KROLL™

Impact of CMMC Options for DIB Contractors

Table of Contents

SECTION 01

CMMC Impact and Options

KROLL

SECTION 01

CMMC Impact and Options

Executive Summary

CMMC, implemented under 32 CFR Part 170 and DFARS 252.204-7021, establishes mandatory cybersecurity verification for Defense Industrial Base contractors. While designed to protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI), the framework creates significant economic and operational burdens for small businesses. This whitepaper summarizes compliance architectures, government cloud pricing models, and long-term economic implications.

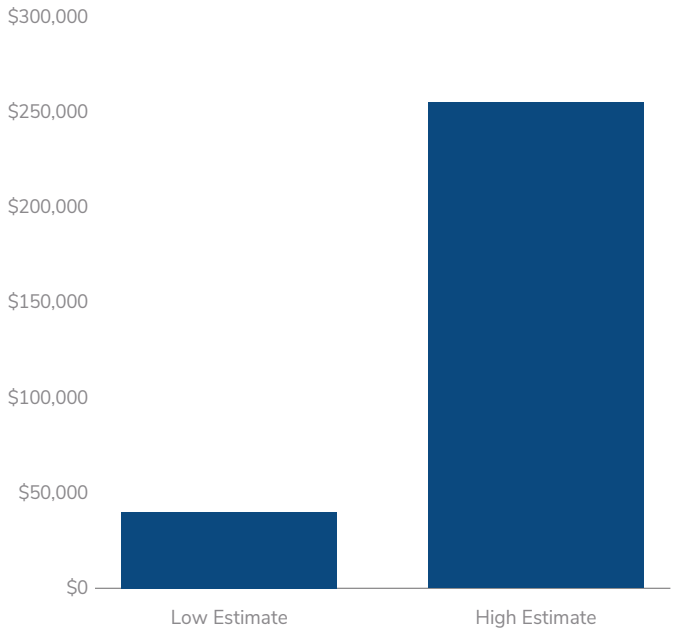
Regulatory Foundations

- 32 CFR Part 170 – CMMC Program Rule
- DFARS 252.204-7012 – Safeguarding Covered Defense Information
- DFARS 252.204-7019 / 7020 – NIST 800-171 Self-Assessment & SPRS Reporting
- DFARS 252.204-7021 – CMMC Requirements
- NIST SP 800-171 Rev. 2 – Level 2 Control Baseline
- Cyber AB Assessment Guides (Level 1 & Level 2)

Estimated Financial Impact

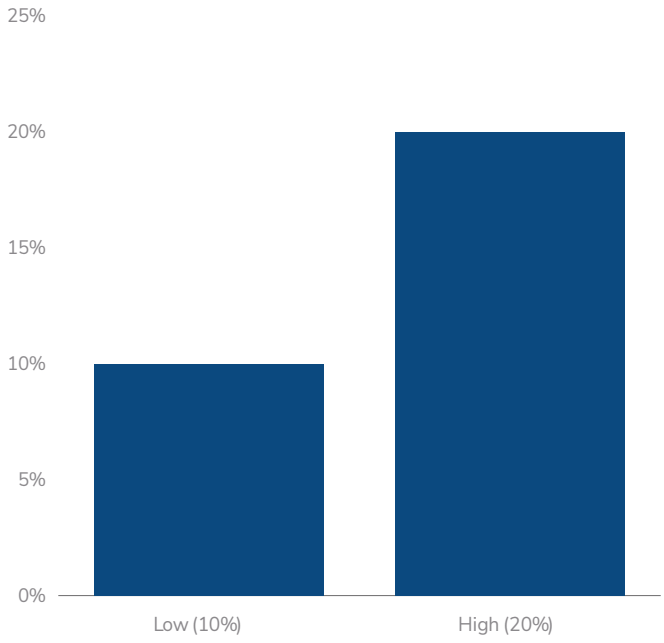
Level 2 readiness and implementation ranges from $40,000 to $250,000+, depending on scope and maturity.

Estimated Level 2 Implementation Cost Range



Ongoing sustainment typically requires 10–20% of annual IT budgets.

Estimated Level 2 Implementation Cost Range



Competitive Stratification Risk

As CMMC requirements are phased into Department of Defense (DoD) solicitations and contract vehicles, certification is rapidly becoming a prerequisite for participation in many segments of the Defense Industrial Base (DIB). Increasingly, prime contractors are prioritizing subcontractors that already possess CMMC certification or demonstrable readiness, even before certification clauses formally appear in solicitations. This trend is driven by the need to minimize program risk, accelerate proposal timelines, and ensure that sensitive program data can be shared without introducing compliance gaps within the supply chain.

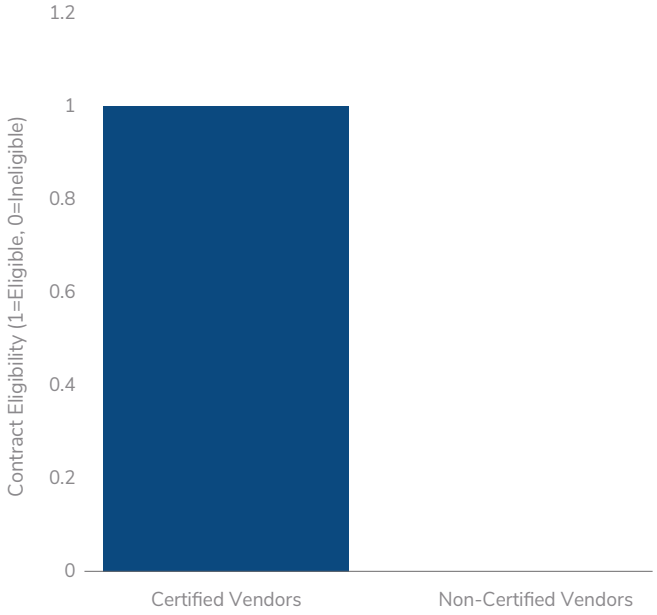
As a result, CMMC certification is evolving from a regulatory requirement into a competitive differentiator. Companies that achieve certification earlier are likely to gain a structural advantage in subcontracting opportunities, as primes seek to assemble compliant supply chains capable of handling Controlled Unclassified Information (CUI) without delays. Conversely, organizations that have not yet achieved certification may face barriers to entry for certain programs, even if they possess strong technical capabilities or long-standing relationships with prime contractors.

This dynamic introduces the risk of competitive stratification within the DIB, where suppliers increasingly fall into distinct tiers based on their ability to invest in and sustain cybersecurity compliance infrastructure. At the top tier are large defense contractors and well-capitalized technology firms that can rapidly implement CMMC-compliant architectures and maintain dedicated cybersecurity teams. These organizations are positioned to expand their market share as smaller competitors struggle to meet compliance requirements.

A second tier may consist of mid-sized contractors that achieve certification through managed enclave environments, government cloud platforms, or partnerships with compliance-focused service providers. While these organizations remain competitive, their participation in certain programs may be shaped by the architectural and operational constraints associated with their chosen compliance solutions.

At the lower end of the spectrum are smaller subcontractors that lack the capital resources or technical expertise required to achieve certification in the near term. These organizations may find themselves excluded from programs involving CUI or sensitive defense technologies, even if their core capabilities remain valuable to the defense ecosystem. Over time, this could lead to consolidation within the supply chain as prime contractors increasingly rely on a smaller pool of certified vendors.

Eligibility Impact of CMMC



Such stratification carries broader implications for innovation and resilience within the DIB. Historically, small businesses have played a critical role in introducing new technologies, niche capabilities, and specialized manufacturing processes into defense programs. If compliance costs prevent these organizations from maintaining access to defense contracts, the result could be reduced supplier diversity and diminished competition within the defense marketplace.

First-Mover Advantage in the CMMC Ecosystem

Another emerging market dynamic is the first-mover advantage associated with early CMMC certification. As DoD contracts begin incorporating CMMC requirements, contractors that achieve certification ahead of their competitors are likely to benefit from expanded access to subcontracting opportunities. Prime contractors frequently build proposal teams months or even years before contract awards, and certified suppliers can immediately participate in programs that require secure handling of CUI.

Organizations that delay certification may find themselves temporarily excluded from proposal teams or contract vehicles until they can demonstrate compliance. This timing factor can significantly influence revenue pipelines, as companies that achieve certification earlier may secure long-term subcontracting relationships and establish themselves as trusted partners within compliant supply chains. In contrast, late adopters may encounter increased difficulty re-entering programs once prime contractors have established stable networks of certified suppliers.

Over time, this first-mover advantage may reinforce the stratification of the DIB into tiers of contractors based on compliance readiness and cybersecurity maturity. Early adopters gain market access and supply-chain positioning, while organizations that delay certification may experience lost opportunities and increased competitive pressure.

FAR and DFARS Requirements Driving CUI Protection

The increasing importance of CMMC certification is directly tied to existing federal acquisition regulations governing the protection of sensitive government information. Many DoD contracts already include provisions within the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) that require contractors to safeguard government data.

One of the foundational requirements is FAR 52.204-21, which establishes basic safeguarding requirements for Federal Contract Information (FCI). This clause requires contractors to implement minimum cybersecurity controls to protect government information that is not intended for public release but does not rise to the level of CUI.

More stringent requirements apply when contractors handle Controlled Unclassified Information (CUI). Several DFARS clauses mandate specific cybersecurity protections for this data, including:

DFARS 252.204-7012 — Safeguarding Covered Defense Information and Cyber Incident Reporting

This clause requires contractors to implement the security requirements defined in NIST Special Publication 800-171, which includes 110 security controls designed to protect CUI stored or processed in non-federal systems. Contractors must also report cyber incidents affecting covered defense information and preserve forensic data related to those incidents.

DFARS 252.204-7019 — Notice of NIST SP 800-171 DoD Assessment Requirements

This clause requires contractors to conduct self-assessments against the NIST 800-171 controls and submit their resulting scores into the Supplier Performance Risk System (SPRS). The scores provide DoD visibility into the cybersecurity posture of contractors within the supply chain.

DFARS 252.204-7020 — NIST SP 800-171 DoD Assessment Requirements

This provision authorizes the DoD to conduct its own cybersecurity assessments of contractor systems to verify the accuracy of the reported SPRS scores and confirm that security controls are implemented as claimed.

DFARS 252.204-7021 — Cybersecurity Maturity Model Certification Requirements

This clause formally incorporates the CMMC framework into DoD contracts. It requires contractors to achieve and maintain a specific CMMC certification level—typically Level 2 for contracts involving CUI—before handling controlled information. The clause also requires prime contractors to flow down CMMC requirements to subcontractors, ensuring that all entities within the supply chain maintain appropriate cybersecurity protections.

Together, these FAR and DFARS provisions establish the regulatory foundation for CMMC and make cybersecurity compliance a contractual obligation rather than a voluntary best practice. As these clauses become more widely embedded in DoD solicitations and contract vehicles, organizations that lack compliant CUI environments may find themselves unable to access or process the information necessary to perform defense work.

Implications for the Defense Supply Chain

Because these requirements flow down through subcontracting relationships, their impact extends beyond prime contractors to thousands of suppliers across the defense ecosystem. Any organization that processes, stores, or transmits CUI in support of a DoD program must demonstrate the ability to protect that information in accordance with NIST 800-171 and CMMC requirements.

Consequently, the ability to operate a compliant CUI environment, whether through government cloud platforms, secure enclaves, or managed compliance solutions has become a prerequisite for participating in many defense programs. Contractors that lack these capabilities may find themselves limited to contracts involving only FCI or publicly releasable information, restricting their access to higher-value defense opportunities.

This regulatory environment further reinforces the competitive dynamics discussed earlier: companies that invest early in compliant architectures gain access to a broader set of defense programs, while organizations that delay investment may experience reduced market participation and diminished visibility within prime contractor supply chains.

Strategic Risks and Implications for Small Businesses Contractors

CMMC compliance introduces significant strategic and financial considerations for small businesses operating within the Defense Industrial Base (DIB). Many organizations must invest substantial capital in cybersecurity infrastructure, compliance architecture, and third-party assessments before securing or renewing Department of Defense (DoD) contracts. This creates financial exposure for contractors who must implement compliance capabilities without guaranteed contract awards or revenue recovery.

For many small contractors, the cost of compliance can approach or exceed annual IT budgets, particularly when implementing secure cloud environments, managed enclave solutions, or continuous monitoring capabilities required for CMMC Level 2. As a result, architecture decisions—such as adopting GCC High environments, managed VDI enclaves, or full government cloud deployments—have a long-term impact on operating costs and technical flexibility.

These economic pressures may also reshape the defense supply chain. Smaller subcontractors that are unable to invest in compliance infrastructure risk exclusion from the DoD ecosystem, potentially accelerating supplier consolidation toward larger prime contractors and well-capitalized vendors. Over time, this consolidation could reduce the diversity of innovative small businesses that historically contribute to the DIB.

At the same time, alternative compliance models—such as managed enclave providers or operating within prime contractor environments—may offer pathways for smaller companies to participate in defense programs while reducing the operational burden of maintaining independent compliance infrastructures. However, these models can introduce dependencies on external platforms and may limit operational control over sensitive data environments.

Policy Recommendations and Advocacy Opportunities

While the Cybersecurity Maturity Model Certification (CMMC) framework is intended to strengthen cybersecurity protections across the Defense Industrial Base (DIB), targeted policy measures may help ensure that small businesses remain able to participate in defense programs while meeting required security standards. Industry associations, including organizations representing veteran-owned and small defense contractors, have an opportunity to advocate for policies that reduce implementation barriers while maintaining the security objectives of the program.

Expand Allowability and Reimbursement of Cybersecurity Compliance Costs

Under the Defense Federal Acquisition Regulation Supplement (DFARS) cost principles, contractors may recover certain cybersecurity expenses as allowable costs. However, many small businesses remain uncertain about which CMMC-related costs—such as secure cloud migration, security monitoring tools, compliance consulting, and certification assessments—are eligible for reimbursement through contract pricing structures.

Advocacy efforts could focus on working with the DoD Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S) to issue clearer guidance that explicitly identifies CMMC compliance investments as allowable indirect costs. Expanded guidance would help contractors incorporate cybersecurity investments into contract pricing and reduce the financial risk associated with upfront compliance implementation.

Expand Use of Existing DoD Cybersecurity Assistance Programs

Several existing DoD initiatives already support cybersecurity improvements across the DIB and could be expanded to assist small businesses pursuing CMMC certification.

Project Spectrum

The Project Spectrum initiative provides cybersecurity training, threat intelligence, vulnerability assessments, and advisory support to DIB contractors. Expanding Project Spectrum to include structured CMMC readiness services—such as control implementation guidance, architecture recommendations, and documentation support—could significantly reduce the learning curve for small contractors preparing for certification.

Manufacturing Extension Partnership (MEP)

The Manufacturing Extension Partnership (MEP) network operates in all 50 states and provides operational assistance to small manufacturers. Several MEP centers already provide cybersecurity advisory services aligned with NIST standards. Expanding these services to include CMMC implementation support could help manufacturers adopt compliant architectures while leveraging existing trusted advisory networks.

Establish Small Business Cybersecurity Grant Programs

Because many small defense contractors operate with limited IT budgets, the upfront cost of implementing a compliant CUI environment can be a major barrier to participation in defense programs. Federal policymakers could explore targeted grant programs designed to support cybersecurity infrastructure investments for small businesses within the DIB.

Potential funding mechanisms could include:

- Small Business Innovation Research (SBIR) cybersecurity initiatives
- Small Business Administration (SBA) cybersecurity grant program
- Defense Production Act (DPA) Title III funding for cybersecurity infrastructure
- State-level cybersecurity resilience grant programs aligned with federal initiatives

These funding mechanisms could help offset investments required for secure cloud migration, monitoring infrastructure, endpoint security platforms, and certification readiness activities.

Introduce Cybersecurity Tax Incentives for Defense Contractors

Another potential policy approach involves introducing tax incentives for cybersecurity investments tied to national security programs. Similar to existing tax incentives used to encourage research and development spending, a cybersecurity tax credit could help small contractors offset investments in secure infrastructure required to protect sensitive government data.

Such incentives could apply to expenditures related to:

- Secure cloud migration and infrastructure deployment
- Security monitoring and threat detection systems
- Compliance consulting and readiness preparation
- CMMC certification assessments

Tax-based incentives may be particularly attractive because they provide support without requiring direct grant administration.

Develop Government-Sponsored Secure CUI Environments

A frequently discussed concept within the DIB policy community involves the creation of government-sponsored secure collaboration environments designed specifically for small defense contractors. These environments could allow organizations to operate within pre-certified infrastructures rather than building independent CMMC-compliant environments.

Shared environments could leverage existing federal cloud platforms such as:

- Microsoft 365 GCC / GCC High
- AWS GovCloud
- Oracle GovCloud
- GCP Public

By inheriting many underlying security controls from these platforms, small contractors could significantly reduce the cost and complexity associated with implementing independent CUI environments.

Encourage Prime Contractor Cybersecurity Mentorship Programs

Prime contractors play a central role in managing cybersecurity risk across defense supply chains. Expanding mentorship programs in which prime contractors assist smaller subcontractors with cybersecurity readiness could help strengthen the entire ecosystem.

Such programs could include:

- Technical guidance on implementing NIST SP 800-171 controls
- Shared security architecture designs
- Access to secure collaboration environments
- Assistance with preparing documentation required for certification

Encouraging prime contractors to actively support supplier cybersecurity readiness could help preserve diversity within the DIB while maintaining strong security standards.

Provide Standardized Compliance Documentation and Reference Architectures

A significant portion of CMMC implementation costs arises from developing policies, procedures, and evidence documentation required for certification. Providing standardized templates and reference architectures could reduce redundant effort across thousands of contractors.

Potential resources include:

- System Security Plan (SSP) templates aligned with NIST SP 800-171
- Plan of Action and Milestones (POA&M) templates
- Incident response playbooks tailored for CUI environments
- Reference architectures for GCC High and GovCloud deployments

Centralized guidance from the DoD or the Cyber AB could improve consistency across the ecosystem and reduce reliance on costly consulting engagements.

Expand the Capacity of CMMC Third-Party Assessment Organizations (C3PAOs)

As CMMC requirements become embedded in more DoD contracts, demand for certification assessments is expected to grow significantly. A shortage of authorized CMMC Third-Party Assessment Organizations (C3PAOs) could lead to scheduling delays and increased assessment costs.

Expanding the assessor ecosystem by encouraging additional organizations to pursue C3PAO accreditation and increasing training for certified assessors would help prevent bottlenecks in the certification process.

Ensuring sufficient assessor capacity will be essential for maintaining momentum as the CMMC program transitions from voluntary preparation to contractual enforcement.

Economic Impact of CMMC Across the Defense Industrial Base

The implementation of the Cybersecurity Maturity Model Certification (CMMC) program represents one of the most significant cybersecurity investments ever undertaken across the Defense Industrial Base (DIB). The DIB includes a vast network of organizations that support Department of Defense (DoD) missions through research, manufacturing, logistics, software development, and specialized technical services. According to estimates from the Department of Defense, the broader defense supply chain includes more than 220,000 companies, the majority of which are small businesses.

Small businesses represent a substantial portion of this ecosystem and historically account for approximately 70–75 percent of companies participating in the defense supply chain. These organizations provide specialized capabilities ranging from advanced manufacturing and materials science to software development, engineering services, and niche component production. As a result, the economic impact of cybersecurity requirements within the DIB extends far beyond large prime contractors and affects thousands of smaller suppliers that support defense programs.

The introduction of CMMC certification requirements is expected to drive a significant increase in cybersecurity spending across this ecosystem. Contractors handling Controlled Unclassified Information (CUI) must implement technical controls aligned with NIST Special Publication 800-171, maintain secure environments capable of protecting sensitive defense information, and undergo periodic assessments conducted by authorized third-party organizations. These requirements necessitate investments in secure cloud infrastructure, identity management systems, security monitoring platforms, vulnerability management tools, and formal cybersecurity governance programs.

For individual contractors, the cost of implementing and maintaining CMMC-compliant environments varies widely depending on organizational size, technical complexity, and the chosen compliance architecture. As discussed earlier in this report, small businesses may adopt several different implementation models, including encrypted collaboration platforms, managed enclave environments, government cloud platforms such as Microsoft GCC High, or dedicated infrastructure deployed in AWS GovCloud, Azure Government, or Oracle Government Cloud regions. Each of these approaches involves different levels of infrastructure investment, operational complexity, and recurring costs.

When aggregated across the entire defense supply chain, the financial implications become substantial. Even conservative estimates suggest that if a portion of the roughly 220,000 organizations within the DIB invest tens or hundreds of thousands of dollars in cybersecurity infrastructure and certification readiness, the total cybersecurity investment associated with CMMC implementation could reach tens of billions of dollars over the coming decade. While these investments strengthen national security by improving the protection of sensitive defense information, they also represent a major structural shift in how cybersecurity capabilities are funded across the defense contracting ecosystem.

Beyond direct cybersecurity expenditures, CMMC implementation may also influence broader market dynamics within the DIB. Organizations that successfully implement compliant environments will be positioned to compete for contracts involving sensitive defense technologies and CUI. Conversely, contractors that lack the resources to implement these protections may face reduced participation in certain segments of the defense marketplace. This dynamic could accelerate consolidation within portions of the supply chain while simultaneously creating new opportunities for cybersecurity service providers and managed compliance platforms.

Despite these challenges, the widespread adoption of stronger cybersecurity practices may ultimately produce long-term benefits for the DIB. By establishing consistent security standards across contractors and suppliers, CMMC helps reduce the risk of cyber espionage, intellectual property theft, and supply chain compromise. Over time, improved cybersecurity maturity across the defense ecosystem may strengthen trust between government agencies, prime contractors, and subcontractors while enhancing the resilience of national security supply chains.

However, balancing these security improvements with the economic realities faced by small businesses remains a critical policy consideration. Ensuring that small contractors can continue to participate in defense programs while meeting cybersecurity requirements will be essential to preserving the diversity, innovation, and technical specialization that define the Defense Industrial Base.

Projected Timeline for CMMC Implementation Across DoD Contracts (2025–2030)

The Department of Defense is implementing the Cybersecurity Maturity Model Certification (CMMC) program through a phased regulatory rollout designed to gradually incorporate certification requirements into defense contracts. This phased approach is intended to allow contractors sufficient time to prepare for certification while enabling the DoD to scale the assessment ecosystem and integrate cybersecurity requirements across the Defense Industrial Base (DIB).

The regulatory foundation for this rollout is established through the CMMC Program Rule (32 CFR Part 170) and the incorporation of DFARS clause 252.204-7021, which formally requires contractors to achieve a specified CMMC level before handling certain categories of defense information. Once implemented in solicitations, these requirements will apply not only to prime contractors but also to subcontractors through mandatory flow-down provisions.

2025 – Initial Rule Implementation

Beginning in 2025, the DoD is expected to begin inserting CMMC requirements into a limited number of new solicitations and contract vehicles. During this early phase, the Department will primarily require CMMC Level 1 or Level 2 self-assessments depending on whether contracts involve Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).

Contractors handling CUI must already comply with DFARS 252.204-7012, which requires implementation of the 110 security controls defined in NIST SP 800-171, as well as submission of self-assessment scores into the Supplier Performance Risk System (SPRS) under DFARS 252.204-7019. The early implementation phase allows organizations to continue using these self-assessment mechanisms while preparing for third-party certification.

2026–2027 – Expansion of Third-Party Certification Requirements

During the next phase of implementation, the DoD is expected to increase the number of solicitations requiring CMMC Level 2 certification through accredited CMMC Third-Party Assessment Organizations (C3PAOs). Contracts involving the processing, storage, or transmission of CUI will increasingly require contractors to demonstrate verified compliance prior to award.

This period is likely to represent the most significant transition point for the DIB. Organizations that have not yet implemented compliant CUI environments may find themselves unable to compete for certain programs until certification is achieved. As a result, many contractors are expected to accelerate investments in cybersecurity infrastructure and compliance readiness during this timeframe.

2028–2030 – Broad Integration Across the Defense Supply Chain

By the end of the decade, CMMC requirements are expected to be integrated into the majority of DoD solicitations that involve sensitive government information. At this stage, certification will likely become a standard prerequisite for participation in programs that require the handling of CUI.

Prime contractors will be required to ensure that subcontractors handling CUI also maintain appropriate CMMC certification levels, effectively extending the program's reach throughout multiple tiers of the defense supply chain. As these requirements propagate across the ecosystem, cybersecurity compliance will become a routine operational requirement rather than a preparatory activity.

Strategic Implications of the Implementation Timeline

The phased rollout of CMMC creates a limited window of opportunity for contractors to prepare before certification becomes a widespread contractual requirement. Organizations that invest early in compliant architectures and certification readiness may benefit from increased access to subcontracting opportunities and improved positioning within defense supply chains.

Conversely, contractors that delay preparation may encounter increased barriers to entry once certification requirements become embedded across major contract vehicles. For small businesses in particular, the next several years represent a critical period for evaluating compliance strategies, selecting appropriate technical architectures, and preparing for eventual certification assessments.

Understanding the timeline for CMMC implementation is therefore essential for both contractors and policymakers. While the program strengthens protections for sensitive defense information, ensuring that the transition occurs in a way that preserves small business participation within the DIB will remain an important strategic consideration for the Department of Defense and industry stakeholders alike.

Conclusion

The Cybersecurity Maturity Model Certification (CMMC) program represents a fundamental shift in how cybersecurity risk is managed across the Defense Industrial Base (DIB). By requiring contractors to implement verifiable cybersecurity controls and undergo independent assessments, the program significantly strengthens protections for Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). In doing so, CMMC helps address longstanding concerns regarding cyber espionage, intellectual property theft, and supply chain vulnerabilities that have historically affected the defense ecosystem.

Standardizing cybersecurity expectations across contractors also improves transparency and accountability within the supply chain. Prime contractors, subcontractors, and government agencies can operate with greater confidence that sensitive information is being protected through consistent security practices aligned with NIST SP 800-171 and related federal cybersecurity frameworks. Over time, these improvements are expected to enhance the overall resilience of the defense supply chain and reduce the likelihood of adversaries exploiting weaker security practices among smaller suppliers.

However, the transition to a certification-based cybersecurity framework also introduces significant economic and operational challenges—particularly for small businesses that form the backbone of the DIB. Implementing compliant CUI environments often requires substantial investment in secure cloud infrastructure, identity and access management systems, monitoring technologies, compliance documentation, and third-party assessments. For many small contractors, these investments represent costs that must be incurred before new contract opportunities materialize, creating financial exposure that may exceed existing IT budgets.

Without targeted federal support mechanisms, these economic pressures could unintentionally reduce participation by smaller suppliers within the defense marketplace. Contractors that lack the resources to implement compliant environments may find themselves excluded from programs involving sensitive defense technologies, even if their underlying technical capabilities remain valuable to national security missions. Over time, this dynamic could contribute to consolidation within the supply chain as prime contractors rely increasingly on a smaller pool of well-capitalized vendors that can more easily absorb compliance costs.

Such consolidation may also carry long-term strategic implications. Small businesses have historically played a critical role in driving innovation within the defense ecosystem, introducing emerging technologies, specialized engineering expertise, and niche manufacturing capabilities. Maintaining access to this diverse pool of innovators is essential for sustaining the technological edge of the United States and preserving competition within defense procurement markets.

Ensuring the long-term success of the CMMC program therefore requires balancing cybersecurity objectives with the economic realities faced by the organizations that comprise the defense supply chain. Targeted policy measures—including expanded cost allowability guidance, cybersecurity assistance programs, grant initiatives, shared secure infrastructure models, and expanded certification capacity—can help reduce barriers to compliance while preserving strong security standards.

Ultimately, CMMC has the potential to significantly strengthen the cybersecurity posture of the Defense Industrial Base while protecting sensitive government information from sophisticated adversaries. Achieving this objective while maintaining a healthy, diverse, and innovative supplier ecosystem will require continued collaboration between the Department of Defense, industry stakeholders, and policymakers to ensure that the program enhances national security without inadvertently constraining the small business participation that has long been a defining strength of the defense industrial base.

KROLL

SECTION 02

Appendix A - 5-Year Economic Modeling (Illustrative) & Enclave Solution Options

SECTION 02

Appendix A - 5-Year Economic Modeling (Illustrative) & Enclave Solution Options

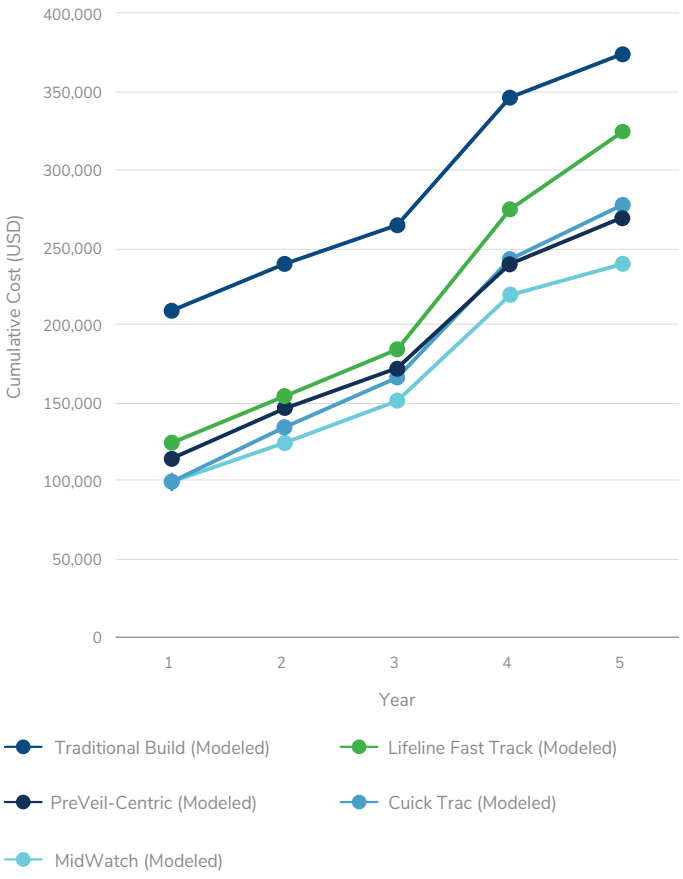
Economic Modeling & Enclave Solutions

Important note: The curves below are an illustrative economic model designed for advocacy discussions. Actual costs vary by scope, user count, tool stack, data types, and existing maturity. Where vendor pricing is not published, models use transparent assumptions and are clearly labeled.

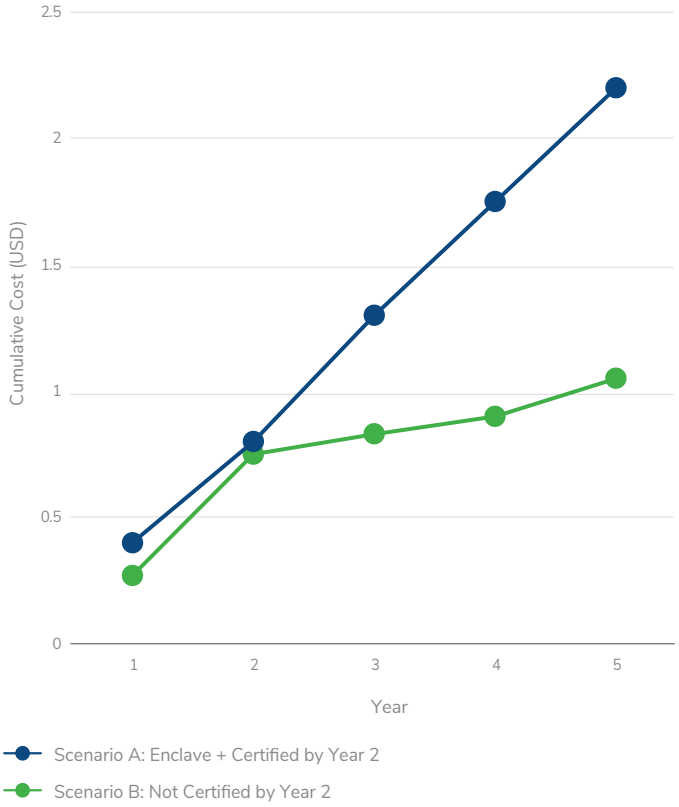
A. 5-Year Impact Curves (Example SMB: 10 CUI Users)

The chart below models cumulative 5-year TCO for several common strategies small businesses are using to reach and sustain CMMC Level 2 readiness and certification. The model includes a readiness/gap effort, annual sustainment, and C3PAO assessment costs in Year 1 and Year 4 (simplified recertification cycle).

Example SMB: 10 CUI users. Curves are modeled for advocacy discussions; actual costs vary by scope.



The second curve models a simplified economic outcome showing how certification timing can affect contract eligibility and revenue preservation. Example: 5-Year Net Impact (Revenue Preserved vs. Eligibility Loss) – Illustrative Scenario.



B. Solution Options & Pricing Models (Publicly Available Information + Transparent Assumptions)

Solution	What it is	Pricing model (public/observed)	Best fit	Notes / caveats
Lifeline Data Centers – CMMC Fast Track / FastTrack Enclave	Turnkey VDI enclave + SOC/SIEM + roadmap support; marketed as high control inheritance.	Public example cited: ~$3,300/month for 10 users + $275 setup + ~$20,000 vCISO fees (verify scope).	SMBs seeking fastest path with inherited controls and outsourced operations.	Pricing varies by apps and storage; confirm included Microsoft licensing, logging retention, IR support.
CUICK TRAC – Managed Enclave (CTME)	Managed virtual enclave/controlled environment with bundled security capabilities; month-to-month subscription.	Public signals: month-to-month user subscription; third-party listing and community posts suggest ~$295/user/month (confirm minimums).	SMBs wanting predictable bundled enclave with minimal internal overhead.	Official pricing generally quote-based; verify per-user vs per-environment and included services.
PreVeil – PreVeil Pass / Encrypted Email & File Sharing	End-to-end encrypted email + file sharing for CUI workflows; Pass includes documentation assets.	Published: $450/month for 3 users (PreVeil Pass) and Business plan at $30/user/month (add-ons may apply).	Firms with limited CUI handling who can enclave data paths rather than rebuild all IT.	Still need broader Level 2 controls: endpoint, logging, vuln mgmt, IR, governance, asset inventory. Workstations/Laptops will be in scope of CMMC certification no matter the location (Corporate or Home).
MidWatch – Defense Cybersecurity Group (DCG)	VDI-based compliance solution + consulting; positioned to reduce compliance burden for SMBs.	Quote-based. Modeled in curves as per-user/month enclave midpoint + onboarding consulting (assumption).	SMBs wanting services-led approach with vendor flexibility.	Ask for 3-year sustainment model, tool inclusions (EDR/SIEM/MDR), and boundary definition.

C. Pricing Model Notes (How to Compare Apples-to-Apples)

- Per user per month
  (licenses + VDI + storage + security tooling).
- One-time onboarding
  (migration, scoping, SSP/POA&M, training).
- Assessment support
  (evidence packaging, mock interviews, POA&M closure).
- 3-year sustainment
  (monitoring, patching, logging retention, IR support, policy maintenance).

D. Suggested Kroll Advocacy Framing

This model supports an advocacy position that (1) certification timing materially affects small business contract eligibility, and (2) enclave options can reduce time-to-readiness but still require federal support for sustainment and assessment costs.

SECTION 03

Appendix B - CMMC Compliance Architecture Cost Model

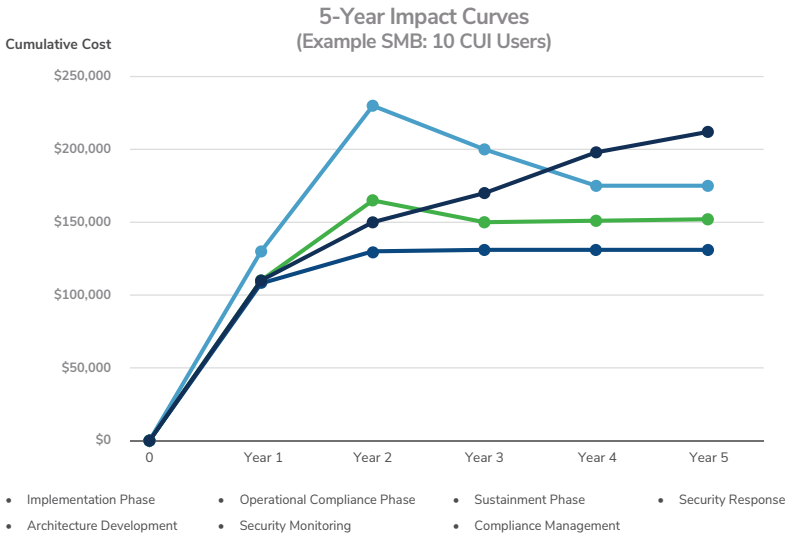
KROLL

SECTION 03

Appendix B - CMMC Compliance Architecture Cost Model

Organizations within the Defense Industrial Base (DIB) can pursue several different technical architectures to meet the cybersecurity requirements associated with protecting Controlled Unclassified Information (CUI) under NIST SP 800-171 and CMMC Level 2. Each approach presents different cost structures, operational constraints, and levels of control over sensitive environments. This appendix provides a comparative overview of common compliance architectures used by defense contractors.

Common CMMC Compliance Architecture Models



Encrypted Collaboration Platform	~ 165K
Managed Secure Enclave	~ 340K
Microsoft GCC High	~ 435K
Government Cloud	~ 670K

Encrypted Collaboration Platforms

Isolates CUI communications using platforms oencryptedn standard IT infrastructure

Examples:
- PreVeil

Pricing:
- Secure VDI
- $4-$7K/year
- Monitoring
- $20K-$40K
- Compliance Consulting
- $20K-$60K

5-year Cost Estimate
$80K-$200K

Managed Secure Enclave (VDI)

Provides fully managed secure environments through desktop virtualization

Examples:
- Lifeline Fast Track
- CUICK TRAC

Pricing:
- Secure VDI
- $0-$7K/year
- Monitoring
- $200K-$400K
- Compliance Consulting
- $20K-$60K

5-year Cost Estimate
$200K-$400K

Microsoft GCC High Environments

Government (community) Cloud environments tailored for defense industry compliance

Pricing:
- SGCC High
- $60-$120/ user /month
- Migration
- $40K-$60K/year
- Security Tools
- $20K-$50K
- Compliance Consulting
- $40K-$80K

5-year Cost Estimate
$250K-$500K

Full Government Cloud (AWS/Oracle/GCP)

Builds dedicated secure architectures in GovCloud environments

Examples:
- AWS GovCloud
- Oracle GovCloud
- GCP Public

Pricing:
- Cloud infrastructure
- $50K-$120K/ year
- Security Tools
- $30K-$60K
- Engineering
- $20K-$60K

5-year Cost Estimate
$400K-$1M+

Architecture Selection Considerations

When selecting compliance architecture, organizations must evaluate several strategic factors:

Operational Requirements

Organizations that require secure engineering collaboration, software development pipelines, or large-scale data processing may need more advanced cloud architectures.

Cost Sustainability

Compliance investments should be evaluated across the full lifecycle of a defense program, including licensing, monitoring, maintenance, and certification costs.

Supply Chain Participation

Some prime contractors may require subcontractors to operate within specific collaboration environments, influencing architecture decisions.

Certification Timeline

Organizations seeking rapid access to defense programs may prioritize architectures that allow faster readiness for CMMC assessments.

Relationship to the Economic Impact Model

The architecture cost ranges described in this appendix illustrate why CMMC compliance represents a major investment for small defense contractors. Because thousands of organizations across the DIB must implement compliant environments to handle CUI, the aggregated cybersecurity investment across the ecosystem is expected to reach tens of billions of dollars over the coming decade.

Understanding the cost trade-offs between these architectures is essential for both contractors planning their compliance strategies and policymakers seeking to ensure that cybersecurity requirements do not unintentionally reduce participation by small businesses within the defense supply chain.

Contacts

James Quilty
Vice President
Cyber Risk
+1 727 519 5587
james.quilty@kroll.com

Tiernan Connelley
Managing Director
Cyber & Data Resilience
+353 14283125
tiernan.connolly@kroll.com

Ira Levy
Associate Managing Director
Cyber & Data Resilience
+1 202 449 1854
ira.levy@kroll.com

Adriana Lamar
Director
CDR Professional Services
+1 212 297 9390
adriana.lamar@kroll.com

Louis Muniz
Senior Vice President
Cyber Risk
+1 201 319 8021
louis.muniz@kroll.com

About Kroll

As the leading independent provider of financial and risk advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.