After the Starting Line:

What Post-November 2026 Looks Like

for the Defense Industrial Base

David W. Koran

CyberAB Registered Practitioner Advanced

April 2026

Introduction

Phase 2 of the Cybersecurity Maturity Model Certification program takes effect on November 10, 2026. From that date forward, Department of Defense solicitations and contracts will require Level 2 certification assessments conducted by accredited Certified Third-Party Assessment Organizations for most contracts involving Controlled Unclassified Information. Self-assessment will no longer satisfy the requirement.

Much of the current industry conversation focuses on how to prepare for that deadline. This paper addresses a different question: what happens after it arrives. The consequences of Phase 2 will not be confined to the organizations that fail to certify in time. The transition will produce ripple effects across the defense industrial base that reshape supply chains, redistribute contract opportunities, alter workforce dynamics, and create sustained legal and financial exposure for organizations at every tier. Understanding those effects is essential for executives who need to plan beyond the certification event itself.

The author was heavily involved in Y2K code repair for the banking, mortgage, and stock brokerage industries in the years leading up to January 1, 2000. That effort is instructive as a point of comparison. Y2K presented a hard deadline with serious operational consequences. The financial services industry recognized the risk early, mobilized resources, and executed a systematic remediation effort in which organizations repaired date-dependent code by converting two-digit year fields to four-digit formats. The work was completed before the deadline, and the result was that the stroke of midnight on January 1, 2000 passed without the catastrophic failures that had been projected. The reason it passed without incident was not that the threat was overstated. It was that the affected industries did the work in advance. The CMMC transition presents a similar hard deadline with similar operational consequences, but the defense industrial base is not responding with the same urgency. What the author observes across the contractor population is a widespread posture of waiting to see what happens, a belief that the deadline will slip, that enforcement will be soft, or that existing contracts will provide a buffer. That posture is fundamentally different from what the financial services industry

adopted in the face of Y2K, and the post-Phase 2 landscape will reflect the consequences of that difference.

The Divide: Certified and Uncertified

Understanding the post-Phase 2 landscape requires a clear picture of the two distinct roles that the CMMC ecosystem relies on to move contractors from noncompliance to certification. Certified Third-Party Assessment Organizations, or C3PAOs, are independent organizations authorized by the Cyber AB to conduct formal CMMC Level 2 assessments and issue certifications. They evaluate whether an organization has implemented the required 110 security controls and 320 assessment objectives, and they submit their findings for certification determination. Registered Practitioner Advanced professionals, or RPAs, are individually credentialed practitioners authorized to provide Level 2 readiness, enablement, and implementation advisory support. They work directly with contractors to scope the CUI environment, develop System Security Plans, implement technical and administrative controls, and prepare the organization for assessment. The CMMC ecosystem was designed with an intentional separation between these two roles, mirroring the audit independence principles used in financial accounting. The organization that advises a contractor on readiness cannot be the same organization that assesses and certifies it. That separation exists to preserve the integrity of the certification process, but it also means that the defense industrial base depends on two separate and independently constrained populations of qualified professionals to move contractors through the pipeline.

The starting condition for the post-Phase 2 environment is a defense industrial base that is sharply divided between organizations that hold Level 2 certifications and those that do not. As of early 2026, approximately 1,042 organizations out of the roughly 80,000 that the DoD estimates will ultimately need Level 2 certification have completed the process. Fewer than 100 C3PAOs are registered to conduct assessments, and fewer than 250 individuals hold the Registered Practitioner Advanced credential required to provide Level 2 readiness advisory support. Both the assessment pipeline and the upstream readiness pipeline are constrained, and neither has the capacity to close the gap before Phase 2 takes effect. At current

throughput levels, the assessment ecosystem cannot process the required population within any operationally relevant timeframe.

The nature of these two constraints is fundamentally different in a way that compounds the problem. A C3PAO assessment is a relatively short engagement, typically completed within two weeks for a single organization. A C3PAO can cycle through multiple assessments in a given quarter. By contrast, a Registered Practitioner Advanced working with a contractor on Level 2 readiness is engaged for twelve to eighteen months, guiding the organization through scoping, System Security Plan development, control implementation, policy and procedure creation, evidence collection, and personnel training. Each RPA can only carry a limited number of concurrent engagements, which means the readiness pipeline moves at a fundamentally slower rate than the assessment pipeline. The separation of duties within the CMMC ecosystem intensifies this dynamic. When a C3PAO encounters an organization that is not ready and halts the assessment during Phase 1 of the process, the C3PAO is prohibited from advising that organization on how to remediate the deficiencies. The contractor must then find an available RPA to address the gaps before it can reattempt the assessment. That contractor reenters the readiness queue, consumes additional RPA capacity, and eventually returns to the C3PAO queue for another assessment slot. The cycle consumes time and resources on both sides of the pipeline and increases demand for the already limited RPA population with each failed or halted assessment.

The result is that November 2026 will arrive with a large majority of the defense industrial base still uncertified. Some of those organizations will be in the assessment queue with C3PAO engagements scheduled. Others will be in various stages of readiness work. A significant number will have taken no meaningful action at all. The pool of organizations eligible to compete for new CUI contracts will shrink substantially on the day Phase 2 takes effect, and it will expand only as fast as the constrained assessment and readiness pipelines can process additional certifications.

Contract Recompetition and Program Disruption

Phase 2 applies to new solicitations and contracts issued after November 10, 2026. Existing contracts are not retroactively modified. That distinction provides a measure of continuity for work already under contract, but it does not insulate the defense industrial base from disruption. Contracts expire, options are exercised, and follow-on competitions are initiated on a continuous cycle. Each of those events becomes a point at which CMMC Level 2 certification status determines whether an incumbent can continue performing.

The author has observed that many contractors holding existing two- or three-year contracts believe they are insulated from Phase 2 pressure because CMMC requirements will not appear until their next recompetition. This is a false sense of security. Prime contractors are not waiting for contract option periods or follow-on solicitations to act. Primes are already distributing cybersecurity compliance questionnaires to their subtier suppliers, evaluating certification timelines, and building contingency plans to identify alternative sources. The objective for primes is straightforward: they need to protect their own compliance posture and cannot afford to discover at option exercise that a critical supplier is uncertified. Primes are actively identifying suppliers that will not certify and are positioning to replace them well before the November 2027 option period requirements take effect. A contractor operating under the assumption that an existing contract provides a buffer may find that the prime has already begun transitioning work to a certified competitor.

For programs that depend on specialized subtier suppliers, the risk is acute. If a sole-source or limited-source supplier has not achieved certification by the time a follow-on contract is awarded, the prime contractor faces a choice between delaying the award, finding an alternative supplier, or accepting the risk of a gap in the supply chain. None of those options is without cost. Qualification of alternative suppliers for precision-manufactured components, specialized coatings, or technical engineering services can require months or years of effort, testing, and

approval. The certification status of a single subtier supplier can create program-level schedule risk that flows upward through the entire contract structure.

Contracting officers will also face new complexity in source selection. CMMC certification status must be verified as a condition of award, adding a binary eligibility gate to the evaluation process. Organizations that would otherwise be competitive on technical merit, price, and past performance will be excluded if they cannot demonstrate a valid certification at the time of award. For contracting officers managing acquisitions with limited competitive pools, this may reduce the number of offerors to a level that complicates the competition itself.

Supply Chain Restructuring

The most significant long-term effect of Phase 2 will be the restructuring of defense supply chains. Prime contractors are responsible for flowing CMMC requirements down to subcontractors at the appropriate level. A prime that awards a subcontract involving CUI to an uncertified supplier introduces risk to its own compliance posture. The rational response, and the one that primes have already begun implementing, is to treat certification status as a prerequisite for subcontract eligibility. In practice, this means that primes will enforce CMMC requirements ahead of the government, because their own risk calculus demands it.

For small and mid-sized manufacturers that operate as subtier suppliers, this creates an existential pressure point. Many of these organizations have operated successfully in the defense supply chain for decades under the prior self-attestation framework. Their core competencies are in manufacturing, engineering, or technical services, not in cybersecurity compliance. The investment required to achieve and maintain Level 2 certification represents a significant cost relative to their revenue from defense work, and the specialized expertise required to navigate the process is in short supply. The same ecosystem constraints that limit C3PAO assessment capacity also limit the availability of qualified Registered Practitioner Advanced professionals who can guide these organizations through Level 2 readiness.

Some of these organizations will achieve certification and continue operating in the defense market. Others will conclude that the cost and complexity of compliance exceeds the value of their defense revenue and will exit the market voluntarily. A third group will be unable to certify in time and will lose their positions in the supply chain to certified competitors. In each case, the result is a contraction of the available supplier base for defense programs.

That contraction carries its own risks. A smaller supplier base means less competition, which can increase costs for the Department of Defense over time. It also means reduced redundancy. Programs that depend on a diverse supplier base for resilience will find fewer qualified options available, particularly in specialized manufacturing sectors where the number of capable firms is already limited. The Department of Defense has acknowledged the importance of maintaining a healthy industrial base, but the structural effect of CMMC on the smallest participants in that base has not been fully accounted for in implementation planning. In this respect, CMMC functions as a market filter as much as a security control, determining which organizations remain in the defense industrial base on criteria that are unrelated to their technical capabilities or the quality of their products.

The Affirming Official and Sustained Legal Exposure

Certification is not the end of legal exposure. It is the beginning. Under 32 CFR 170.22, a senior company executive designated as the affirming official must submit an annual affirmation in the Supplier Performance Risk System that the organization has implemented and will maintain all applicable security requirements. That affirmation is a legal certification submitted as a condition of contract eligibility, and it recurs every year for the life of the certification.

The Department of Justice has established a clear enforcement posture around cybersecurity compliance. At the ACI False Claims Act Forum in January 2026, Deputy Assistant Attorney General Brenna Jenny stated that cybersecurity enforcement cases are premised on misrepresentations, not on data breaches. An organization does not need to suffer a cyber incident to face liability. It needs only

to have submitted an affirmation that is false or was made with reckless disregard for the truth. The DOJ recovered $52 million in False Claims Act cybersecurity settlements in fiscal year 2025, and that figure is expected to grow as the population of certified organizations submitting annual affirmations increases.

For executives in the post-Phase 2 environment, this means that the moment of greatest legal risk is not the assessment itself. It is the period between assessments, when the organization must maintain its security posture without the external structure of a pending evaluation. Security controls degrade over time as systems are updated, personnel change, and operational pressures divert attention from compliance activities. An affirmation that was accurate at the time of certification may no longer reflect reality twelve or eighteen months later if the organization has not invested in ongoing monitoring and maintenance.

The affirming official requirement also creates a new category of personal risk for the individual who signs. Unlike a general corporate representation, the SPRS affirmation is tied to a named individual who is certifying specific compliance status. In a False Claims Act investigation, that individual's knowledge, diligence, and decision-making process will be scrutinized. Executives who sign affirmations without understanding the current state of their organization's compliance are assuming personal legal exposure that they may not fully appreciate.

Conditional Certification and the Rolling Wave of Lapses

A significant number of organizations that undergo C3PAO assessments in the months surrounding Phase 2 will receive conditional rather than full certifications. Conditional status is available to organizations that meet at least 80 percent of the 110 requirements, with the remaining deficiencies documented in a Plan of Action and Milestones. The conditional certification permits the organization to compete for and receive contract awards, but all POA&M items must be closed within 180 days. There is no extension mechanism.

The 180-day constraint creates a predictable pattern. Organizations that receive conditional certifications in the first quarter of 2027 will face POA&M closure deadlines in the third quarter of 2027. If a significant number of those organizations fail to close their items, the defense industrial base will experience a rolling wave of certification lapses that coincides with active contract performance periods. An organization that loses its certification while performing on a contract creates an immediate compliance problem for the prime contractor and potentially for the contracting officer who awarded the work.

Certain requirements are designated as non-POA&M-eligible, meaning they must be fully implemented before the assessment takes place. These are foundational controls drawn from FAR 52.204-21 and DFARS 252.204-7012. An organization that arrives at its C3PAO assessment without having implemented these baseline controls will not receive even a conditional certification. It will receive a finding of insufficient implementation, requiring a full reassessment after remediation. The cost and delay of a failed assessment, combined with the need to reenter the C3PAO scheduling queue, can add six months or more to an organization's certification timeline.

The aggregate effect of conditional certifications, POA&M failures, and reassessment cycles is a period of sustained instability in the certification landscape that will extend well into 2028. Program managers, contracting officers, and prime contractors will need to account for this instability in their planning and build contingency measures into their supply chain strategies.

Workforce and Competitive Dynamics

The certification divide will also influence workforce dynamics within the defense industrial base. Certified organizations will be positioned to compete for new contract awards, which means they will need to staff those programs. In sectors where the labor pool is already constrained, particularly in cleared technical positions, certified organizations will have a recruiting advantage over uncertified competitors that cannot offer the same pipeline of new work.

At the same time, organizations that exit the defense market due to the cost or complexity of CMMC compliance will release skilled workers into the labor pool. Some of those workers will migrate to certified competitors, effectively consolidating both contract portfolios and human capital among a smaller number of firms. The long-term effect is a defense industrial base that is more concentrated and less diverse at the small business and subtier levels than it was before CMMC implementation.

For organizations that achieve certification, the competitive landscape after Phase 2 presents opportunity alongside obligation. A certified organization competing against a reduced field of eligible offerors has improved win probability on individual procurements. The organizations that recognized this dynamic early and invested in readiness accordingly will be the primary beneficiaries of the post-Phase 2 transition. Those that arrive late to the certification process will find the competitive advantages already distributed.

The Regulatory Horizon: Revision 3 and Evolving Standards

CMMC Level 2 is currently anchored to NIST SP 800-171 Revision 2. The Department of Defense cannot transition the CMMC framework to Revision 3 without further rulemaking, and no such rulemaking has been initiated as of April 2026. For the immediate future, the certification target remains the 110 controls and 320 assessment objectives defined in Revision 2.

However, the General Services Administration published CUI protection requirements in January 2026 that are based on Revision 3, which introduces additional assessment objectives and represents a higher security bar. For organizations that hold contracts with both the Department of Defense and civilian agencies, this creates a diverging compliance landscape that will persist for several years. Meeting CMMC Level 2 requirements satisfies the DoD obligation but may not satisfy the GSA requirement.

The eventual transition to Revision 3 within CMMC is a question of when, not whether. Organizations that build compliance programs narrowly optimized for a single assessment cycle will face higher costs and greater disruption when the standard evolves. Those that build adaptable programs with strong documentation practices, mature change management processes, and ongoing security monitoring will absorb the transition more efficiently. The post-Phase 2 environment rewards organizations that treat compliance as a sustained operational discipline rather than a periodic event.

Conclusion

November 2026 is not the finish line for CMMC implementation. It is the point at which the program's effects begin to compound across the defense industrial base. The certification divide will reshape competitive dynamics, contract recompetition activity will test the resilience of supply chains, conditional certifications will create a rolling wave of compliance risk through 2028, and the affirming official requirement will sustain legal exposure for every certified organization on a recurring annual cycle.

The defense industrial base that emerges from this transition will be structurally different from the one that entered it. It will be smaller at the subtier level, more concentrated among certified firms, and subject to a continuous compliance obligation that did not exist under the prior self-attestation framework. The organizations that recognized these dynamics early and planned accordingly will hold the strongest positions in that reshaped landscape. The effects of Phase 2 will unfold over years, not months, and the decisions that executives make in 2026 will determine their organizations' standing in the defense market for the remainder of the decade.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced and the founder of David Koran & Associates Inc., a CMMC compliance consulting firm serving Defense Industrial Base contractors and their legal counsel. The firm provides readiness, enablement, and implementation advisory services for organizations navigating the CMMC certification process. David is an Associate Member of the American Bar Association Section of Public Contract Law and the author of *The CMMC Decision*. He can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

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

48 CFR Defense Federal Acquisition Regulation Supplement, CMMC Acquisition Rule, published September 10, 2025. https://www.federalregister.gov/documents/2025/09/10/2025-15596/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of-cybersecurity

Brenna Jenny, Deputy Assistant Attorney General, remarks at the ACI False Claims Act Forum, January 2026.

Cyber AB Town Hall, certification statistics, February 2026.

David McKeown, DoD Deputy Chief Information Officer, remarks at CMMC 2.0 Town Hall, February 2022. Estimated 80,000 DIB contractors requiring Level 2 third-party assessment. https://www.meritalk.com/articles/dod-expects-more-companies-to-need-cmmc-level-2-assessments/

Cyber AB Marketplace, C3PAO registry. https://cyberab.org

General Services Administration, CUI Protection Requirements, January 2026. https://www.gsa.gov

NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST SP 800-171 Revision 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, National Institute of Standards and Technology, May 2024.
https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/final