One Standard, Two Levels of Assurance: A Practical Path Forward for CMMC Level 2

How self-assessment can preserve small-business access while voluntary third-party assessment restores confidence for executives, prime contractors, and the Defense Industrial Base

David W. Koran

CyberAB Registered Practitioner Advanced

July 15, 2026

The Question Facing Contractors This Summer

In machine shops, engineering firms, and specialty suppliers across the defense supply chain, the same conversation has been running since July 13. The owner wants to know whether the third-party CMMC assessment the company budgeted for is still necessary, still available, or still worth anything. The information technology lead wants to know whether 2 years of security work just lost its purpose. The contracts manager wants to know what the primes will now require. And the executive who signs the annual affirmation in the Supplier Performance Risk System wants to know what evidence supports that signature, and whether the company could defend it if the government later challenged the underlying representations.

The Department of War answered one question decisively when it suspended advancement to CMMC Phase II: the planned phased expansion of mandatory third-party assessments was creating costs, capacity constraints, and timing problems the Department considered incompatible with expanding the Defense Industrial Base.[1] The suspension did not answer the harder question. Executives still must affirm compliance, prime contractors still must judge which suppliers can be trusted with CUI, and government programs still depend on the security of thousands of small companies. Suspending the planned expansion removed the immediate barrier, but it also cast doubt on the principal scalable, contractor-initiated mechanism for obtaining independent assurance.

This paper proposes a resolution that requires neither a return to the universal mandate nor an acceptance of unsupported attestation: a single cybersecurity standard with two levels of assurance. CMMC Level 2 Self should remain the affordable contractual entry point, as designated by the contract, while contractors should be permitted to pursue a voluntary official Level 2 C3PAO assessment when they need greater independent assurance, stronger credibility with prime contractors, or a better evidentiary basis for executive affirmation. The progression is for the contractor to implement the controls, complete a defensible self-assessment, build revenue and maturity, obtain independent assessment when the business case supports it, and then maintain the assessed environment. The proposal also carries a preservation purpose that should be stated openly. The mandatory C3PAO model may not return in its previous form, and the current review creates a material risk that independent assessment will be reduced or removed from the program rather than repositioned. This paper argues for repositioning it in a voluntary, market-driven form before that question is resolved by default.

What Changed on July 13, 2026, and What Did Not

On July 13, 2026, the Department of War announced the immediate suspension of CMMC Phase II, including the November 10, 2026 transition date, as well as pending and future CMMC implementation milestones in solicitations and contracts.[1] The accompanying memorandum from the Department of War Chief Information Officer, titled Removing Barriers to Defense Industrial Base Expansion, described the current program as structurally incompatible with the need to expand the industrial base, citing Small Business Administration reporting on prohibitive compliance costs, shortages in third-party assessment capacity, and regulatory timelines that were pushing small and nontraditional companies out of defense work.[2] A CMMC Reform Task Force will conduct a 60-day review, informed by a public request for information, and the Department has stated that further guidance will follow.[1]

The implementation memorandum gives the suspension its operational shape. During the suspension, program managers and requiring activities may designate only CMMC Level 1 Self or Level 2 Self in procurement requirements. They may not designate Level 2 C3PAO or Level 3 DIBCAC; contracting officers are directed to amend solicitations and contracts that already contain those requirements, and CMMC waiver procedures are suspended pending the review.[2]

Several things did not change. Phase I self-assessment requirements remain in place for applicable contracts, and the Department stated that it will continue enforcing NIST SP 800-171 Revision 2 through self-assessments and select government-led assessments.[1] DFARS 252.204-7012 and the underlying obligation to safeguard covered defense information remain fully in effect.[7] The regulation at 32 CFR Part 170 also remains on the books, including both the Level 2 Self pathway at section 170.16 and the Level 2 C3PAO pathway at section 170.17, along with the rule that achieving Level 2 C3PAO status also satisfies Level 2 Self for the same CMMC Assessment Scope.[3,4] The suspension did not repeal the regulation, and it did not eliminate C3PAOs.

Two points of precision matter for everything that follows. First, the suspension documents govern what government-required activities may be placed in solicitations and contracts. They do not expressly state whether a contractor that initiates a voluntary C3PAO assessment during the suspension will have that assessment processed through the CMMC instantiation of eMASS, transmitted to SPRS, and officially recognized; that question requires an explicit Department policy determination, and this paper treats voluntary assessments during the suspension as a proposal for the Department to adopt rather than an established option. Second, the outcome of the review is not predetermined, but the signals deserve a sober reading. The Chief Information Officer's

memorandum describes a future focused on tangible cyber hygiene rather than third-party certifications,[2] and the mandatory C3PAO model may not return in its previous form. The material risk the review poses is that independent assessment will be reduced or removed rather than repositioned, and the graduated model proposed here argues for repositioning it.

The Problem Mandatory Certification Tried to Solve

The original mandatory C3PAO model was not an arbitrary bureaucratic invention. It attempted to solve a real problem: the government had little reason to trust unsupported contractor self-assessments. The evidence for that distrust is public. In June 2026, the Department of Justice announced a settlement with LOGZONE Inc., a Huntsville, Alabama defense contractor that had reported a perfect self-assessment score of 110 for its NIST SP 800-171 implementation, and that the Defense Contract Management Agency later assessed at (negative) -170, near the bottom of a scoring range that ends at (negative) -203.[14] The settlement resolved allegations rather than adjudicated facts, but the gap between the self-reported score and the government assessment illustrates the assurance problem the original third-party assessment model was designed to address.

The mandatory model, however, created operational problems of its own, and the Department has now identified them in its suspension rationale: prohibitive compliance costs for small and emerging companies, severe shortages of third-party assessment capacity relative to the population requiring certification, and complex regulatory timelines.[2] In practice, implementation and remediation also require substantial lead time before any assessor arrives, particularly for contractors starting from immature systems, so the compliance clock ran long before certification was available. For nontraditional suppliers evaluating whether to enter defense work at all, the certification requirement functioned as an entry toll collected before the first contract dollar, and the Small Business Administration reported that capable companies were leaving or avoiding the Defense Industrial Base as a result.[2] Most fundamentally, the phased certification timetable was driven by procurement milestones rather than by an individual contractor's revenue, size, risk profile, or maturity.

The Risk That Self-Assessment Shifts Rather Than Removes

It would be a mistake to read the suspension as evidence that self-assessment solves the assurance problem. Moving broadly to self-assessment lowers the entry barrier, but the underlying uncertainty about whether the 110 requirements are actually implemented remains. It moves on to the company Affirming Official, who now signs an annual affirmation with no independent evaluation to back it. It moves on to prime contractors, who must decide how much due diligence to apply to each supplier's self-attested posture, to contracting officials who rely on SPRS data in award decisions, and to the government programs whose CUI will be handled by those suppliers. And it moves on to responsible contractors, who invest in genuine implementation and then compete for the same work against companies that post optimistic or unsupported scores.

The policy choice now before the Department should not be framed as a choice between continued progression toward broadly mandatory C3PAO assessments and indefinite reliance on unsupported self-assessment. That is a false binary, and both ends of it have already demonstrated their failure modes. The mandatory end priced small companies out of the industrial base. The unsupported end creates the risk of inflated scores and leaves the government to address material misrepresentations through audits and False Claims Act enforcement after the fact, one settlement at a time, which is the most expensive and least protective form of quality control available.

One Standard, Two Levels of Assurance

The graduated model proposed here maintains a single cybersecurity standard and varies only the level of independent assurance associated with it. Both pathways evaluate the same 110 security requirements of NIST SP 800-171 Revision 2, using the same NIST SP 800-171A assessment methodology, scoping rules, and scoring methodology.[5] A contractor that moves from Level 2 Self to Level 2 C3PAO is therefore not moving to a higher cybersecurity standard; it is moving from first-party assurance, in which the company evaluates its own implementation, to independent third-party verification that the same requirements are implemented within a defined assessment scope. The structure already exists in the regulation. Section 170.16 defines the self-assessment pathway, section 170.17 defines the certification pathway, and section 170.17 expressly provides that achieving Level 2 C3PAO status also satisfies Level 2 Self for the same CMMC Assessment Scope.[3,4] What the graduated model changes is the trigger. Instead of a phased government implementation that would progressively make certification a condition of award across applicable procurements, the contractor

chooses independent assessment when its revenue, risk profile, and customer relationships justify the investment.

Pathway 1: A Defensible Level 2 Self-Assessment

Level 2 Self remains sufficient where the contract designates it, and under the current suspension, it is the highest CMMC status a requiring activity may designate for CUI contracts. This pathway is what allows a 25-person machine shop to enter or remain in the Defense Industrial Base without financing a certification assessment before it has meaningful defense revenue. Preserving it is the access half of the policy.

The word self in Level 2 Self describes who performs the assessment, not how rigorous it is. A contractor on this pathway must still define an accurate CMMC Assessment Scope, identify every system that processes, stores, or transmits CUI, and implement all required security controls. It must conduct the assessment using the NIST SP 800-171A methodology, maintain a System Security Plan that reflects the environment as it actually operates, and submit a score into SPRS that the underlying evidence can support. Any Plan of Action and Milestones must stay within the limits of 32 CFR 170.21, which prohibits POA&M treatment for certain requirements and requires closeout within 180 days.[5] The Affirming Official must affirm continuing compliance at the time of the assessment and annually thereafter; the self-assessment must be repeated every 3 years, and the company must retain the assessment evidence and keep the controls operating between assessments.[3,5] The government also reserves the right under DFARS 252.204-7020 to conduct its own assessment, and a DIBCAC result takes precedence over a contractor-posted score.[3,8]

A self-assessment that consists of an informal questionnaire, a policy binder review, a consultant opinion letter, or a management declaration unsupported by evidence does not meet these requirements, whatever score accompanies it into SPRS. The LOGZONE matter shows where that path leads. A defensible self-assessment is a genuine assessment performed by the company against the published methodology, with objective evidence behind every MET determination.

Where Credentialed Practitioners Fit

Most small contractors entering defense work for the first time have never scoped a CUI environment, read an assessment objective, or calculated an SPRS score. This is where Registered Practitioners, Registered Practitioners Advanced, and Certified CMMC Professionals can do useful work on the self-assessment pathway. A competent

practitioner can help a company understand what CUI it actually receives and what its contracts flow down, define an assessment boundary that is neither too broad to afford nor too narrow to be honest, and map how CUI moves through people, systems, and service providers. From there, the practitioner can review the NIST SP 800-171 implementation requirement by requirement, help develop or correct the System Security Plan, organize the objective evidence, calculate a score the evidence supports, separate permitted POA&M items from prohibited ones, set remediation priorities, and establish the recurring processes that keep the program alive between assessments. Perhaps most valuably, a practitioner can prepare management and the Affirming Official to understand what the annual affirmation asserts before anyone signs it, and can position the company to graduate to a certification assessment later without rework.

Budget and funding guidance also belongs on this list. Federal and state programs, including the NIST Manufacturing Extension Partnership cost-share model and grant programs in several states with significant defense manufacturing sectors, can offset part of the readiness investment, and a practitioner familiar with them can help a client plan the project and its financing realistically.[15]

The limits of the role matter as much as its content. An RP, RPA, or CCP acting as a consultant does not issue an official CMMC status, does not certify compliance, does not sign the company affirmation, and does not substitute for the self-assessment the company itself must conduct and stand behind. Nor should engaging one be mandatory. Qualified internal personnel or other competent consultants can perform the same preparation work, and the value of these credentials must come from demonstrated competence and marketplace credibility rather than from any government-created consulting requirement.

Pathway 2: Voluntary Independent Assessment

The second pathway serves the contractor whose circumstances have changed. Defense revenue has grown from incidental to material. A prime has moved the company from occasional vendor to strategic supplier. The CUI footprint has expanded, or the Affirming Official has concluded that signing another annual affirmation on first-party evidence alone is no longer comfortable. At that point, the contractor should be able to obtain an official Level 2 C3PAO assessment voluntarily, on its own initiative and its own schedule, rather than waiting for a government mandate that may or may not return.

The mechanics already exist in section 170.17. An authorized or accredited C3PAO assesses the same requirements against the same methodology for a defined assessment scope, submits the results into the CMMC instantiation of eMASS with automated transmission to SPRS, and the record carries the CMMC unique identifier, the associated CAGE codes, and the conditional or final status.[4] A successful voluntary assessment would produce the official Level 2 C3PAO status for that scope, satisfy Level 2 Self for the same scope under the existing rule, give the Affirming Official an independently supported basis for the required affirmation, give prime contractors a reusable supplier-assurance credential, and reduce the need for duplicative customer assessments of the same requirements. What the Department must do, as part of or following the current review, is confirm explicitly that contractor-initiated voluntary assessments are permitted, accepted into the CMMC instantiation of eMASS, transmitted to SPRS, recorded, and officially recognized. That approach would leverage the assessment infrastructure, regulatory framework, and data systems already established under 32 CFR Part 170.

A Verifiable Third-Party Assessed Credential

For the voluntary pathway to carry commercial weight, its result needs to be visible and verifiable. The plain-language commercial description proposed here is Third-Party Assessed, tied directly to the official Level 2 C3PAO status rather than existing as a decorative private logo. An authorized customer checking the credential should be able to verify the contractor identity, the applicable CAGE codes, the CMMC unique identifier or equivalent assessment identifier, the C3PAO status, the assessment date and expiration date, whether the status is conditional or final, the defined assessment scope, whether the current annual affirmation is in place, and whether any material change has called continued reliance into question.

Two disciplines keep the credential honest. First, it must be scope-specific. A certification covering one CUI enclave at one facility must not be presented as covering the whole company, every facility, every subsidiary, or every information system unless that is actually true, and the verification record should make the scope plain. Second, it must claim only what an assessment can support. An assessment establishes that defined requirements were verified as implemented within a defined scope as of a defined date. It does not make a contractor breach-proof, completely secure, or immune from enforcement, and the credential should never be marketed as such.

The registry that supports verification can be controlled without being secret. A model already operates in aerospace quality: the IAQG OASIS database lets customers confirm that a supplier holds a recognized certification, see its status and scope, and check currency, without exposing the underlying audit working papers.[10] A CMMC equivalent

would let a prime verify supplier assurance without gaining access to detailed vulnerabilities, assessment evidence, network diagrams, or sensitive findings, all of which should remain between the contractor, the assessor, and the government systems of record.

The AS9100 Precedent

Aerospace manufacturing already employs a mature version of the voluntary assurance model proposed in this paper. AS9100 is not imposed as a universal federal regulatory requirement, although customers and individual contracts may require it; yet it has become a practical prerequisite for participation in much of the aerospace supply chain because the ecosystem around it works. There is a broadly recognized industry baseline, a population of independent certification bodies, qualified auditors working to a consistent audit methodology, and a verifiable registry in OASIS where certifications are recorded and a lapsed or withdrawn certificate becomes visible.[10] Customers accept the recognized certificate in supplier selection and surveillance; that recognition can reduce duplicative supplier reviews, allow customer surveillance to focus on contract-specific risks rather than repeatedly examining the full quality-management baseline, and give suppliers that invest in certification commercial value for having done so.

The analogy has limits that should be stated plainly. AS9100 is a quality management standard, not a cybersecurity regulation; it is not legally equivalent to CMMC, and holding it substitutes for nothing in DFARS. The lesson is narrower and more useful: third-party assessment becomes valuable when customers trust and recognize it, not merely because the government forces every supplier to purchase it. Many aerospace and defense manufacturers already operate within the AS9100 certification ecosystem and will understand a voluntary Level 2 C3PAO status on the same commercial terms, as an investment justified by customer recognition.

What the Affirming Official Actually Gains

The obligation to affirm deserves precise treatment because it is where wishful thinking does the most damage. A voluntary C3PAO assessment does not remove responsibility or legal risk from the Affirming Official. The framework requires affirmation following a Level 2 C3PAO assessment and annually thereafter, just as it does on the self-assessment pathway.[4,5] No certificate signs the affirmation for the executive, and none ever will.

What the assessment changes is the factual foundation under the signature. An Affirming Official relying solely on a self-assessment is affirming based on the work of

the same organization whose compliance is in question. An official relying on a current, properly scoped independent assessment has third-party support for the condition of the assessed environment as of the assessment date, which materially strengthens the factual and evidentiary basis for the affirmation. That is a real difference, and for many executives it will be the difference that justifies the cost of the assessment.

The official remains responsible for everything the assessor could not see or that happened after the assessor left: truthful disclosure to the assessment team, the accuracy of the assessment scope, changes to systems, facilities, service providers, or CUI flows, known control failures, the continuing operation of the controls between assessments, prompt investigation and remediation of newly discovered deficiencies, and avoiding any representation that conflicts with facts the official knows. Independent assessment reduces uncertainty and supports due diligence. Concealment and deliberate ignorance do not transfer to anyone.

The False Claims Act, Considered Honestly

Since the Department of Justice launched its Civil Cyber-Fraud Initiative in October 2021, cybersecurity representations to the government have carried False Claims Act consequences, and the pace has increased rather than slowed.[11] Aerojet Rocketdyne paid 9 million dollars in July 2022 to resolve allegations that it misrepresented its cybersecurity compliance.[12] The Department of Justice reported more than 52 million dollars across nine cybersecurity fraud settlements in the fiscal year ending September 2025, and stated that civil cybersecurity settlements had more than tripled in each of the 2 preceding years.[13] The June 2026 LOGZONE settlement shows the government building a case directly on the gap between a contractor-posted SPRS score and a later government assessment.[14] The Aerojet and LOGZONE matters resolved allegations rather than adjudicated findings, and the Department of Justice expressly stated in the LOGZONE announcement that there was no determination of liability, a distinction that should be preserved whenever these cases are discussed.

Against that backdrop, no responsible advisor should tell an executive that a C3PAO assessment eliminates FCA liability, creates a safe harbor, or guarantees that reasonable care was exercised. What a properly performed independent assessment can do is generate contemporaneous evidence of reasonable diligence, support the accuracy of the representations made at the time, and demonstrate good-faith reliance on qualified outside evaluation. It can also do something less comfortable and equally valuable: identify deficiencies management must then address. An assessment finding that management receives and ignores could increase rather than reduce exposure because it converts a compliance gap into a known one.

This paper proposes, as a policy recommendation and not a statement of current law, that the Department of War and the Department of Justice establish formal enforcement credit for good-faith reliance on a current, properly scoped C3PAO assessment. The credit, however styled in enforcement guidance, should apply only where the Affirming Official confirmed that the assessment scope covered the relevant environment, disclosed fully to the assessor, lacked actual knowledge of a material unmet requirement, maintained reasonable change-monitoring procedures, promptly investigated credible concerns, and disclosed and remediated material deviations. Enforcement guidance cannot bind a court's evaluation of knowledge, materiality, or reliance, but it would reward the behavior the government wants: verified implementation and honest disclosure, without shielding the behavior it prosecutes.

What Prime Contractors Gain

Prime contractors carry an assurance problem the suspension made harder, not easier. A prime flowing CUI to hundreds or thousands of subcontractors needs a scalable way to differentiate supplier risk, and a patchwork of subcontractor representations, voluntarily shared SPRS verification, and customer-specific questionnaire responses does not provide a uniform independent assurance signal. A subcontractor relying on Level 2 Self may remain fully eligible under the contract, but the prime may reasonably apply more supplier due diligence to that score: evidence sampling, scope verification, additional contractual representations, or ongoing monitoring. A subcontractor holding a current official Level 2 C3PAO status gives the prime something categorically stronger: an external assurance signal generated by an authorized assessor against the published methodology.

Reliance still requires verification, which the credential described above makes fast. The prime should confirm that the assessment is current, that the CAGE codes match the entity performing the subcontract, that the CUI flowing under the subcontract will remain within the assessed scope, that the annual affirmation is in place, and that no known material change undermines reliance. Where those checks pass, and no contradictory information or contract-specific risk exists, the prime should be permitted to accept the current independent status rather than repeat a full proprietary audit against the same requirements. That acceptance is where the business value of the voluntary pathway becomes tangible for the supplier: faster onboarding, preferred-supplier consideration, fewer duplicative questionnaires, fewer customer-specific cybersecurity audits, stronger access to sensitive work packages, better standing in supplier-risk scoring, and, for small suppliers a prime considers critical, the realistic possibility of prime sponsorship or cost sharing for the assessment itself. None of this makes the prime automatically immune from liability because a

subcontractor held a certificate, and no prime should treat it that way; it makes the prime's diligence cheaper, faster, and better documented.

The Incumbent's Objection

The fairest objection to a voluntary model comes from the contractor that already has the work. If the contract requires only Level 2 Self and the orders keep arriving, why pay for a third-party assessment? For some contractors, the objection simply wins, and a model that depended on universal uptake would fail; universal uptake was the mandate's mistake, not this proposal's goal. The incentives that move a contractor arrive with time and exposure. Existing work is re-decided at every recompete, option exercise, and follow-on award, which are exactly the moments when a prime performing supplier-risk triage can distinguish a self-attested score from a verified status. The Affirming Official feels a second form of pressure with each annual signature supported only by the company's own evidence, and the LOGZONE matter shows the downside when a later government assessment contradicts the posted score. A third incentive is arithmetic: a supplier answering security questionnaires and hosting customer audits from three or four primes each year is already paying for assurance in fragments, and a single recognized assessment beats that cost the moment primes accept it in place of their own reviews.

There is also a quieter effect, and it may be the most important one. Any contractor serious about protecting government information will take its self-attestation seriously precisely because it knows the outcome of a future move up to a C3PAO assessment depends on it. Both pathways evaluate the same requirements using the same methodology within the same defined scope, which means the self-assessment is not a disposable formality but the working foundation that an independent assessor will later re-examine. A company that scopes honestly, gathers real evidence, and posts a score the evidence supports arrives at its certification assessment with most of the work already done. A company that inflates its self-assessment converts every unsupported MET determination into a future finding, discovered at the worst possible time and at the company's own expense. The graduated model therefore raises the quality of self-attestation across the population, including among contractors that have not yet purchased an assessment, because the pathway upward keeps the pathway at entry honest.

Preventing a Hidden Mandate

The principal weakness of a voluntary model is that it may not stay voluntary. A large prime could write a third-party assessment into its standard subcontract terms for every

supplier, and the entry barrier the Department just dismantled at the contract line would reappear one tier down, imposed by flowdown instead of regulation. If every prime does this reflexively, the voluntary credential becomes a pay-to-play condition for all defense work, and the access half of the policy fails.

The corrective is a norm that the Department can articulate and that primes can adopt. Primes should be free to recognize Level 2 C3PAO status as a positive supplier-risk factor, to prefer it, and to reward it, but they should not impose it universally where the government contract requires only Level 2 Self unless a documented contract-specific, program-specific, or CUI-risk justification supports the requirement. Small contractors must retain a legitimate self-assessment pathway into the industrial base. The credential should function as an earned advantage, not an admission ticket.

A Sustainable Division of Labor

A graduated model gives the CMMC ecosystem a durable structure, though preserving anyone's revenue is not the reason to adopt it. The division is simple: the RP, RPA, or CCP prepares and helps sustain the contractor's program, and the C3PAO independently evaluates it. The line between preparation and assessment must stay clean, and the regulation already draws it precisely. Under the Code of Professional Conduct requirements of 32 CFR 170.8(b)(17), CMMC Ecosystem members are prohibited from participating in the Level 2 certification assessment process for an organization they previously served as a consultant to prepare for any CMMC assessment within 3 years.[6] Because a CCP may also serve on a C3PAO assessment team, that restriction operates at the individual level as well as the organizational one. A voluntary market makes this independence more important, not less, because a credential earns commercial trust only as long as customers believe the assessor had no stake in the outcome.

There is also a capability argument the review should weigh. The assessment infrastructure of authorized C3PAOs, certified assessors, and the accreditation and training apparatus behind them took years to build, and it will not idle indefinitely without a market; organizations will exit the business and assessors will move to other work. A voluntary pathway would preserve much of that existing capability without requiring the government to build a new assurance structure, keeping independent assessment available for critical programs, high-risk suppliers, or a future policy direction. The alternative on the current trajectory is not a leaner mandatory program; it is the gradual loss of the assessment infrastructure itself.

How a Small Machine Shop Would Use This

Consider a 30-person aerospace machine shop, AS9100-certified, that has built its business on commercial aviation work and receives its first meaningful defense opportunity: a subcontract from a tier-1 supplier that will place technical drawings marked as CUI in the shop's hands. Under the graduated model, the company does not begin by pricing a certification assessment. It begins by containing the problem. Working with an RPA or a CCP, or with qualified internal staff, it defines a limited CUI enclave, a small set of systems and people that will receive, store, and use the controlled drawings, rather than dragging its entire enterprise network into scope. The practitioner helps map the CUI flow, review the requirements against the enclave, close any gaps, build the System Security Plan, and assemble objective evidence.

When, and only when, the requirements are implemented, the company conducts its Level 2 self-assessment, posts a score the evidence supports, and its Affirming Official signs the affirmation, understanding exactly what it asserts. The company becomes eligible to compete for and perform the work without having financed a certification assessment it could not yet justify. Over the following 2 to 3 years, defense orders grow from an experiment into a product line, and contract revenue funds better infrastructure, additional staffing, tighter documentation, and continuous monitoring, the same pattern by which the shop once matured into its AS9100 certification. When a second prime begins asking detailed supplier-assurance questions and defense work reaches a share of revenue worth protecting, the business case for independent assurance closes on its own terms. The company engages a C3PAO with which it has no prior relationship, undergoes a voluntary assessment, and converts its self-assessed status into a Third-Party Assessed credential that both primes can verify without each having to repeat a full baseline audit of the same requirements. Nothing in this progression allowed the company to delay required controls until revenue arrived, and no consultant guaranteed the assessment result. The requirements were implemented before the first self-assessment was represented as compliant; what changed over time was who verified them.

Policy Recommendations

The Department's 60-day review is the right moment to build the graduated model into whatever framework follows. Twelve specific recommendations:

1. Retain Level 2 Self as the baseline entry pathway where designated by the contract.

2. Explicitly authorize contractor-initiated voluntary Level 2 C3PAO assessments during and after the current review.

3. Ensure that contractor-initiated voluntary official assessment results are accepted into the CMMC instantiation of eMASS, transmitted to SPRS, recorded, and officially recognized.

4. Preserve the existing rule that Level 2 C3PAO status satisfies Level 2 Self for the same CMMC Assessment Scope.

5. Create a verifiable, scope-specific Third-Party Assessed supplier designation tied to official C3PAO status.

6. Permit prime contractors to accept the credential in place of duplicative reviews of the same requirements when the scope matches the subcontract.

7. Establish formal enforcement credit recognizing good-faith reliance on a current assessment as evidence of due diligence, without creating blanket False Claims Act immunity.

8. Require annual affirmation, material-change monitoring, and prompt action whenever continued compliance is called into question.

9. Preserve a meaningful role for RPs, RPAs, and CCPs in preparation, remediation, self-assessment support, and continuing compliance, based on competence rather than mandate.

10. Preserve C3PAO independence, including the existing 3-year restriction on preparers participating in the certification assessment.

11. Prevent the voluntary pathway from becoming an automatic universal subcontract requirement where the government contract requires only Level 2 Self.

12. Build the program around measurable security operations and evidence rather than possession of documents or a decorative certificate.

Conclusion

The Department suspended advancement toward the broader mandatory third-party assessment model after concluding that its cost, capacity, and implementation structure were creating unacceptable barriers to participation in the Defense Industrial Base, while self-assessment alone does not provide the level of assurance that executives who sign affirmations, primes who select suppliers, and government programs whose CUI is at stake actually need. Both of those statements are true at the same time, and the current review will fail if it honors only one of them. The risk on the present trajectory is

that independent assessment is removed rather than repositioned, which would trade one mistake for its mirror image and surrender an assessment capability the Department spent years standing up.

The practical answer is not to eliminate independent assessment. It is to stop using it as the only doorway into the Defense Industrial Base. Small contractors should be able to enter through a defensible self-assessment, supported where necessary by competent practitioners, and as a contractor grows, takes on greater risk, or needs stronger credibility, it should be able to earn an independently assessed status that primes and government customers recognize and can verify. The standard never changes; the assurance behind it rises with the stakes. Self-assessment should provide the entry point, and independent assessment should become the credential a serious defense contractor chooses to earn.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced (RPA) and the founder of a consulting practice serving Defense Industrial Base contractors and their legal counsel. His work focuses on CMMC readiness, enablement, and implementation; his firm performs consulting engagements. He 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

1. Department of War, "Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements," July 13, 2026. war.gov

2. Department of War Chief Information Officer, memorandum, "Removing Barriers to Defense Industrial Base Expansion: Immediate Suspension and Strategic Review of Cybersecurity Maturity Model Certification Requirements," July 13, 2026, and companion memorandum, "Implementing Department of War Chief Information Officer's Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements." Available via the Department of War CIO CMMC page: dodcio.defense.gov/cmmc

3. 32 CFR 170.16, CMMC Level 2 self-assessment and affirmation requirements. ecfr.gov

4. 32 CFR 170.17, CMMC Level 2 certification assessment and affirmation requirements. ecfr.gov

5. 32 CFR 170.19 (CMMC scoping), 170.21 (Plan of Action and Milestones requirements), 170.22 (Affirmation), and 170.24 (CMMC Scoring Methodology). ecfr.gov, Part 170

6. 32 CFR 170.8(b)(17)(ii)(G), Code of Professional Conduct policy, prohibiting CMMC Ecosystem members from participating in the Level 2 certification assessment process for an assessment in which they previously served as a consultant to prepare the organization for any CMMC assessment within 3 years. ecfr.gov, Subpart C

7. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. acquisition.gov

8. DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements. acquisition.gov

9. DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements. acquisition.gov

10. International Aerospace Quality Group, Online Aerospace Supplier Information System (OASIS). iaqg.org/tools/oasis

11. U.S. Department of Justice, "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative," October 6, 2021. justice.gov

12. U.S. Department of Justice, "Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Case," July 8, 2022. justice.gov

13. U.S. Department of Justice, False Claims Act Settlements and Judgments, Fiscal Year 2025 fact sheet. justice.gov

14. U.S. Department of Justice, "Alabama Defense Contractor Agrees to Pay $507,144 to Resolve False Claims Act Liability Relating to Cybersecurity Violations," June 18, 2026, and associated settlement agreement. justice.gov

15. David W. Koran, "Need Funds for Your CMMC Program? Federal and State Grant Funding for Defense Manufacturing," March 2026, davidkoran.com; see also National Institute of Standards and Technology, Manufacturing Extension Partnership, nist.gov/mep.