeline for a contractor that begins with few or no controls in place and intends to engage a C3PAO for a full assessment is twelve to eighteen months. That window covers the time required to scope the CUI environment correctly, secure executive sponsorship and bring management into the role the standard assumes, draft and revise the system security plan against actual operations, configure or replace systems that do not meet the requirement, train staff on revised procedures, and run the controls long enough to generate the artifacts that demonstrate operation. Several control families require evidence of activity over time. Audit and accountability, security assessment, incident response, and awareness and training requirements cannot be conjured at the point of assessment. They have to operate in production for a period that gives the assessor genuine evidence to evaluate.

Management adoption is the most commonly underestimated element of that timeline. The CMMC standard assumes an organization in which executive leadership has approved the security program, signed off on the system security plan, allocated budget for the required tools and personnel, and committed to the ongoing procedural changes the controls require. In engagements observed during 2026, most contractors have handed the project to internal IT staff and treated it as a technical exercise. IT staff cannot enforce the organization-wide procedures the controls require, approve security policies on behalf of the company, mandate workforce training across departments, or commit the organization to the governance structures the affirming official role assumes. Without active executive sponsorship, the project stalls or produces a documentation set that does not reflect actual organizational practice. Building that executive engagement, often from a starting point where senior leadership has had limited exposure to the standard, consumes time that the typical IT-led project plan does not allocate. The early months of an engagement frequently go to that organizational work before the technical implementation can proceed against a stable management baseline.

The candor gap inside the practitioner community matters here. RPs, RPAs, CCAs, CCPs, and C3PAOs all hold credentials that imply a working understanding of what readiness requires. When a contractor asks whether three months is realistic, the candid answer is no for almost every contractor that has not already been working the requirement for several years, and that candid answer is not always what the

contractor receives. Some practitioners hesitate to push back on a prospective client. Others have built business models around faster engagements that depend on the contractor accepting an aggressive timeline. The result is a market in which the contractor receives reassurance that the timeline is workable, and the C3PAO readiness check later discovers that it was not.

That dynamic produces the false start phenomenon directly. A contractor that began with a three month plan, accepted reassurance that the plan was reasonable, and arrived at the C3PAO door without the operational record to support assessment is the same contractor that the readiness check turns away. The consulting engagement does not necessarily end at that point, because the readiness gap creates additional consulting work. The contractor loses the time invested, the budget allocated to the original assessment, and the contract opportunities that depended on certification within a planned window.

What this means for practitioners is a question of professional candor. The credentialing programs through CyberAB ask practitioners to act with integrity in their work. Setting a contractor up for an avoidable readiness failure does not meet that standard. Practitioners who push back on unrealistic timelines, who explain the operational evidence requirements honestly, and who scope engagements against the work the standard actually requires will produce contractors who reach assessment ready. Practitioners who do not will continue to feed the false start statistics that show up in C3PAO readiness checks.

The SPRS Delta and the Documentary Record

A second factor compounds the readiness gap. Many contractors filed SPRS scores in the 90 to 110 range, sometimes the maximum 110, without producing the artifacts those scores imply. DFARS 252.204-7019 requires those scores to be filed before contract award. Once filed they sit in a federal system, attached to contract awards, and exposed to False Claims Act review.

A contractor that engages a C3PAO and produces a Level 2 score materially below the SPRS filing creates a documentary record of the gap. That record may be reviewed by counsel for the contractor, by counsel for the prime, by the DoD, or by

qui tam relators. The exposure is not theoretical. Multiple FCA actions in recent years have used cybersecurity related representations as the basis for liability claims.

The result is hesitation. Contractors weigh the cost of an assessment that may reveal the delta against the cost of remaining where they are. Some choose to wait, hoping flowdown pressure does not reach them. Others take readiness seriously for the first time and discover that the work required to close the gap is substantial. A few engage counsel and begin a structured process to remediate the implementation, document the corrective actions, and update the SPRS filing. That process takes time, and it slows the rate at which contractors arrive at C3PAO doors ready to be assessed.

The SPRS delta is the unspoken reason behind a portion of the slow demand. It is also a reason that consulting work focused on scoping, implementation, and honest self attestation will continue to grow even as the assessor pool sits underutilized.

Phase 4 Steady State and the Growth Trajectory

Phase 4 of the CMMC rollout begins after November 2029. At that point every contractor in the Defense Industrial Base subject to CMMC will need to be on a three year recertification cycle. The DoD estimates that this steady state requires 16,610 assessments per year. That number translates to 319 active assessment teams running at one assessment per team per week.

The ecosystem is on track to reach 319 teams before Phase 1 ends in November 2026. At the current growth rate of 29 new CCAs per month, the assessor pool will pass the threshold required for Phase 4 steady state more than three years before that steady state is actually reached. ISACA's involvement in training is likely to push the growth rate higher rather than lower.

What this means for the next three years is that the ecosystem will hold excess capacity throughout Phases 1, 2, and 3. The capacity will be underutilized as the demand curve catches up with the supply curve. That underutilization will only

resolve in Phase 4 or later, when the recertification cycle adds steady predictable annual demand on top of new contractor certifications.

Practitioners considering the long term economic case for the CCA credential should weigh that timing carefully. The credential becomes economically robust when steady state begins. Until then individual practitioners face an uncertain demand environment in which paid work is available but not at the volume the early shortage narrative promised.

Practitioner Attrition and the Self Fulfilling Risk

CCAs and CCPs are working professionals. They held cybersecurity and IT roles before they pursued the CyberAB credentials, and many of them maintain those roles alongside their CMMC work. The credential carries cost. Training, examination fees, recertification, and the ongoing time commitment to remain current with assessment guidance and policy updates all add up.

A practitioner who watches assessment volume stay flat through 2026 will reasonably question whether the credential pays for itself. Some will let the credential lapse. Others will return their attention fully to general cybersecurity and IT consulting where billable demand is steadier. The ecosystem will lose practitioners not because the requirement disappeared but because the demand never materialized at the scale that was advertised.

That outcome creates a second order problem. When the demand surge does arrive, driven by prime flowdown notices, contract award gates in late 2026 and 2027, and the documented Phase 2 enforcement starting November 10, 2026, the ecosystem will have shed practitioners who would otherwise have absorbed the work. The shortage narrative may eventually become true, but only because the early shortage narrative drove practitioners to leave.

There is a real risk of equilibrium settling at a smaller assessor pool than the steady state demand actually requires. The pool that remains will consist of practitioners who have either built sustainable consulting practices around CMMC readiness

work or who can absorb the cost of the credential as part of a broader cybersecurity practice. Those practitioners are not the same population as the larger group that sat the exam in the past two years expecting steady assessment work to follow.

The Work Contractors Must Do

The work that needs to happen in the current window is not the production of more assessors. It is helping contractors close the readiness gap before they engage a C3PAO.

The first task is honest scoping. Many contractors do not yet know which of their systems handle Controlled Unclassified Information and which do not. Without that boundary established no implementation work can be measured against the requirement. Scoping is also where the heaviest cost reduction opportunities live, because correctly defining the CUI environment often cuts the assessable boundary substantially.

The second task is implementation against NIST SP 800-171 Revision 2. The control set has not changed in years. The artifacts required to demonstrate implementation are well documented in NIST SP 800-171A, the assessment guide. Contractors that have not built those artifacts need to build them. That is where the consulting hours will continue to flow.

The third task is honest self attestation. SPRS scores need to reflect actual implementation. Contractors that filed scores higher than the underlying evidence supports need to address the gap, in coordination with counsel, before a C3PAO engagement creates an unavoidable record of the delta. That process may include filing a corrected score, documenting the corrective actions taken, and recording the timeline that demonstrates good faith remediation.

These are the activities that move a contractor from unready to assessable. They are also the activities that the assessor pool cannot perform on a contractor's behalf, both because the rules forbid it and because the work belongs to the contractor.

Conclusion

The capacity to certify the Defense Industrial Base exists today and has for some time. The argument that the ecosystem cannot keep up with demand does not survive contact with the published assessor counts and the DoD's own projections in Table 8. What the ecosystem cannot do is move contractors through readiness on its own behalf, because the implementation work belongs to the contractor.

The next twelve months will determine which contractors close the gap and which contractors find themselves outside the eligibility line when prime flowdown notices reach them. The assessor pool is in place and waiting for ready contractors to arrive. The slow pace of those arrivals is the actual story behind the shortage narrative.

Practitioners, primes, and contractors should treat this picture as data rather than as a marketing message. The data identifies readiness, rather than capacity, as the constraint. Acting on that distinction reduces wasted effort, sets appropriate expectations for assessment timelines, and protects practitioners from the self fulfilling risk of leaving a credential behind in a market that will need them in three years.

About the Author

David W. Koran is the founder of David Koran & Associates, a consulting firm serving Defense Industrial Base contractors and their legal counsel. The firm's work focuses on CMMC readiness, enablement, and implementation. David holds the CyberAB Registered Practitioner Advanced credential and is an associate member of the ABA Section of Public Contract Law. He is the author of The CMMC Decision.

Contact: dkoran@davidkoran.com | (802) 335-2662

References

Summit 7. (May 2026). *The Numbers Behind CMMC Assessment Capacity*. YouTube. https://www.youtube.com/watch?v=e_1FztgNCHM

Department of Defense. (October 15, 2024). *Cybersecurity Maturity Model Certification (CMMC) Program*. 32 CFR Part 170, Federal Register. https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

National Institute of Standards and Technology. (February 2020, updated January 2024). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. NIST Special Publication 800-171, Revision 2. https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

National Institute of Standards and Technology. (June 2018, updated June 2021). *Assessing Security Requirements for Controlled Unclassified Information*. NIST Special Publication 800-171A. https://csrc.nist.gov/pubs/sp/800/171a/final

Defense Federal Acquisition Regulation Supplement. *252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting*. https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting

Defense Federal Acquisition Regulation Supplement. *252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements*. https://www.acquisition.gov/dfars/252.204-7019-notice-nist-sp-800-171-dod-assessment-requirements

Defense Federal Acquisition Regulation Supplement. *252.204-7020, NIST SP 800-171 DoD Assessment Requirements*. https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements

CyberAB. *The CyberAB Marketplace*. https://cyberab.org/Marketplace

Department of Defense. *Supplier Performance Risk System*. https://www.sprs.csd.disa.mil/