The CMMC Cost Stack

What Compliance Actually Costs the Defense Industrial Base

David W. Koran

CyberAB Registered Practitioner Advanced

May 2026

David Koran & Associates, Inc.

Summary

This paper maps the full cost of CMMC compliance for contractors in the Defense Industrial Base. The central argument is that the total cost is substantially higher than what contractors and primes publicly acknowledge, that the cost is distributed across categories practitioners rarely discuss together, and that the cumulative pressure is producing supply chain consolidation rather than supply chain compliance.

The cost conversation in the trade press, in vendor marketing, and in regulatory discussion has been piecemeal. A contractor reads about consulting costs in one article and tooling costs in another, while the C3PAO fee gets named in one webinar and the ongoing maintenance cost gets named in another. Each category alone seems manageable, and the complete picture is harder to find because no single party has a strong incentive to publish it.

The paper serves three audiences. Contractors who need to understand what CMMC will actually cost them across the full compliance cycle. Primes and large enterprises who need to understand the cost burden their supply chain is absorbing and the consolidation pressure that follows. Legal counsel advising on contract cost recovery, FCA exposure, and supply chain risk who need a defensible analytical framework for the cost question.

The paper is not a price list. It is a structural analysis of the cost categories, the cost drivers within each category, the cumulative effect across the compliance cycle, and the strategic implications for the contractor base. The figures cited are practitioner observations from current engagements rather than vendor list prices, because the actual cost a contractor pays differs from published list prices once the operational reality of each contractor situation is taken into account.

The provocation is that the piecemeal cost conversation has produced the false impression that CMMC compliance is more affordable than it is. Mapping the full stack honestly makes the consolidation pressure visible, and forces a different conversation about which contractors can realistically remain in defense work as Phase 2 begins and as the recertification cycle takes hold over the next three years.

Section 1. The Cost Conversation Most Practitioners Avoid

The cost of CMMC compliance has been discussed in public, in trade press, in vendor marketing, and in regulatory commentary since the program was first announced. What has not been published is a complete map of what compliance actually costs a contractor across the full compliance cycle. The partial conversation is not accidental but rather structural.

Practitioners who deliver readiness consulting have legitimate reasons to be cautious about publishing total cost figures. The figures vary by contractor and by engagement, and overgeneralizing risks producing client conversations where actual figures land differently from published expectations. Practitioners working in legal counsel are constrained by client confidentiality and by the legal sensitivity of the FCA exposure that runs through SPRS attestations. Practitioners who serve as MSP and ESP providers have business reasons to highlight some of their cost categories and minimize others. Each practitioner category contributes to the cost conversation but each contributes only a portion of the total picture.

Vendor incentives compound the gap. A GRC platform vendor publishes pricing on the GRC platform but does not discuss the consulting cost required to make the platform produce usable evidence. A C3PAO publishes assessment pricing but does not discuss the readiness cost required to make the assessment passable. A cloud provider publishes infrastructure pricing but does not discuss the integration cost required to make the infrastructure CMMC-aligned. Each vendor speaks honestly about the piece they sell. The cumulative picture requires combining vendor perspectives in a way that no single vendor has the incentive to produce.

Trade press coverage follows the same pattern, with articles on CMMC cost typically addressing one category at a time, whether C3PAO pricing, GCC High licensing, or consulting rates in isolation. Each piece holds the reader attention by treating one cost category alone. The complete picture would require the reader to assemble figures from a dozen separate articles, and few readers do that work.

Contractors discover costs sequentially rather than in advance. A contractor begins CMMC readiness with a budget that addresses the costs the contractor anticipates. Additional costs emerge as readiness work progresses, including tooling costs the contractor did not budget, infrastructure changes the contractor did not anticipate, MSP service expansion the contractor did not plan, and insurance premium adjustments the contractor did not foresee. By the time the contractor reaches assessment, the actual cost has exceeded the initial budget substantially. This pattern is not the result of contractor failure but rather the result of the partial cost conversation that produced the initial budget.

The Government Accountability Office addressed the cost question in March 2026 in report GAO-26-107955. The report identified program demand as an external risk factor that DoD should evaluate because CMMC program costs and requirements may affect the extent to which existing DIB companies decide to continue doing business with DoD. The report further noted that small businesses may decide not to participate in the program due to the cost associated with assessment and certification. The GAO concern was structural, recognizing that cost has been treated as a known variable when the total cost is not yet known publicly in a form that contractors can use to make participation decisions.

DoD's own regulatory cost model in 32 CFR Part 170 is not a full contractor compliance budget. The model prices the assessment, reporting, and affirmation burden, while excluding Level 1 and Level 2 implementation and remediation costs on the premise that those costs should already have been incurred under existing FAR 52.204-21 and DFARS 252.204-7012 obligations. The exclusion is consequential because the implementation and remediation work is the largest single category of CMMC compliance cost for most contractors, and the regulatory cost model leaves that work outside the official figure.

DoD has described the DIB sector as consisting of over 220,000 companies that process, store, or transmit FCI or CUI, while the 32 CFR Part 170 narrative identifies 8,350 medium and large entities expected to require Level 2 C3PAO certification, with 7,665 of those classified as small entities and 685 as other than small. As reported in the April 2026 Cyber AB Town Hall, the CMMC ecosystem had reached 1,198 Final Level 2 certifications and 42 Conditional Level 2 certifications, with 124

Level 2 assessments in progress. Combined, 1,240 contractors have entered Level 2 certified status (Final or Conditional) and 124 are mid-assessment. The gap between the addressable population and the realized assessment volume is the structural reality this paper engages with, and the cost stack is the most consequential variable explaining that gap.

The paper that follows maps the cost stack across nine categories. The categories are defined in operational terms a contractor can identify and budget against. The figures cited within each category are practitioner observations from current engagements presented as ranges to communicate the variance that contractors should expect.

A note on the purpose of this paper and the cost figures it presents. The paper exists to identify the hidden cost factors contractors should consider when planning CMMC compliance work, not to project the actual cost any specific contractor will pay. The dollar ranges throughout are not vendor list prices and should not be read as universal market pricing. They are practitioner-observed planning ranges derived from current CMMC readiness, remediation, assessment-support, and sustainment work with small and mid-size DIB contractors. Where public regulatory or vendor pricing is available, this paper cites it directly. Where public pricing is unavailable or varies substantially by scope, the figures are presented as planning ranges rather than fixed estimates. A contractor seeking an accurate projection of their own compliance cost needs to apply the framework in this paper to their specific operational conditions, scope, and engagement choices.

Section 2. Direct Readiness Costs

Direct readiness costs are the consulting time, internal labor, and remediation expenditure that a contractor incurs between deciding to pursue CMMC compliance and arriving at the point where the contractor is assessment-ready. This category is the largest single category in the cost stack for most contractors and is also the category most often understated in initial planning.

Consulting time is the most visible component. Field observation across recent engagements with small and mid-size contractors places the typical consulting

requirement at 200 to 300 hours for a contractor starting from a moderate baseline of existing IT discipline. Contractors with mature IT operations and existing security tooling may complete readiness with 100 to 150 hours of consulting time. Contractors with limited internal cybersecurity capability or substantial control gaps may require 400 to 500 hours. The variance is large and is driven primarily by the contractor starting condition rather than by contractor size alone.

The consulting rate for credentialed practitioners working in this space ranges from $125 to $325 per hour for the readiness work itself. The range is wide because the practitioner credentialing structure spans from Registered Practitioner (RP) at the entry level through Registered Practitioner Advanced (RPA), Certified CMMC Professional (CCP), Certified CMMC Assessor (CCA), and Lead CCA at the senior end. Engagement structures where Registered Practitioners deliver the readiness work under the supervision of a more senior practitioner typically produce rates in the $125 to $175 per hour range. Engagement structures where senior practitioners and partners deliver the work directly typically produce rates in the $250 to $325 per hour range and sometimes higher for specialized work. The applicable rate within a given engagement depends on the work being performed, the practitioner experience level, and the engagement structure including onsite versus offsite, retainer versus project, and sole-source versus competitive bid. The rate range is consistent with comparable regulated cybersecurity consulting markets such as SOC 2 readiness, HIPAA compliance, and PCI-DSS work, where credentialed practitioners holding CISA, CISSP, or similar certifications bill in comparable ranges based on engagement structure and seniority.

Applying the typical range, a small contractor at the median requires 200 to 300 hours of consulting time at $125 to $325 per hour. The consulting line in the cost stack alone produces a budget range of $25,000 to $97,500 before any tooling, infrastructure, assessment, or maintenance cost is considered. Contractors who begin readiness work with budgets in the $25,000 to $40,000 range, which is a common initial budget for small contractors planning their CMMC work, may find that the lowest-rate consulting engagement consumes the entire budget at the lower bound of hours, while typical median engagements substantially exceed the budget before the rest of the cost stack is encountered.

Internal labor is the second component within direct readiness costs and is often ignored in initial budgeting because internal labor is not invoiced. The compliance lead within the contractor organization spends substantial time during the readiness period on documentation, internal coordination, vendor management, and the iterative work of bringing controls into operational state. IT staff spend time on configuration changes, tool deployment, network segmentation, and the technical implementation work that the consulting engagement specifies. Executive leadership spends time on governance decisions, scope definition, vendor selection, and the Affirming Official function. The cumulative internal labor across a 12 to 18 month readiness period for a small contractor typically represents 800 to 1,500 internal hours distributed across roles. At fully-loaded internal labor rates, the dollar value of that internal time runs from $50,000 to $150,000 depending on the role mix and the contractor labor cost structure.

Remediation expenditure is the third component. Remediation costs cover the actual technical work and equipment purchases required to bring controls into compliance. The work typically includes firewall replacements where existing equipment cannot support required configurations, identity and access management tooling deployment where existing IAM is inadequate, multi-factor authentication infrastructure where MFA is not already in place, configuration management tooling where current practice is manual, audit log infrastructure where logging is not centralized or retained, and network segmentation work where the existing network does not isolate CUI from non-CUI traffic. The remediation cost varies substantially by contractor starting condition. Contractors with mature IT may have most of this infrastructure already and incur minimal remediation expense, while contractors with limited cybersecurity investment may face $50,000 to $200,000 in remediation expenditure during the readiness period.

Taken together, direct readiness costs for a typical small to mid-size contractor produce a range of $125,000 to $450,000 before the contractor encounters a C3PAO. The range encompasses the variance described above, and the actual figure depends on the specific starting condition, the chosen consulting approach, the practitioner credentialing level engaged, and the remediation scope identified during the engagement.

The structural observation is that the direct readiness costs alone exceed the published C3PAO assessment cost by a factor of three to ten. Contractors and primes who anchor the CMMC compliance cost on the assessment fee are understating the total cost by an order of magnitude. The piecemeal cost conversation contributes directly to this anchor effect because the assessment fee is the most publicly discussed cost category, and the readiness costs that produce the assessment-ready state are discussed less frequently and less specifically.

Section 3. Tooling and Infrastructure Costs

Tooling and infrastructure costs are the recurring expenditures that support the controls implemented during readiness work. This category is often understated because contractors think of it as routine IT spending rather than as CMMC-specific spending. The structural reality is that some portion of the tooling and infrastructure stack is required specifically because of CMMC, and that portion is recurring rather than one-time.

The most visible single component is the licensing cost for a FedRAMP-authorized cloud environment to handle CUI. The Microsoft Government Community Cloud (GCC) and Government Community Cloud High (GCC High) products are the most common choices for contractors handling DoD CUI. Microsoft publishes pricing for these products on its commercial pricing pages, and reseller channels publish current government pricing that often varies by enterprise agreement terms, commitment length, and add-on selections. Public reseller pricing in 2026 places GCC High Enterprise G3 at approximately $60 per user per month and GCC High Enterprise G5 at approximately $93 per user per month, with commercial-tier GCC pricing somewhat lower at approximately $44 per user per month for G3 and $71 per user per month for G5. Contractors handling export-controlled technology under ITAR typically require GCC High rather than GCC, and that decision adds both cost and complexity.

Microsoft licensing is applied to the users within the CUI-access boundary rather than to the contractor total headcount. A small aerospace contractor with 40 to 50 total employees may have only 25 to 35 users requiring GCC High licensing for direct CUI handling, with another five to ten users handling FCI but not CUI, and

shop floor personnel (CNC operators, machinists, quality inspectors) exposed to CUI through printed travelers, G-code files, or controlled USB media rather than through licensed Microsoft endpoints. The scoping reality matters because the licensing cost scales with the CUI-access user count, not the total employee count, and contractors who scope their CUI handling carefully can substantially reduce the licensing line.

For a small contractor with 33 users in the CUI-access boundary at GCC High G5 pricing, the licensing line runs approximately $3,070 per month or $36,800 per year. For a mid-size contractor with 100 users in the CUI-access boundary at the same pricing, the licensing line runs approximately $9,300 per month or $111,600 per year. These figures cover Microsoft licensing only and do not include the third-party tools that integrate with the Microsoft environment to deliver specific CMMC controls, the migration cost to move from commercial to government cloud, or the managed services that operate the environment.

Third-party tooling stacks vary across contractors but typically include a Governance, Risk, and Compliance platform for evidence collection and control mapping, a Security Information and Event Management platform for audit log centralization and analysis, an endpoint detection and response platform for endpoint security monitoring, a vulnerability scanning service for the regular vulnerability assessment requirements, and a configuration management platform for the configuration baseline and change management requirements. The total annual cost for the third-party tooling stack for a small contractor with roughly 33 users in the CUI-access boundary typically runs from $30,000 to $100,000, with the variance driven by the specific platforms chosen, the depth of feature use, and the SIEM ingestion volume required to support audit log retention in GCC High environments.

Infrastructure costs beyond licensing include the networking equipment, identity management infrastructure, and supporting hardware required to operate the CMMC-aligned environment. For contractors who began readiness work with consumer-grade or small-business-grade infrastructure, the infrastructure modernization required during readiness may add $20,000 to $75,000 in capital

expenditure depending on the scope of the network and the number of facilities involved.

The annual recurring cost of tooling and infrastructure for a small contractor with roughly 33 users in the CUI-access boundary typically runs from $80,000 to $180,000 once licensing, third-party tooling, and infrastructure maintenance are combined. The recurring nature of this cost is the part most often missed in initial planning. Contractors who budget the readiness work as a one-time project frequently fail to budget the recurring annual cost that begins immediately and continues through the certification cycle and beyond.

The structural observation is that tooling and infrastructure cost is not optional and is not bounded by the readiness period. A contractor who completes initial certification and discontinues the supporting tooling cannot maintain assessable evidence and faces recertification failure three years later. The tooling and infrastructure stack is therefore best understood as a permanent operational cost added to the contractor baseline once CMMC compliance is pursued, not as a project cost that ends when the initial assessment is completed.

Section 4. MSP and ESP Service Costs

MSP and ESP service costs are the recurring fees contractors pay to managed service providers and external service providers to deliver portions of the CMMC-aligned environment that the contractor cannot or chooses not to operate internally. The category overlaps with tooling and infrastructure cost in some areas and stands separately in others. The defining characteristic is that the contractor is paying for an ongoing service relationship rather than for a one-time deployment.

Standard managed service provider fees for a contractor with an existing MSP relationship typically run from $2,000 per month for a small contractor with simple needs to $15,000 per month for a mid-size contractor with broader IT scope. The figures reflect general managed IT services rather than CMMC-specific work. Contractors who engage MSPs that have built specific CMMC support capability typically pay a premium of 30 to 50 percent above standard managed service rates

because the CMMC-aware MSP carries additional credentialing, additional process discipline, and additional liability exposure that justifies the premium pricing.

External service provider fees for specialized services run in addition to the standard MSP fees. SIEM as a service, GRC as a service, hosted CUI environments, and specialized compliance management platforms all fall within the ESP category. The pricing varies by service category and contractor size. A typical small contractor with roughly 33 users in the CUI-access boundary may pay $1,500 to $5,000 per month for ESP services in aggregate, with the variance driven by which specific services the contractor chooses to outsource versus operate internally.

The continuity risk within MSP and ESP relationships is the part most contractors and most practitioners have only recently begun to discuss in public. The NeoSystems collapse in May 2026 made the risk visible. A 26-year-old firm with established CMMC credentials and a perfect SPRS score dissolved over a weekend, leaving clients in the position of finding alternative service arrangements for their CUI environments on short notice and without a clear transition plan. The continuity risk has now been demonstrated in the field, and contractors relying on a single MSP or ESP for their CUI handling and their compliance posture have a continuity question to answer that goes past the assessment timeline.

The cost of mitigating continuity risk runs in two forms. The first is the cost of maintaining backup arrangements or in-house capability that could absorb the work if the primary provider failed. The second is the cost of transitioning when a primary provider fails, which includes new provider onboarding, data migration, environment rebuild in some cases, and the operational disruption during the transition period. Neither cost shows up in the contractor budget until it is needed, and at that point the cost is forced rather than chosen.

Taken together, MSP and ESP services for a typical small to mid-size contractor produce an annual recurring cost in the range of $30,000 to $200,000 with substantial variance based on the specific service arrangements. The three-year cost across the initial certification cycle typically falls between $90,000 and $600,000. Contractors who treat MSP and ESP fees as routine IT cost rather than as CMMC-specific cost are not budgeting accurately for the compliance picture.

Section 5. C3PAO Assessment Costs

C3PAO assessment costs are the direct fees paid to the Certified Third-Party Assessor Organization for the formal Level 2 assessment that produces the certification. This category is the most publicly discussed cost in the CMMC conversation and is also one of the smallest single line items in the total cost stack. The visibility-to-magnitude mismatch is the structural feature most likely to mislead contractor budgeting.

Current C3PAO pricing for typical small and mid-size contractors falls in the range of $30,000 to $50,000 for the formal Level 2 assessment, with substantial variance based on scope and complexity. DoD's regulatory cost model in 32 CFR Part 170 estimates the C3PAO engagement component for a small-entity Level 2 certification assessment at approximately $31,234, based on 120 hours at $260.28 per hour. The same model estimates the full small-entity assessment and affirmation support burden at approximately $101,752, with three-year cost of approximately $104,670. The DoD estimates align reasonably with the C3PAO fee component as observed in the field, while the broader assessment-support burden the regulatory model captures includes contractor labor and supporting work that contractors sometimes underestimate. Larger contractors, contractors with multi-facility scope, contractors with complex CUI handling, and contractors handling export-controlled technology under ITAR typically face higher assessment fees ranging from $60,000 to $150,000 or more depending on the scope and complexity factors.

The drivers within C3PAO pricing include the assessment scope (number of users, number of facilities, complexity of the CUI handling environment), the geographic distribution of the contractor (which affects travel cost), and the special considerations that may require additional assessor expertise (ITAR-controlled technology, classified handling capability, specialized industry requirements). Contractors with simpler operations face lower assessment fees, while contractors with complex operations face substantially higher fees.

Beyond the C3PAO fee itself, the contractor incurs additional costs during the assessment period, including travel and onsite expenses for the assessment team and contractor labor cost during the assessment week. The contractor labor cost

typically requires substantial time from the compliance lead, the IT staff, the Affirming Official, and any subject matter experts who must demonstrate specific controls or answer assessor questions. At fully-loaded internal labor rates, the contractor labor cost during the assessment week alone can run $20,000 to $50,000 for a typical small contractor.

The conditional certification path adds another cost dimension. Contractors who do not achieve full compliance during the assessment may be offered conditional certification with a Plan of Action and Milestones (POAM) for the gaps identified. The remediation work required to close the POAM gaps and convert conditional certification to full certification adds consulting time, internal labor, and potentially additional tooling expenditure. The conditional certification path typically adds $25,000 to $75,000 in remediation cost beyond the initial assessment fee.

Taken together, the direct C3PAO assessment cost line typically runs $40,000 to $90,000 for a typical small to mid-size contractor when the assessment fee, the contractor labor during the assessment week, and the conditional certification remediation costs are combined. The figure that contractors usually anchor on is the $30,000 to $50,000 assessment fee in isolation, which understates the true assessment-period cost by roughly 50 percent. The structural observation is that the C3PAO assessment cost is real but represents a small fraction of the total compliance cost. Treating it as the headline figure produces budgeting decisions that miss the larger cost categories elsewhere in the stack.

Section 6. Ongoing Compliance and Maintenance Costs

Ongoing compliance and maintenance costs are the recurring expenditures that keep a contractor in compliant operating state between initial assessment and recertification. This category is the one contractors are least prepared for because the initial readiness conversation typically frames the work as a project with a defined endpoint rather than as an ongoing operational discipline. The structural reality is that compliance maintenance is permanent, distributed across three

operational rhythms, and resource-intensive in ways that initial readiness budgets rarely accommodate.

The first rhythm is continuous attention to operational controls. Account management reviews, access certifications, audit log review, vulnerability management, patching cadence, and configuration baseline management cannot wait for a quarterly review. These controls operate continuously and require continuous attention. A small contractor typically allocates 0.5 to 1.0 full-time-equivalent staff time to the operational compliance function across the year. A mid-size contractor typically allocates 1.0 to 2.5 full-time-equivalent staff time. At fully-loaded compliance staff cost ranging from $90,000 to $150,000 per year, the operational compliance function alone runs $45,000 to $375,000 per year depending on contractor size.

The second rhythm is time-anchored compliance work that recurs on annual or semiannual cycles. The work includes annual security awareness training delivery, incident response plan testing and exercise, contingency plan exercise and tabletop, annual risk assessment update, annual policy review and approval, and annual control testing and evidence sampling. The time-anchored compliance work typically requires 200 to 400 hours of compliance staff time per year for a small contractor, with substantial variance depending on the complexity of the contractor environment.

The third rhythm is structural compliance work driven by change events rather than calendar dates. The work includes boundary changes when CUI scope shifts, system inventory updates when new systems are introduced, configuration baseline updates when major changes occur, new personnel onboarding for compliance-relevant roles, and subcontractor flow-down review when new subcontracting relationships are established. The structural compliance work has variable volume but typically adds 100 to 300 hours of compliance staff time per year for a typical small to mid-size contractor.

The Affirming Official function adds executive time cost that is often invisible in compliance budgeting. The AO must remain engaged with the compliance program across the entire certification cycle, not just at attestation moments. AO involvement in quarterly compliance reviews, in significant change events, in

subcontractor compliance decisions, and in the annual recertification preparation typically requires 50 to 100 hours of executive time per year. At fully-loaded executive labor rates, the AO function alone adds $20,000 to $50,000 per year to the maintenance budget.

Evidence aging is the silent failure mode that drives much of the maintenance work. Controls keep operating but the documentation becomes stale, with access review logs from 18 months ago no longer proving the control is currently operating and configuration baselines from the initial assessment no longer proving the current system matches. Evidence collection, evidence refresh, and evidence preservation across the certification cycle is the work that turns control operation into assessable certification posture. The maintenance work that keeps evidence current is the work that produces the next successful certification.

Taken together, ongoing compliance and maintenance costs for a typical small to mid-size contractor run $75,000 to $250,000 per year once the compliance staff time, the time-anchored compliance work, the structural compliance work, the AO function, and the evidence management overhead are combined. The three-year cost across the initial certification cycle typically falls between $225,000 and $750,000. Contractors who budget initial readiness without budgeting ongoing maintenance face the predictable failure mode of arriving at recertification with stale evidence and degraded compliance posture, which produces a higher-cost recertification or a failed recertification altogether.

Section 7. Recertification Cycle Costs

Recertification cycle costs are the expenditures associated with maintaining Level 2 C3PAO certification across the three-year certification window and producing the next successful certification at the end of the cycle. The category is forward-looking from the initial certification moment and is poorly understood by most contractors entering CMMC compliance for the first time.

The CMMC program requires Level 2 C3PAO certification renewal every three years. The renewal is not a paperwork exercise but rather a full assessment of the contractor compliance posture as of the renewal date, with the same rigor as the

initial assessment. Contractors who maintained their compliance posture continuously across the certification window face a renewal that confirms the maintained state, while contractors who allowed compliance posture to degrade across the window face a renewal that exposes the degradation.

The cost of recertification varies substantially based on how well sustainment was maintained across the certification cycle. A contractor that maintained the compliance discipline continuously, kept evidence current, refreshed training annually, tested the incident response plan regularly, and engaged the Affirming Official in ongoing oversight typically faces a recertification cost of 50 to 80 percent of the original certification cost. The reduced cost reflects that the documentation, the controls, and the operational discipline are already in assessable state and the recertification confirms what is already running.

A contractor that allowed sustainment to lapse across the certification cycle faces a substantially different cost picture at recertification. Stale evidence, drifted configurations, unrefreshed training, untested response plans, and disengaged AO oversight all produce findings during recertification that require remediation. The remediation work compresses 30 months of neglected maintenance into the months leading up to recertification, at a higher per-hour cost than continuous maintenance would have produced. The recertification cost for a contractor in this state typically runs 100 to 150 percent of the original certification cost, sometimes higher when the gaps are severe.

The compounding effect across multiple certification cycles is the part contractors and primes most often miss. Over a ten-year contractor horizon spanning the initial certification and roughly three recertifications, the total cost of compliance ranges from approximately 2.5 times the initial certification investment for contractors with strong sustainment discipline to 4 times or more for contractors who cycle through neglect and crisis. The cumulative number is substantial. A contractor whose initial certification cost approximately $500,000 across all categories may spend $1.25 million to $2 million over the ten-year horizon when recertification cycles are included.

The structural observation is that the certification cycle is not a series of independent assessment events. The certification cycle is a continuous compliance

discipline punctuated by formal assessment moments. Contractors who understand this structure budget for the discipline, allocate sustained resources to the compliance function, and produce recertifications that confirm rather than rediscover their compliance posture. Contractors who do not understand this structure budget for the assessment moments, allow the discipline to lapse between them, and produce recertifications that surface the cumulative cost of neglected maintenance.

Section 8. Insurance and Risk Transfer Costs

Insurance and risk transfer costs are the premiums and coverage adjustments associated with the cybersecurity and regulatory exposure that CMMC compliance work makes more visible. This category is often invisible in contractor budgeting until a coverage discussion forces it onto the table, and even then the conversation tends to treat cyber insurance as a single line item rather than as the layered risk transfer picture it actually represents.

Cyber liability insurance is the most familiar single component. Contractors carrying cyber liability coverage typically see premium adjustments following CMMC readiness work. The adjustment direction depends on the contractor starting state and the coverage carrier underwriting position. Contractors who improved their security posture substantially through readiness work may see modest premium reductions reflecting the improved underwriting picture. Contractors who maintained existing coverage levels typically see premium increases of 15 to 40 percent reflecting carrier recognition that DIB contractors carry distinct exposure profiles requiring different pricing. More recent industry coverage suggests that these premiums have begun to stabilize for contractors that demonstrate strong cybersecurity maturity, while contractors with material gaps continue to face premium adjustments at the upper end of the range. The variance across the cyber liability category alone runs $5,000 to $50,000 per year for typical small to mid-size contractors.

False Claims Act exposure represents a separate insurance category that is emerging as the FCA case law on cybersecurity misrepresentation develops. The Aerojet Rocketdyne settlement in 2022 at $9 million, widely considered the

foundational case for the Department of Justice Civil Cyber-Fraud Initiative, the Penn State settlement in 2024 at $1.25 million, and the Georgia Tech Research Corporation settlement in 2025 at $875,000 all establish that cybersecurity misrepresentations on federal contracts can produce FCA liability. Insurance carriers are responding by offering FCA-specific coverage as a distinct policy or as an endorsement on existing coverage. Pricing varies substantially based on contractor size, contract volume, and SPRS score history. A typical small to mid-size DIB contractor with active SPRS attestations and contracts of substantial value may face FCA-specific coverage premiums of $5,000 to $30,000 per year.

Errors and omissions coverage for the contractor cybersecurity function and directors and officers exposure for executive leadership both require attention in the CMMC compliance context. The Affirming Official role may cause brokers and counsel to revisit D&O and management-liability coverage, particularly where cybersecurity attestations, SPRS scores, or contract certifications create executive-level signoff risk. Coverage adjustments to address AO-specific exposure typically add $3,000 to $15,000 per year to the directors and officers premium.

The cumulative insurance and risk transfer cost picture for a typical small to mid-size DIB contractor runs $15,000 to $100,000 per year once cyber liability premium adjustments, FCA-specific coverage, errors and omissions coverage, and directors and officers coverage adjustments are combined. The three-year cost across the initial certification cycle typically falls between $45,000 and $300,000. The variance is large because the contractor risk profile, the contract volume, and the carrier underwriting position all interact in ways that produce different cumulative outcomes.

The interaction between cyber insurance coverage and CMMC compliance posture is more complex than the cyber liability conversation alone suggests. The cumulative exposure across cybersecurity events, regulatory enforcement, and contract performance produces an insurance picture that contractors and their brokers are continuing to develop as the FCA case law matures and as carriers refine their underwriting positions for the DIB market.

Section 9. Indirect and Opportunity Costs

Indirect and opportunity costs are the expenditures and lost value that do not appear on any invoice but materially affect the contractor financial picture during the CMMC compliance period. This category distinguishes a complete cost analysis from a partial one because the indirect costs are typically equal to or greater in magnitude than several of the categories that do appear on invoices.

The opportunity cost of executive and senior staff time is the largest single component. Executive leadership engaged in CMMC governance decisions, vendor selection, scope definition, and the Affirming Official function is not engaged in business development, customer relationships, or strategic operations during that time. The opportunity cost is real even when it is not invoiced. For a typical small to mid-size contractor in the active readiness period, the opportunity cost of executive time alone may equal 10 to 20 percent of the total compliance budget when measured at fair value rather than at internal labor rates.

Lost contracts during readiness periods represent a second indirect cost category. Contractors who are not yet compliance-ready cannot bid on Phase 2 contracts that require Level 2 C3PAO certification. The lost bidding capacity during the 12 to 18 month readiness window may produce real contract losses or may simply mean that the contractor pursues smaller or less competitive opportunities during that period. Either way, the contractor revenue trajectory during readiness differs from what it would have been without the readiness work consuming bidding capacity.

Flow-down failure represents a related cost category. Contractors whose primes update flow-down language to require accurate SPRS scores, completed C3PAO certifications, or specific compliance attestations may lose subcontract awards when they cannot meet the updated flow-down requirements. The flow-down failure cost is sometimes immediate, when a specific contract is lost, and sometimes deferred, when the contractor is no longer invited to bid on future work from a particular prime.

Reduced bidding capacity during peak readiness work is a more granular version of the lost contracts cost. The compliance staff time, the executive time, and the

operational disruption during heavy readiness work all reduce the contractor capacity to pursue new work during that period. The reduction is not always quantifiable as specific lost contracts but appears in the contractor pipeline as fewer proposals submitted, fewer customer meetings scheduled, and reduced presence in the competitive landscape.

The strategic cost of boundary decisions is the most subtle indirect cost. Every decision about what to bring inside the CMMC boundary and what to leave outside affects the contractor operational flexibility, future scope flexibility, and ongoing maintenance cost. Bringing more inside the boundary increases the compliance cost permanently. Leaving things outside the boundary may produce operational friction or future compliance issues if the boundary is later adjusted. The strategic cost of getting the boundary decision wrong is paid across the entire certification cycle and beyond.

Organizational disruption during the readiness period adds a final indirect cost component. The internal change management work, the training, the role redefinition, the documentation work, and the cultural adjustment required to operate within CMMC discipline all consume organizational capacity. The disruption cost is real and is sometimes large enough to produce employee turnover, delayed product releases, or other downstream operational effects.

Taken together, indirect and opportunity costs for a typical small to mid-size contractor during the initial certification cycle typically run 15 to 30 percent of the total invoiced compliance cost. A contractor with $1 million in direct compliance costs across the three-year cycle typically carries an additional $150,000 to $300,000 in indirect costs that do not appear in any compliance budget line item.

Section 10. The Cumulative Picture

The cumulative picture across the nine cost categories produces a substantially larger total than most contractors and most primes acknowledge in their compliance planning. The numbers below represent practitioner observation aggregated across recent engagements with small and mid-size DIB contractors, presented in ranges to communicate the variance contractors should expect. The

total cost across the initial three-year certification cycle is the figure contractors and primes need to be working from when they plan compliance budgets and supply chain pricing.

For a typical small contractor with 10 to 50 employees and modest CUI handling scope, the cumulative three-year cost ranges from approximately $875,000 to $3,150,000. The lower end of the range reflects contractors with mature IT operations, simple environments, disciplined sustainment, and engagement with practitioners at the lower end of the credentialing structure. The upper end of the range reflects contractors with limited starting infrastructure, complex environments, or remediation-heavy readiness work delivered by senior practitioners.

For a typical mid-size contractor with 50 to 200 employees and broader CUI handling scope, the cumulative three-year cost ranges from approximately $1,960,000 to $6,050,000. The variance reflects the same drivers as the small contractor range, scaled to the larger operational footprint.

For a typical larger contractor with 200 or more employees, multi-facility operations, and complex CUI handling, the cumulative three-year cost typically exceeds $5,000,000 and may reach $15,000,000 or more depending on scope and complexity. Larger contractors are outside the primary focus of this paper because their cost picture is dominated by enterprise IT factors that operate differently from the small and mid-size contractor cost stack.

The table below summarizes the typical cumulative three-year cost picture for small and mid-size contractors across the nine cost categories.

Cost Category	Small Contractor (10 to 50)	Mid-Size Contractor (50 to 200)
Direct readiness costs	$125K to $450K	$300K to $800K
Tooling and infrastructure (3 years)	$240K to $540K	$540K to $1.2M
MSP and ESP services (3	$90K to $600K	$240K to $1.2M

years)		
C3PAO assessment (year 1)	$40K to $90K	$70K to $150K
Ongoing compliance and maintenance (3 years)	$225K to $750K	$450K to $1.2M
Insurance and risk transfer (3 years)	$45K to $300K	$90K to $600K
Indirect and opportunity costs (3 years)	$110K to $400K	$270K to $900K
Three-year cumulative total	**$875K to $3.15M**	**$1.96M to $6.05M**

The table figures are derived from the practitioner observations within each category section of this paper. The ranges are presented to communicate variance rather than to suggest precision. The actual cost for a specific contractor will fall somewhere within these ranges based on the contractor starting condition, the chosen vendor relationships, the scope and complexity of the CUI handling, and the sustainment discipline maintained across the certification cycle.

The cumulative picture produces several observations that are not visible when the cost categories are discussed individually. The direct readiness costs and the ongoing maintenance costs together typically exceed the tooling, infrastructure, MSP, ESP, and assessment costs combined. The C3PAO assessment fee, which is the most publicly discussed cost in the CMMC ecosystem, represents 2 to 5 percent of the three-year total cost. The indirect and opportunity costs are roughly comparable in magnitude to the C3PAO assessment cost but typically receive far less attention in contractor budgeting.

The structural observation is that the CMMC compliance cost picture is not assessment-centered. The assessment is one moment within a multiyear compliance discipline that requires substantial sustained investment. Contractors and primes who plan around the assessment fee are budgeting for the wrong line item. The dominant cost drivers are readiness, sustainment, and the recurring

tooling and service relationships that operate continuously between assessment events.

Section 11. The Consolidation Pressure

The cost stack produces consolidation in the Defense Industrial Base rather than universal compliance. This is the strategic argument that emerges from the cumulative picture, and it is the argument that contractors, primes, and policy participants need to engage with as Phase 2 begins.

The cost burden as a function of contractor revenue from defense work is the structural relationship that determines whether compliance is economically viable for a given contractor. A contractor whose defense work represents 80 percent of revenue carries a different cost-to-revenue ratio for compliance than a contractor whose defense work represents 15 percent of revenue. The high-defense-share contractor can amortize the compliance cost across a substantial defense revenue base. The low-defense-share contractor cannot. The compliance cost as a percentage of defense revenue determines whether the contractor remains in defense work or exits to commercial work where the cost is not required.

Field observation across recent engagements shows the break-even point sitting roughly where compliance cost equals 8 to 15 percent of three-year defense revenue. Contractors above this threshold face an economic case for exiting defense work rather than absorbing the compliance burden. The threshold varies by contractor margin profile, by competitive position, and by the strategic importance of defense work to the broader business, but the general shape holds across small and mid-size contractors.

Applying the threshold to typical contractor cost stacks, a small contractor with $5 million in three-year defense revenue facing $900,000 to $3,100,000 in compliance cost is in the 18 to 62 percent range. The contractor is well above the economic threshold for compliance to be sustainable. The contractor either has a strong strategic case for absorbing the cost or has a strong economic case for exiting defense work. The decision depends on factors beyond the cost picture alone but the cost picture is determinative for many contractors.

Mid-size contractors with $20 million to $50 million in three-year defense revenue facing $2 million to $6 million in compliance cost are in the 4 to 30 percent range. The mid-range contractors typically have the strongest case for absorbing the cost because the cost-to-revenue ratio is more manageable and the alternative paths are less attractive. The mid-range contractors are also the contractors most likely to acquire smaller contractors who are exiting defense work, because the acquisition price for a small contractor exiting on cost grounds typically reflects the compliance cost the acquiring contractor would have to absorb anyway.

The supply chain consequence of this dynamic is consolidation, with small contractors exiting defense work, mid-size contractors absorbing smaller contractors, and the total number of contractors in the DIB shrinking as a result. Primes lose some suppliers and consolidate purchasing with the contractors that remain. The remaining contractors gain pricing power because the supplier base has contracted, and C3PAOs price against a smaller addressable market where assessment costs may rise rather than fall as the market clears. The cost stack produces a smaller, more concentrated DIB rather than a larger, more compliant one.

The exit decisions are happening in the field now rather than hypothetically in the future. Contractors are calculating their cost stacks, examining their defense revenue trajectories, and making strategic decisions about whether to pursue compliance or to pivot to commercial work. The decisions are not always public. They show up in declined RFP responses, in business development conversations that do not happen, in subcontractor relationships that do not get renewed, and in the gradual disappearance of contractors from the active DIB pool.

The structural observation is that the DIB will be smaller in three to five years than it is today as a direct consequence of the cost stack. The Government Accountability Office identified this risk in March 2026 in report GAO-26-107955 when it warned that CMMC program costs may affect the extent to which existing DIB companies continue doing business with DoD. The warning is now showing up in field outcomes, with the cost stack producing the exit pattern, the exit pattern producing the consolidation pressure, and the consolidation pressure reshaping the DIB in ways that policy participants have only begun to engage with.

Section 12. What Contractors Should Be Doing Now

The cost stack analysis above produces operational guidance for contractors who are still navigating compliance decisions and for contractors who are already deep in the readiness work. The guidance is practical and does not require new analytical work to apply.

Map the full cost stack honestly before beginning or continuing readiness work. The mapping exercise alone surfaces budgeting gaps that initial planning conversations typically miss. Use the nine categories from this paper as the working framework and produce a contractor-specific estimate within each category. The exercise takes a compliance lead and a finance lead two or three working sessions and produces a cost picture that supports more accurate budgeting and more honest strategic decisions.

Many contractors will benefit from senior practitioner involvement in the cost stack mapping itself. The work requires both CMMC compliance expertise and budget and finance judgment, applied across the nine cost categories and across the certification cycle. The integration of compliance knowledge and financial planning sits at the senior practitioner level in the CMMC credentialing structure, including the Registered Practitioner Advanced (RPA) credential. A senior practitioner engaged early in the readiness conversation, before substantial cost has been committed, can produce a defensible contractor-specific cost picture, identify the strategic decisions the contractor faces, and serve as both project manager and budget advisor across the readiness period. Contractors who attempt the cost mapping internally without senior practitioner involvement typically discover costs sequentially during readiness rather than planning for them in advance, which is the structural pattern this paper has described.

The CMMC credentialing structure validates baseline competence but does not guarantee the integrated capability the cost mapping work requires. Many credentialed practitioners come from technical or IT backgrounds and have not operated as project managers or budget advisors at the executive level. Contractors

evaluating senior practitioner candidates should look for direct experience managing multi-phase engagements with defined budget envelopes, exposure to contractor financial operations including accounting and cost recovery, and the ability to translate technical compliance requirements into dollar figures that finance leadership can validate. The qualifying conversation matters because the cost mapping work fails when the practitioner can name the controls but cannot price them, or can price isolated components but cannot integrate them across the certification cycle.

Risk management judgment is the final qualification that separates integrated senior practitioners from technical-only practitioners. The cost stack engagement runs alongside legal exposure that the contractor may not fully appreciate, including False Claims Act exposure on SPRS attestations, CUI scope decisions that affect contractor liability, and MSP and ESP arrangements that produce flow-down complications. A senior practitioner who recognizes when a contractor decision is creating legal or CUI risk, pauses the engagement to involve counsel, or revisits the planned approach is materially more valuable than a practitioner who treats every contractor instruction as a directive to execute. Contractors should look for a practitioner who has demonstrated this restraint in prior engagements rather than one who treats CMMC work as pure project management or pure technical implementation.

Senior practitioner involvement does not replace the need for the contractor existing financial and legal advisors. The cost mapping work touches accounting questions (cost allocation across direct and indirect categories, cost recovery on existing contracts, capital versus operational expense classification of tooling investments) that contractor accountants are positioned to address. The same work touches legal questions (FCA exposure on SPRS attestations, contract modification opportunities, supply chain flow-down risk) that contractor counsel is positioned to address. Contractors planning CMMC budgets should include line items for outside accountant and legal counsel time as part of the overall cost stack rather than treating these advisors as outside the budget. The senior practitioner serves as the integrator who recognizes when the accountant or counsel should be brought into a specific decision and who frames the questions for those advisors to address.

Larger contractors typically need multiple practitioners engaged at different credential levels rather than a single senior practitioner. The engagement structure for a mid-size contractor with multi-facility scope may include one or more RPAs serving as senior project managers and budget advisors, multiple RPs delivering implementation support across the technical control families, CCAs or Lead CCAs engaged for mock assessments and assessment readiness work, and specialist support for specific technical areas. The credentialing structure works as a layered model where each credential level operates within the boundary the higher-credential practitioners establish. Contractors planning large engagements should budget for this multi-level practitioner model rather than assuming a single practitioner can deliver the full engagement at the necessary scale.

Build the cost picture into contract pricing and cost recovery conversations with primes. Contractors who are absorbing CMMC compliance costs that exceed the contract pricing they are receiving have a legitimate case for renegotiation, scope adjustment, or contract repricing. The conversation requires the contractor to demonstrate the cost stack with specific numbers rather than with generalized complaints about compliance burden. The cost stack documentation from this paper, adapted to the contractor specific situation, supports those conversations directly.

Distinguish CMMC-specific cost from broader IT modernization cost in the contractor internal budgeting. Some portion of the tooling and infrastructure spend would be productive even without CMMC requirements because the underlying IT modernization improves business operations independent of compliance. The distinction matters for cost recovery conversations, for general budget allocation, and for understanding what the contractor is actually paying for CMMC versus what the contractor would have spent anyway.

Make the strategic decision about defense work participation early rather than late. Contractors whose cost-to-revenue ratio is well above the sustainability threshold should engage with that reality during readiness rather than after substantial cost has been sunk. The strategic exit is a legitimate decision and is being made by capable contractors across the DIB. The strategic absorption is also a

legitimate decision but requires explicit recognition of the multiyear cost commitment that follows.

Engage the Affirming Official and senior leadership in the cost conversation rather than treating it as an IT decision. The cost magnitude and the recurring nature of the spending make CMMC compliance a strategic business decision rather than an IT operational decision. The governance structure that the regulation envisions for the Affirming Official function is also the governance structure that produces sound cost decisions across the certification cycle.

The CMMC compliance cost is real and substantial, but it is also manageable when it is understood, planned for, and engaged with strategically. The work in front of contractors is not to argue with the cost. The work is to understand it, budget for it, and decide whether the defense work that produces the cost is worth pursuing under the new economic conditions Phase 2 establishes.

About the Author

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

David can be reached at dkoran@davidkoran.com or by phone at (802) 335-2662.

References

32 CFR Part 170. Cybersecurity Maturity Model Certification Program. Final Rule. October 15, 2024. https://www.federalregister.gov/documents/2024/10/15/2024-22905

32 CFR Part 170 (current). Cybersecurity Maturity Model Certification (CMMC) Program. Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

U.S. Government Accountability Office. Defense Contractor Cybersecurity: DOD Should Address External Factors That Could Impede Program Implementation. Report GAO-26-107955. March 12, 2026. https://files.gao.gov/reports/GAO-26-107955/index.html

National Institute of Standards and Technology. NIST Special Publication 800-171 Revision 2. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. February 2020 (with updates). Current CMMC Level 2 baseline. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

National Institute of Standards and Technology. NIST Special Publication 800-171A. Assessing Security Requirements for Controlled Unclassified Information. June 2018. Current CMMC Level 2 assessment baseline. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf

National Institute of Standards and Technology. NIST Special Publication 800-171 Revision 3. May 2024. Referenced for future framework evolution. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf

Department of Defense. CMMC Assessment Guide - Level 2. Version 2.13. https://dodcio.defense.gov/CMMC/

Microsoft Corporation. Microsoft 365 Government plans pricing. https://www.microsoft.com/en-us/microsoft-365/government/compare-office-365-government-plans

Secureframe. GCC High Pricing and Licensing Guide 2026. Per-User Costs Explained. https://secureframe.com/blog/gcc-high-pricing

The Cyber AB. CMMC April 2026 Town Hall. https://cyberab.org/News-Events/Town-Hall

CyberAB. CMMC Ecosystem Marketplace. https://cyberab.org/marketplace

U.S. Department of Justice. Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations Related to Cybersecurity Violations. July 8, 2022. https://www.justice.gov/archives/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity

U.S. Department of Justice. The Pennsylvania State University Agrees to Pay $1.25M to Resolve False Claims Act Allegations. October 22, 2024. https://www.justice.gov/archives/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating

U.S. Department of Justice. Georgia Tech Research Corporation Agrees to Pay $875,000 to Resolve Civil Cyber-Fraud Litigation. September 2025. https://www.justice.gov/opa/pr/georgia-tech-research-corporation-agrees-pay-875000-resolve-civil-cyber-fraud-litigation

Federal News Network. DoD to evaluate external CMMC risks. March 2026. https://federalnewsnetwork.com/cybersecurity/2026/03/dod-to-evaluate-external-cmmc-risks/

SmallGovCon. GAO Evaluation of CMMC Program and Important Information for Defense Contractors. March 2026. https://smallgovcon.com/federal-government-contracting/gao-evaluation-of-cmmc-program-and-important-information-for-defense-contractors/

Additional Reading

Readers interested in the cost stack themes may find the following related work from the firm useful for further context.

Koran, David W. The Inverted Bottleneck: An Examination of CMMC Assessment Capacity, Readiness, and the SPRS Delta. May 2026. On the structural mismatch between assessment capacity and contractor readiness. https://davidkoran.com/white-papers/cmmc-inverted-bottleneck/

Koran, David W. The Bottleneck: 97 C3PAOs, 80,000 Contractors. On the original capacity analysis preceding the Phase 1 implementation data. https://davidkoran.com/white-papers/cmmc-bottleneck-assessment-capacity/

Koran, David W. Double the Trouble: CMMC and Cyber Insurance Dual Exposure. On the interaction between CMMC compliance work and cyber liability coverage. https://davidkoran.com/white-papers/

Koran, David W. The MSP and ESP Paradox. On the structural risk in compliance service provider relationships. https://davidkoran.com/white-papers/cmmc-msp-esp-compliance/

Koran, David W. The Score Before the Score: SPRS Self-Attestations After Phase 1. On SPRS attestation accuracy and the False Claims Act exposure that runs through it. https://davidkoran.com/white-papers/

Koran, David W. CMMC Phase 1 Realities. A Practitioner Reading of the GAO Findings. On the practitioner interpretation of GAO findings on CMMC program implementation. https://davidkoran.com/white-papers/cmmc-phase1-realities-gao-analysis/