The CMMC Decision

Second Edition

—

David W. Koran

CMMC Registered Practitioner Advanced

The CMMC Decision

Second Edition

April 2026

This book is provided for informational purposes only and does not constitute legal advice. CMMC requirements and program implementation
details continue to evolve through rulemaking, contract language, and Department of Defense guidance. Readers should validate applicability and requirements against their specific contracts, data types, and operating environments.

The views expressed in this book are those of the author and do not represent the positions of the CyberAB, the Department of Defense, or any other government agency.

For additional information: davidkoran.com

For Robert Willson, Esq.

Advisor, friend, and fellow sailor.

I sent him every unedited white paper I wrote.
He sent them back better, with suggestions that
sharpened the thinking and guided the direction.
His counsel shaped the business, the writing, and this book.

Fair Winds Bob

Acknowledgments and Disclaimer

This book is provided for informational purposes only and reflects a management perspective on CMMC preparation and readiness. It does not constitute legal advice and is not a substitute for qualified legal counsel, contractual review, or formal assessment guidance from a CMMC Third Party Assessment Organization. Nothing in this book should be construed as legal counsel or as guidance on any specific legal matter. CMMC requirements and program implementation details continue to evolve through rulemaking, contract language, and Department of Defense guidance. Organizations should validate applicability and requirements against their specific contracts, data types, and operating environments. Readers facing potential legal exposure related to CMMC compliance, SPRS scoring, or False Claims Act risk should consult a qualified attorney before taking action.

The enforcement cases and settlement figures cited in this book reflect publicly available information as of the publication date. Penalty ranges, regulatory requirements, and program implementation timelines are subject to change. Readers should verify current figures and deadlines through official government sources.

The views expressed in this book are those of the author and do not represent the positions of the Cyber AB, the Department of Defense, or any other government agency.

For additional information: davidkoran.com

Table of Contents

Chapter 4: The Twelve Month Roadmap

A phase by phase timeline from Discovery through Assessment Certification, including the evidence window, project management, and why the timeline resists compression

Chapter 5: The Expertise Gap

Why internal IT is not enough, the tool versus program confusion, the Registered Practitioner and Registered Practitioner Advanced credentials, and the training mandate

Chapter 6: Blind Spots

Physical security risks that live outside IT, from cleaning crews and third party access to the trash can test, printers, whiteboards, and after-hours building access

Chapter 7: The Dress Rehearsal

The mock audit process, the say-do gap, interview preparation, the mock audit report, and the go or no-go decision

Chapter 8: Assessment Day

Executive presence during formal Assessment Certification, the staff speak principle, the practitioner's limited role, the outbrief, and the post-assessment review process

Preface

The requirements behind CMMC 2.0 are not particularly complicated. The direction is clear, contractual implementation is advancing through phased adoption, and the costs, while substantial, are manageable for organizations that plan appropriately. The challenge is not the framework itself but the way the information reaches executives: buried in technical jargon, scattered across government websites, or filtered through vendors whose primary interest is selling a product or service rather than explaining a regulatory obligation.

What has been missing is a straightforward guide written for the person who has to make the investment decision, allocate the resources, accept the risk, and sign the certification.

I wrote this book for CEOs and senior executives of small and mid-sized defense contractors. These organizations form the backbone of the defense industrial base, yet they do not have the compliance departments or dedicated security teams that large prime contractors maintain. Their executives need to understand CMMC well enough to make informed decisions without becoming cybersecurity experts themselves.

This book will not make you a technical specialist. What it will do is provide the strategic framework to ask the right questions, evaluate the answers you receive, allocate resources appropriately, and lead your organization through

the compliance process. It will help you understand what you are actually signing when you certify your organization's security posture, and what that signature means in both legal and professional terms.

The organizations that navigate CMMC most effectively are the ones whose leadership treats it as a business decision rather than a technical project. Compliance is not something that can be delegated entirely to an IT department or outsourced without executive understanding of what is being committed to. The chapters that follow are designed to give you that understanding, clearly and without unnecessary complexity, so that when you sign your name to a certification you know exactly what it represents.

Introduction: The New Prerequisite for Growth

Cybersecurity is no longer an IT project. It is a revenue preservation strategy. For decades, defense contractors treated information security as a technical concern, something delegated to the IT department and addressed through periodic audits and self-assessments. Leadership involvement was minimal, budget allocation was reactive, and the connection between an organization's security posture and its business survival seemed abstract at best.

The Cybersecurity Maturity Model Certification program has fundamentally changed the relationship between security and revenue in the defense industrial base. CMMC certification is becoming a contractual requirement for organizations that intend to win and retain Department of Defense contracts. Solicitations will specify the required CMMC level, and organizations that have not achieved certification will not be eligible to compete. The practical consequence is that cybersecurity has moved from an operational overhead category to a market access requirement.

The shift from self-attestation to third-party validation represents the most significant structural change in the program. For years, contractors assessed their own compliance and reported scores with minimal verification. That system invited

optimism, enabled shortcuts, and produced security postures that existed more on paper than in practice. CMMC formalizes assessment pathways that include self-assessments and, for specified procurements, independent certification assessments conducted by CMMC Third Party Assessment Organizations. Organizations either meet the requirements and can demonstrate that they do, or they do not.

That shift creates both risk and opportunity for defense industry executives. Organizations that cannot achieve certification will lose access to contracts they may have held for decades. At the same time, organizations that achieve certification early will compete in a market with fewer qualified competitors as those unable or unwilling to meet requirements exit the defense industrial base entirely.

The decision facing executive leadership is not whether to comply; for organizations that intend to remain in the defense market, compliance is mandatory. The real decision is how to comply: how to scope a program efficiently, allocate resources effectively, manage the timeline realistically, and build a compliance posture that withstands both contract pressure and assessment scrutiny.

This book is written for CEOs and senior executives who need to understand CMMC well enough to govern their compliance programs without becoming technical specialists themselves. It addresses the questions executives actually ask: what this is going to cost, how long it will take, what happens if the

organization does not pass, and where the risks are that internal teams may not see.

The chapters that follow examine CMMC from an executive perspective. They explore the data categories that determine compliance scope, the liability framework that makes misrepresentation a federal matter, the actual costs that budgets often miss, the timeline that compliance realistically requires, the expertise gap that internal teams cannot fill alone, the physical security blind spots that derail otherwise well-prepared organizations, and the assessment process that determines whether the investment actually produces certification.

The goal is not comprehensive technical knowledge. The goal is executive competence: the ability to ask the right questions, evaluate the answers, make informed resource decisions, and lead an organization through a complex compliance process to successful certification.

Chapter 1: The Teeth of Compliance

For years, defense contractors assessed their own cybersecurity compliance with minimal oversight and even less consequence.

You checked the boxes on your self-assessment, submitted your score to the Supplier Performance Risk System, and moved forward with contract performance. Auditors rarely appeared. Enforcement was largely theoretical. The practical consequence of overstating your security posture was, for most organizations, nonexistent.

That era has ended.

The federal government has fundamentally restructured how it enforces cybersecurity requirements in the defense industrial base. What was once a contractual formality has become a legal liability with personal consequences for executives who misrepresent their organization's security status. Understanding this enforcement landscape is not optional for CEOs pursuing Department of Defense contracts. It is essential context for every investment decision and every attestation you will sign.

Three enforcement mechanisms now create substantial risk for defense contractors: the False Claims Act, personal liability doctrines targeting individual executives, and whistleblower provisions that incentivize internal reporting. Together, these mechanisms transform CMMC compliance

from a best efforts exercise into a legal obligation with serious consequences for failure.

The False Claims Act: Fraud Without Intent

The False Claims Act dates to the Civil War era, originally enacted to combat suppliers who sold defective goods to the Union Army.

In its modern form, it prohibits knowingly submitting false claims for payment to the federal government. Civil penalties are adjusted annually for inflation. As of the Department of Justice's July 2025 adjustment, penalties range from $14,308 to $28,619 per false claim, in addition to treble damages. Those figures are per claim. A single contract with multiple invoices can generate dozens or hundreds of individual violations.

The critical word in that definition is "knowingly." The False Claims Act does not require proof that you intended to defraud the government. It requires only that you knew, or should have known, that your claim was false. Deliberate ignorance and reckless disregard for the truth both satisfy this standard. Applied to cybersecurity, the implications are substantial. When you submit a bid for a DoD contract, you make representations about your security posture. When you attest to your CMMC level, you certify that specific controls are in place. When you accept contract payments while failing to maintain required security measures, you submit claims based on false premises.

The Department of Justice has made clear that it views cybersecurity misrepresentations as False Claims Act violations.

In October 2021, the Department announced its Civil Cyber-Fraud Initiative, explicitly targeting government contractors who misrepresent their cybersecurity practices. The Initiative focuses on three categories of conduct: knowingly providing deficient cybersecurity products or services, knowingly misrepresenting cybersecurity practices or protocols, and knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

This was not an abstract policy statement. In fiscal year 2025, the Department of Justice reported total False Claims Act recoveries exceeding $6.8 billion, the highest single year amount in the history of the statute. Within that total, cybersecurity related settlements accounted for more than $52 million across nine separate cases. Cybersecurity fraud recoveries have more than tripled in each of the past two years. The trajectory is clear, and it is accelerating.

The Cases That Define the Risk

The enforcement actions that have followed the Civil Cyber-Fraud Initiative illustrate both the breadth of the government's reach and the specificity of its expectations.

In 2022, Aerojet Rocketdyne agreed to pay $9 million to resolve allegations that it misrepresented its compliance with cybersecurity requirements in federal contracts. That case was initiated by a whistleblower, a detail that matters significantly for reasons discussed later in this chapter.

In March 2025, MORSECORP, a Massachusetts technology company, agreed to pay $4.6 million based on failures that

should be instructive for every defense contractor. The company's Department of Defense contracts incorporated CUI safeguarding requirements. MORSECORP failed to ensure that a third party software provider hosting its email complied with contract requirements for cloud service providers and FedRAMP Moderate equivalency. It failed to maintain a consolidated written plan for each of its covered information systems. It submitted an inaccurate SPRS self-assessment score and did not update that score after learning it was wrong. The company had given itself an SPRS score of 104. A subsequent third party assessment produced a score of negative 142. That is a gap of 246 points between what the company reported and what actually existed.

In May 2025, a major defense contractor paid $8.4 million to settle False Claims Act claims based on cybersecurity failures. A whistleblower alleged the contractor failed to implement NIST SP 800-171 requirements for its computer network, specifically the requirement to develop a system security plan. The government intervened, taking the position that compliance with contractual cybersecurity requirements was a condition of payment.

In September 2025, Georgia Tech Research Corporation settled for $875,000 over allegations that the university failed to adhere to proper standards in processing and storing controlled unclassified information related to Department of Defense contracts. In December 2025, Swiss Automation, an Illinois precision machining company, settled for $421,234 based on allegations that it failed to provide adequate cybersecurity as required by DFARS 252.204-7012 for technical drawings it received from contractors. That case was initiated by a former employee.

The pattern across these cases is consistent. The government does not distinguish between large and small contractors, between technology companies and machine shops, between universities and defense manufacturers.

The common element is misrepresentation: organizations that certified compliance they had not achieved, reported scores that did not reflect reality, or accepted contract payments while knowing their security posture did not meet contractual requirements.

The Criminal Dimension

Civil settlements represent one end of the enforcement spectrum. Criminal prosecution represents the other.

In December 2025, the Department of Justice unsealed a criminal indictment against a former senior manager at a defense contractor that provided cloud computing services to the Department of the Army. The alleged fraud exceeded $29 million. This is not a civil penalty or a negotiated settlement. It is a federal criminal case targeting an individual for conduct related to cybersecurity misrepresentation.

The distinction between civil and criminal enforcement matters for executive decision making. Civil cases produce financial penalties. Criminal cases produce personal consequences that no corporate insurance policy or indemnification agreement can mitigate. The December 2025 indictment signals that the Department of Justice is

willing to pursue individuals, not just organizations, when cybersecurity fraud reaches a sufficient scale.

Personal Liability: The Executive Accountability Standard

The enforcement framework does not treat cybersecurity compliance as a purely organizational matter.

Federal enforcement increasingly focuses on individual accountability. The "should have known" standard embedded in the False Claims Act applies to executives personally. A CEO who signs an attestation certifying that the organization meets specific cybersecurity requirements assumes personal responsibility for the accuracy of that certification.

The practical consequence is that willful blindness is not a defense. An executive cannot delegate cybersecurity compliance entirely to an IT department, decline to inquire about the organization's actual security posture, and then claim ignorance when the posture turns out to be materially deficient. The False Claims Act's knowledge standard captures precisely this behavior. If you had the ability to know and chose not to look, the law treats that choice the same as actual knowledge.

This is not a theoretical concern. The Department of Justice's enforcement pattern demonstrates a consistent focus on the gap between what organizations certified and what they actually implemented. Every case described in this chapter involved organizations that made representations to the federal government about their cybersecurity posture. In every case, those representations were materially inaccurate.

The executives who signed those representations bore responsibility for the accuracy of what they certified.

The Whistleblower Multiplier

The most significant enforcement accelerant in the False Claims Act framework is the qui tam provision, which allows private citizens to file lawsuits on behalf of the federal government.

Under the qui tam provision, an individual who has knowledge of false claims against the government can file a lawsuit in federal court. If the case results in a recovery, the whistleblower, known as a relator, receives a percentage of the proceeds. When the government intervenes and takes over the case, the relator typically receives between 15 and 25 percent. When the government declines to intervene and the relator proceeds independently, the percentage can reach 30 percent.

In fiscal year 2025, whistleblower actions reached an all time high, with 1,297 new qui tam suits filed and more than $5.3 billion recovered from those matters. Applied to cybersecurity enforcement, the qui tam provision creates a specific dynamic that defense industry executives need to understand. The person most likely to know that your organization's cybersecurity posture does not match its SPRS score is someone who works inside your organization: a system administrator, a compliance officer, a frustrated IT manager, or a former employee who left on difficult terms.

Of the nine cybersecurity related settlements in fiscal year 2025, five were initiated by whistleblowers. The Swiss Automation case was brought by a former employee. The MORSECORP case was a qui tam action. The Aerojet Rocketdyne settlement originated from whistleblower

allegations. The financial incentives for reporting are substantial. In 2025, whistleblowers in cybersecurity cases received more than $4.5 million in collective awards.

The practical reality is that your cybersecurity posture is not a matter that exists only between your organization and the Department of Defense. Every employee, contractor, and former staff member who has visibility into your actual security practices is a potential qui tam relator with a direct financial incentive to report discrepancies between your certifications and your operations.

The Certification Moment

Every enforcement mechanism described in this chapter converges at a single point: the moment an executive signs a certification attesting to the organization's cybersecurity posture.

That signature is not an administrative formality. It is a legal representation to the federal government that specific security controls are in place, functioning, and documented. If those controls are not in place at the time of certification, the signature creates False Claims Act liability. If the controls degrade after certification and the organization continues to accept contract payments without disclosing the change, additional liability accrues with each subsequent claim.

Before signing any CMMC attestation or SPRS self-assessment, an executive should be able to answer several questions with confidence. What specific controls are we certifying? Has an independent assessment verified that

those controls are actually implemented? Are there any open remediation items that would affect the accuracy of this certification? Do our internal teams have any concerns about the accuracy of what we are reporting? Are we prepared to defend this certification if the Department of Justice or a whistleblower challenges it?

If the answer to any of those questions is uncertain, the appropriate response is to resolve the uncertainty before signing. The cost of delaying a certification to ensure accuracy is always less than the cost of defending an inaccurate one.

Enforcement as Context for Investment

The enforcement framework described in this chapter is not presented to create alarm. It is presented to establish context for the investment decisions that follow in subsequent chapters.

CMMC compliance requires meaningful expenditure of time, money, and organizational attention. Executives making resource allocation decisions need to weigh those costs against the consequences of noncompliance. The enforcement landscape makes that calculation straightforward. Civil penalties starting at $14,308 per false claim, treble damages, potential criminal prosecution, whistleblower incentives that ensure internal visibility into compliance gaps, and an enforcement apparatus that has produced $52 million in cybersecurity settlements in a single fiscal year collectively define the risk of inaction.

At the same time, genuine compliance creates competitive advantage. As enforcement actions remove noncompliant competitors from the market, organizations that have invested in legitimate compliance programs compete in a smaller, more qualified field. The enforcement framework, viewed clearly, rewards organizations that take the requirement seriously and penalizes those that treat it as a paperwork exercise.

The chapters that follow examine the specific investments required: the data categories that determine compliance scope, the actual costs that budgets must account for, the timeline that compliance realistically requires, and the expertise that internal teams alone cannot provide. The enforcement context established here is the foundation for understanding why those investments are not discretionary.

Chapter 2: The Data Divide

Before an organization can determine what CMMC requires, it must first understand what kind of federal data it actually handles.

This is where most companies encounter trouble early in the compliance process. The common assumption is that holding a Department of Defense contract means the entire business falls under the highest security requirements. That assumption leads to inflated budget estimates, an overwhelming project scope, and a compliance effort that appears unmanageable before it begins.

The reality is more precise. CMMC compliance is not about securing everything an organization operates. It is about identifying the specific categories of federal data present in the environment and applying the appropriate level of protection to each. Getting this distinction right at the outset determines whether the compliance program will be efficient or wasteful, sustainable or unsustainable.

Two Categories of Federal Data

The Department of Defense is concerned with two types of information in contractor environments: information the government has provided and information created in performance of a federal contract.

Everything else, including payroll systems, commercial customer data, human resources records, and general business communications, falls outside the scope of CMMC

requirements entirely. The Department of Defense does not regulate how contractors manage their own business operations. It regulates how they protect federal information.

Federal data arrives in two distinct classifications, each carrying substantially different security obligations. Understanding the difference between these two categories is the foundation on which every subsequent compliance decision rests.

Federal Contract Information

Federal Contract Information, or FCI, represents the baseline category of protected federal data.

FCI encompasses information provided by or generated for the government under a contract that is not intended for public release. This includes contract terms, delivery schedules, pricing information, invoices, purchase orders, and general administrative correspondence related to contract performance. It is routine business information associated with government work.

While FCI requires protection from unauthorized disclosure, it does not carry national security implications if compromised. A leaked delivery schedule or pricing document is a contractual problem, not a strategic one. The security requirements that apply to FCI reflect this distinction. They are meaningful but manageable.

FCI is defined at FAR 52.204-21, which establishes the basic safeguarding requirements that apply to all government

contractors. Any organization performing work under a federal contract that generates or receives information not intended for public release is handling FCI and must meet the corresponding security requirements.

Controlled Unclassified Information

Controlled Unclassified Information, or CUI, represents a fundamentally different risk category.

CUI includes technical data, engineering specifications, designs, research findings, test results, and operational information that could compromise national security, provide adversarial advantage, or harm competitive positioning if disclosed. Examples include export controlled technical drawings, government furnished design specifications, critical infrastructure data, and information regarding military system capabilities or vulnerabilities.

The government designates information as CUI through contract language, marking requirements, and the categories established in the National Archives CUI Registry. When a contract includes DFARS 252.204-7012, the organization is handling CUI and must protect it according to the security requirements specified in NIST Special Publication 800-171.

The distinction between FCI and CUI is not a matter of degree. It is a structural difference that determines which CMMC level applies, what security controls must be implemented, how compliance is verified, and what the organization will spend to achieve and maintain certification.

The Three CMMC Levels

CMMC 2.0 establishes three certification levels, each corresponding to the sensitivity of the information being protected and the rigor of the verification process.

Level 1 applies to organizations that handle only Federal Contract Information. It requires implementation of 17 basic security practices derived from FAR 52.204-21. These practices represent the floor of responsible cybersecurity: limiting system access to authorized users, protecting information during transmission and storage, maintaining current antivirus and malware protection, identifying and addressing vulnerabilities, controlling physical access, and maintaining data recovery capability. Level 1 compliance is verified through annual self-assessment. The organization evaluates itself against the requirements, affirms the results, and enters its score into the Supplier Performance Risk System. No third party assessor is involved.

Level 2 applies to organizations that handle Controlled Unclassified Information. It requires implementation of all 110 security requirements specified in NIST Special Publication 800-171 Revision 2, organized across 14 security domains: access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, and system and information integrity. For most contracts involving CUI, Level 2 certification requires a formal third party assessment

conducted by a CMMC Third Party Assessment Organization, referred to as a C3PAO. The resulting certification is valid for three years. For some contracts where the CUI risk is lower, self-assessment may be permitted, but the trend in Department of Defense contracting is toward requiring third party certification for contracts involving sensitive technical information.

Level 3 applies to organizations working on the most sensitive national security programs. It builds on the 110 requirements from Level 2 and adds enhanced security requirements from NIST Special Publication 800-172, which addresses advanced persistent threats from sophisticated state actors. Level 3 assessments are conducted by the Defense Contract Management Agency rather than private C3PAOs. This level applies to a relatively small number of contractors working on the highest priority Department of Defense programs, and those organizations are identified directly by the government.

For the overwhelming majority of defense contractors, the relevant question is whether the organization is operating at Level 1 or Level 2. That determination depends on a single factor: does the organization handle CUI?

Level 1 in Practice

If an organization handles only FCI, Level 1 is the compliance target.

The 17 practices required at this level represent the floor of responsible cybersecurity, and most organizations with mature IT management will find they are already close to

compliant. The requirements cover fundamentals: limiting system access to authorized users and restricting what those users can do, protecting information during transmission and storage, maintaining current antivirus and malware protection, identifying and addressing security vulnerabilities, controlling physical access to systems and data, and maintaining the ability to recover data in the event of a loss.

None of these requirements are exotic. They represent hygiene-level practices that competent IT management should already include. The compliance requirement at Level 1 is the ability to affirm, accurately and honestly, that these controls are in place and functioning.

The annual self-assessment and affirmation process is straightforward but not without consequence. An executive with authority to bind the organization signs the affirmation, certifying that the 17 practices are implemented. That signature carries the same legal weight described in Chapter 1. A false affirmation is a false claim. For organizations that genuinely maintain basic security practices, Level 1 compliance should not require significant additional investment. For organizations that have deferred even basic cybersecurity hygiene, Level 1 compliance may surface gaps that require attention before an honest affirmation can be signed.

Level 2: Where the Investment Begins

Level 2 represents a substantial increase in both the number of requirements and the rigor of verification.

Moving from 17 practices at Level 1 to 110 security requirements at Level 2 is not a proportional increase in effort. It is a qualitative shift in what the organization must build, document, operate, and demonstrate. Level 2 compliance requires capabilities that most small and mid-sized defense contractors do not have in place: multi-factor authentication across all CUI systems, endpoint detection and response platforms, security information and event management systems, encrypted communications for all CUI transmission, formal incident response plans with tested procedures, comprehensive audit logging with defined retention periods, configuration management baselines for every system in scope, and written policies and procedures for each of the 14 security domains.

The documentation burden alone is substantial. CMMC Level 2 requires a System Security Plan that describes every in-scope system, the security controls applied to each, and how those controls satisfy each of the 110 requirements. It requires a Plan of Action and Milestones for any requirement that is not yet fully implemented. It requires policies, procedures, and evidence of consistent execution for every security domain. When an assessor arrives, the organization must be able to demonstrate not only that controls exist but that they have been operating consistently over a sustained period.

The assessment itself is rigorous. A C3PAO assessment team reviews documentation, interviews personnel across multiple organizational roles, examines technical configurations, and tests controls through direct observation. The assessment evaluates whether the organization meets each of the 110 requirements as MET,

NOT MET, or NOT APPLICABLE. The organization must achieve a MET determination on a sufficient number of requirements to receive certification, and certain requirements are weighted more heavily than others. A failed assessment means the investment in preparation does not produce certification until the identified deficiencies are remediated and a reassessment is conducted.

The Scoping Decision That Determines Cost

The most consequential financial decision in CMMC compliance occurs before any technology is purchased or any policy is written.

That decision is scoping: defining which systems, networks, facilities, and personnel fall within the compliance boundary. Every system that processes, stores, or transmits CUI must meet Level 2 requirements. Every system outside that boundary does not. The difference between a broad scope and a narrow scope can represent hundreds of thousands of dollars in implementation cost and years of ongoing maintenance expense.

Most defense contractors maintain substantially less CUI than initial assessments suggest. A mid-sized manufacturing firm may assume that the entire network of 200 endpoints requires Level 2 controls because the company holds DoD contracts. A careful data flow analysis often reveals that CUI is concentrated in a small number of systems accessed by a limited number of personnel. The result is that Level 2 requirements may apply to 15 or 20 workstations rather than 200, with the remainder of the organization requiring only the Level 1 controls that are largely already in place.

The mechanism for achieving this is a CUI enclave: a defined, segregated environment where CUI is processed, stored, and transmitted under Level 2 controls, while the broader business network operates at Level 1. The enclave approach requires clear boundaries, strict access controls, and disciplined data flow management to prevent CUI from migrating into the general environment. When CUI escapes

the enclave, through an email forwarded to a general business account, a file saved to a personal device, or a document printed and carried to an unsecured area, the compliance boundary expands to include every system that information touched.

Scoping is examined in greater detail in Chapter 4 as part of the compliance timeline. For executive planning purposes, the critical principle is that the size of the compliance boundary directly determines the cost of compliance. Controlling that boundary is the single most effective financial lever available.

The Question Every Executive Must Answer

The enforcement framework described in Chapter 1 and the data categories described here converge on a practical question that every defense industry executive must resolve.

Does the organization handle CUI? If the answer is yes, the organization requires CMMC Level 2 certification, which means third party assessment, 110 security requirements, and the investment described in Chapter 3. If the answer is no, the organization requires Level 1 compliance, which means annual self-assessment against 17 practices and a signed affirmation.

The answer to that question is not always obvious. It requires reviewing every active federal contract, examining data requirements and DFARS clauses, tracing information flows through the organization, and understanding what the government has designated as CUI. Organizations that

assume they know the answer without performing this analysis risk one of two outcomes: investing in Level 2 controls they do not need, or operating at Level 1 when their contractual obligations require Level 2. The first outcome wastes resources. The second creates the False Claims Act exposure described in Chapter 1.

The chapters that follow address the financial, operational, and organizational implications of whichever level applies. Chapter 3 examines the actual costs that compliance programs require. Chapter 4 provides the timeline for achieving certification. Chapter 5 addresses the expertise that internal teams alone cannot provide. In each case, the scope and cost of the effort depend directly on the data categories and CMMC level established here.

Chapter 3: The Cost of Compliance

Every executive considering CMMC compliance asks the same question early in the conversation: what is this going to cost?

It is a reasonable question. CMMC compliance represents a significant capital expenditure, and responsible executives need accurate projections to secure budget approval, plan cash flow, and evaluate whether specific contracts justify the investment. Unfortunately, the answers most organizations receive before engaging qualified expertise are often incomplete. Vendor estimates tend to reflect only the products being sold. Internal IT estimates tend to reflect only the technology being deployed. Neither captures the full cost of achieving and maintaining certification.

The problem is not that the numbers are deliberately misleading. The problem is that CMMC compliance costs are distributed across multiple categories, and organizations that budget for only the obvious ones find themselves facing unplanned expenditures at the worst possible time, typically months into a process they cannot afford to restart.

This chapter examines compliance costs across three distinct phases: Discovery, Remediation, and Assessment Certification. It addresses the hidden costs that most initial estimates miss, provides benchmarking ranges for mid-sized organizations, and establishes the three year financial perspective that accurate planning requires.

The Three Phases of Compliance Cost

CMMC compliance costs fall into three sequential phases, each with distinct cost drivers and budget considerations.

Discovery is the diagnostic phase. It encompasses the scoping, data flow analysis, and control-by-control evaluation that establishes where the organization stands against the applicable requirements. Remediation is the implementation phase, where identified gaps are closed through technology deployment, policy development, process changes, and personnel training. Assessment Certification is the formal third party evaluation conducted by a C3PAO that determines whether the organization has earned certification.

Each phase must be adequately funded. Organizations that underinvest in Discovery produce inaccurate scoping that inflates remediation costs. Organizations that underinvest in Remediation arrive at Assessment Certification unprepared and either fail or must withdraw. Organizations that budget for Discovery and Remediation but neglect Assessment Certification costs find themselves unable to complete the process they have already invested in.

Discovery: The Diagnostic Investment

Discovery is the phase where an organization determines its actual compliance posture against the applicable CMMC level.

A thorough Discovery engagement evaluates every applicable security requirement, identifies where the organization

meets the standard and where it falls short, maps data flows to define the compliance boundary, and produces the findings that drive remediation planning. It is the foundation on which every subsequent decision rests.

Discovery costs vary widely depending on the size of the organization, how many locations it operates, and how complex the CUI environment turns out to be. For a small single location contractor, a focused Discovery engagement might run $5,000 to $10,000. For a mid-sized organization with multiple facilities and a broader data footprint, that number can reach $25,000 to $35,000 or more. The more complex the environment, the more ground there is to cover.

Discovery should produce several deliverables: a detailed findings report identifying every gap against the applicable requirements, a scoping analysis that defines the compliance boundary, a data flow map that traces CUI through the organization, and a remediation roadmap that prioritizes the work required. These deliverables become the planning documents for everything that follows.

Some organizations attempt to conduct Discovery internally to reduce costs. This approach carries risk. Internal teams often lack the methodology training required to evaluate controls objectively, and there is an inherent conflict in asking the people responsible for building and maintaining systems to evaluate whether those systems meet external standards.

There is also a category of findings that internal teams are structurally unable to see. Physical security is the most common example. Employees who walk past the same

propped open side door every morning stop registering it as a security condition. The rock holding the door open has been there for years. The printer in the hallway outside the controlled area has always been there. The visitor log at the front desk has not been reviewed in months. These are not technical failures. They are environmental conditions that become invisible to the people who work in them every day. An outside evaluator walking the facility for the first time will identify physical security gaps in the first hour that internal staff have not noticed in years. Chapter 6 examines these blind spots in detail.

This is one of the reasons organizations benefit from engaging a CMMC Registered Practitioner or Registered Practitioner Advanced for Discovery. Practitioners credentialed through the CyberAB are trained in the assessment methodology that mirrors what a C3PAO will evaluate during Assessment Certification. They bring the outside perspective necessary to see what internal teams cannot, combined with the domain expertise to evaluate both technical and physical controls against the standard. A thorough Discovery engagement will also identify opportunities to reduce the compliance boundary, a perspective that internal teams, already embedded in the existing environment, frequently miss. The savings from boundary reduction alone often exceed the cost of engaging external expertise for Discovery.

Remediation: Where the Majority of Cost Accumulates

Remediation is the most expensive phase of CMMC compliance and the one most frequently underestimated.

Remediation costs break down into three subcategories: technology, labor, and documentation. Each carries its own cost drivers, and all three must be addressed to achieve certification.

Technology investments for a Level 2 compliance program typically include endpoint detection and response platforms, security information and event management systems, multi-factor authentication infrastructure, encrypted communications capabilities, backup and recovery systems that meet retention requirements, and network segmentation to support enclave architecture. For a mid-sized organization with a CUI enclave of 20 to 40 systems, technology costs typically range from $40,000 to $80,000. Organizations with larger footprints, older infrastructure, or more complex network architectures will spend more.

These figures represent initial deployment. Most security platforms operate on annual subscription or licensing models, meaning technology costs recur every year the organization maintains certification. The annual cost of maintaining security tooling after initial deployment typically ranges from $15,000 to $35,000 depending on the platforms selected and the number of endpoints covered.

Labor costs represent both external consulting fees and internal staff time. External consulting and implementation support for a Level 2 program typically ranges from $35,000

to $60,000, covering remediation guidance, configuration support, and readiness validation. Internal labor costs are harder to quantify but no less real. CMMC compliance requires sustained attention from IT staff, management, and operational personnel. The cumulative opportunity cost of internal labor diverted to compliance activities typically represents $20,000 to $40,000 or more in absorbed productivity, depending on the organization's size and the scope of remediation required.

Documentation development is a cost category that surprises most organizations. CMMC Level 2 requires a System Security Plan, a Plan of Action and Milestones, policies and procedures for each of the 14 security domains, and evidence of consistent implementation over a sustained period. This is not a collection of templates with company names inserted. Assessors evaluate whether documentation reflects the actual operating environment. Custom documentation development typically costs $15,000 to $30,000 when performed by qualified personnel. Organizations that attempt to shortcut documentation by adapting generic templates frequently discover during Assessment Certification that their documentation does not match their environment, a finding that can prevent certification.

The Hidden Costs Most Budgets Miss

Beyond the three primary phases, several cost categories routinely catch organizations unprepared.

Managed Service Provider adjustments represent one of the most significant hidden costs in CMMC compliance. If the

organization relies on an MSP for IT management, and that MSP has administrative access to systems within the CUI environment, the MSP's infrastructure becomes part of the compliance boundary. Any MSP with administrative access to in-scope systems must operate at the same security level as the organization seeking certification. If the current MSP cannot meet these requirements, the organization faces a choice: fund the MSP's compliance effort, which will be reflected in increased service fees, or migrate to a provider that already meets the standard. Either option carries substantial cost, and migration carries additional risk and timeline impact. MSP-related adjustments can add $20,000 to $50,000 or more in annual operating costs, and migration projects can consume months of the compliance timeline.

Cloud service adjustments present a similar challenge. CMMC Level 2 requires that cloud services processing CUI meet FedRAMP Moderate equivalency or demonstrate equivalent security through other means. If the organization uses commercial cloud platforms that do not meet this standard, migration to compliant alternatives is required. The cost and complexity of cloud migration depend on how deeply embedded the current platforms are in daily operations.

Training program development represents both direct cost and ongoing commitment. CMMC requires security awareness training for all personnel and specialized CUI handling training for anyone who accesses controlled information. Commercial security awareness platforms cost $15 to $40 per user annually. CUI handling training may require custom development to address the organization's specific marking, storage, and transmission requirements.

Training is not a single event. CMMC requires ongoing training with annual refreshers. The budget must account for a sustainable program, not a single compliance exercise.

Physical security improvements are frequently overlooked because they fall outside the IT budget. Depending on the organization's facilities, compliance may require access control systems, visitor management procedures, secure storage for CUI media, document destruction equipment, and controlled areas for CUI processing. For manufacturing environments, this may extend to controlled parts storage, prototype areas, and certified destruction processes for scrap and rejected components containing controlled technical data. These costs are examined in detail in Chapter 6.

Opportunity cost of delayed contracts is perhaps the most significant hidden cost, though it never appears on a budget spreadsheet. The time required to achieve CMMC compliance is time during which the organization cannot bid on contracts requiring certification. Every month of delay represents potential revenue foregone. This cost argues for beginning compliance efforts early, before contract opportunities force compressed timelines that increase both cost and risk.

Assessment Certification: The C3PAO Investment

Assessment Certification is the formal third party evaluation that determines whether the organization's compliance program produces an actual certification.

A C3PAO assessment for CMMC Level 2 typically costs between $40,000 and $100,000, depending on the size of the assessment scope, the number of locations, and the complexity of the environment. The assessment involves a team of certified assessors who review documentation, interview personnel across multiple organizational roles, examine technical configurations, and test controls through direct observation. The assessment is typically conducted over several days on site, with additional time for pre-assessment document review and post-assessment reporting.

This cost represents the final gate in the compliance process. If the organization is not ready, the C3PAO assessment does not produce certification, and the investment is not recoverable. Deficiencies identified during Assessment Certification must be remediated before a reassessment can be scheduled, and the reassessment carries its own cost. The financial argument for thorough preparation, including the mock audit described in Chapter 7, is that it reduces the risk of an unsuccessful Assessment Certification, which is by far the most expensive possible outcome in the compliance process.

Benchmarking: What to Expect

Given the variability across organizations, precise universal budgets are not possible. However, benchmarking against similar organizations provides useful planning ranges.

For a mid-sized defense contractor with 50 to 150 employees, existing but immature security practices, and a defined CUI enclave of 20 to 40 systems, total CMMC Level 2 compliance costs typically range from $150,000 to $275,000 over an 18 to 24 month period. This breaks down approximately as follows: Discovery at $5,000 to $35,000 depending on organizational complexity, technology investments at $40,000 to $80,000, external consulting and implementation support at $35,000 to $60,000, documentation development at $15,000 to $30,000, internal labor opportunity cost at $20,000 to $40,000, Assessment Certification by C3PAO at $40,000 to $100,000, and MSP and cloud service adjustments that vary but can add $20,000 to $50,000 or more in annual operating cost increases.

Organizations with larger CUI footprints, multiple locations, or minimal existing security infrastructure should budget toward the higher end or beyond these ranges. Organizations with mature security programs, smaller enclaves, or existing documentation may achieve compliance at lower cost.

The Three Year Financial Perspective

CMMC certification is valid for three years, after which reassessment is required. Compliance

budgeting must account for this ongoing cycle, not merely initial certification.

First year costs are highest, encompassing the full Discovery, Remediation, and Assessment Certification process. Second year costs include maintaining implemented controls, continuing training programs, conducting internal reviews, and addressing any findings from initial certification. Third year costs include these ongoing maintenance activities plus preparation for recertification.

A reasonable estimate for ongoing annual compliance maintenance, exclusive of recertification costs, ranges from $30,000 to $60,000 for a mid-sized organization. This covers security tool licensing, MSP premiums, training programs, internal review activities, and periodic consulting support.

One of the most effective uses of ongoing maintenance budget is retaining a Registered Practitioner or Registered Practitioner Advanced on a recurring engagement to verify that controls remain in place and operating as documented. Security postures degrade over time. Staff turnover introduces personnel who have not been trained. Configuration changes drift from documented baselines. Policies that were followed rigorously in the months before certification receive less attention once the immediate pressure subsides. An RP or RPA conducting periodic reviews, whether quarterly or semiannually, identifies these issues while they are still correctable rather than allowing them to accumulate into findings that surface during recertification. Organizations that maintain this kind of ongoing practitioner relationship approach their three year

reassessment with confidence rather than uncertainty, because compliance has been verified continuously rather than reconstructed under deadline pressure.

Recertification costs in year three should approximate 60 to 75 percent of initial certification costs, assuming no significant changes to the environment or requirements. Major changes to scope, substantial remediation needs identified during maintenance, or increased program requirements could increase this figure.

Total three year compliance costs for a mid-sized organization, including initial certification and ongoing maintenance, typically range from $275,000 to $450,000. This represents the true cost of maintaining access to Department of Defense contracts requiring CMMC Level 2 certification.

Building the Business Case

These figures represent substantial investment. For many organizations, CMMC compliance costs will exceed any previous cybersecurity expenditure.

Securing budget approval requires framing compliance as investment rather than expense, and the business case rests on three foundations.

Revenue protection is the most direct calculation. If the organization derives $5 million annually from contracts that will require CMMC certification, the compliance investment protects that revenue stream. Failure to achieve certification means losing that revenue entirely. Measured against the

three year cost of compliance, the investment typically represents a fraction of the revenue it preserves.

Competitive positioning is the strategic benefit. CMMC creates qualification requirements that will reduce competition for certified organizations. Competitors unwilling or unable to invest in compliance will exit the defense market. Organizations that achieve certification early compete in a field with fewer qualified participants.

Risk mitigation addresses the enforcement context established in Chapter 1. False Claims Act penalties, personal liability, and whistleblower incentives create potential costs that dwarf any compliance investment. Genuine compliance eliminates this exposure. The security improvements required for CMMC also reduce actual breach risk, protecting the organization from incident costs that can reach millions of dollars.

The question is not whether to invest in CMMC compliance. For organizations dependent on Department of Defense revenue, compliance is a business requirement. The question is whether to invest proactively, with adequate time and resources to achieve genuine compliance, or reactively, under the pressure of deadlines and competition. Proactive investment is almost always less expensive and more effective.

The next chapter translates these cost frameworks into a practical timeline, mapping the twelve month roadmap for achieving CMMC certification.

Chapter 4: The Twelve Month Roadmap

The most common question after cost is timeline: how long will this take?

The honest answer is that CMMC compliance cannot be rushed. Organizations that attempt to compress the timeline inevitably encounter problems: incomplete remediation, insufficient evidence, failed Assessment Certifications, and costs that exceed what a properly paced program would have required. The compliance process has natural phases that resist acceleration, and understanding these phases is essential for realistic planning.

A well executed CMMC Level 2 compliance program requires twelve to eighteen months from initiation to certification. Some organizations with mature security programs and limited scope may achieve certification faster. Organizations with significant gaps, complex environments, or resource constraints may require longer. Twelve months represents a reasonable baseline for planning purposes, and it is the timeline examined here.

This chapter provides a phase by phase roadmap for achieving CMMC certification. The timeline assumes an organization with moderate existing security maturity, a defined but not yet secured CUI environment, and adequate resources to maintain momentum throughout the process. Adjust the timeline based on specific circumstances, but resist the temptation to compress phases that require time to execute properly.

Months One and Two: Discovery

The first two months establish the foundation for everything that follows.

This phase has two primary objectives: defining precisely what requires protection and understanding exactly where the organization stands today. These objectives correspond to scoping and gap analysis, which together constitute the Discovery process described in Chapter 3.

Scoping determines the compliance boundary. As discussed in Chapter 2, CMMC requirements apply only to systems that process, store, or transmit CUI. Every system outside this boundary represents cost the organization does not need to incur. Scoping is therefore both a compliance activity and a cost optimization exercise.

Effective scoping requires tracing CUI through the organization. Where does it enter? Who receives it? Where is it stored? Who accesses it? Where does it go when work is complete? This data flow analysis identifies every system, device, network segment, and physical location that touches CUI. The scoping exercise should also identify opportunities to reduce the compliance boundary. Can CUI be consolidated onto fewer systems? Can network segmentation create a smaller enclave? Can process changes eliminate CUI from systems where it does not need to reside?

Gap analysis evaluates the organization's current security posture against every applicable requirement. For Level 2, this means a control by control evaluation against all 110 requirements in NIST SP 800-171. Each requirement receives a determination: met, partially met, or not met. The

result is a precise understanding of where the organization stands and how far it needs to travel.

The gap analysis must be honest. Optimistic self-evaluation at this stage compounds into problems at every subsequent phase. Requirements rated as met when they are only partially implemented will not receive remediation attention. When those gaps surface during Assessment Certification, the organization faces findings it could have addressed months earlier. The gap analysis is sometimes called the honesty mirror for exactly this reason. It reflects the organization's actual security posture, not the posture leadership assumes exists.

By the end of month two, the organization should have a defined compliance boundary, a complete gap analysis against applicable requirements, a data flow map, and a prioritized remediation roadmap. These deliverables drive every decision for the remaining ten months.

Months Three Through Six: Remediation

Remediation is where the organization closes the gaps identified during Discovery.

This is the most labor intensive phase of the compliance program and the period where most of the budget described in Chapter 3 is consumed. Remediation work falls into four parallel tracks: technology deployment, documentation development, process implementation, and physical security.

The author's recommendation is to treat the entire CMMC compliance effort as a formal project, and remediation in

particular should be run through a project manager with clear task assignments, deadlines, and accountability. Four parallel tracks with dependencies across internal departments, external vendors, and the consulting team will not manage themselves. A qualified CMMC consultant should arrive with a project template ready to deploy, structured around the remediation findings from Discovery, with tasks defined and ready for assignment to internal and external resources. This is not an area where the organization should be inventing a management structure from scratch. The project plan becomes the operating document for the next four months, tracking what needs to be done, who is responsible, what the dependencies are, and whether the program is on schedule. Organizations that run remediation without formal project management consistently underestimate the coordination required and arrive at the evidence window with work still incomplete.

Technology deployment addresses gaps that require new capabilities. This typically includes implementing endpoint detection and response, deploying multi-factor authentication, configuring security information and event management, establishing encrypted communications for CUI, implementing network segmentation to define the enclave boundary, and configuring backup and recovery systems that meet retention requirements. Technology deployment should be sequenced based on dependencies. Network segmentation often needs to come first because it defines the enclave that other controls will protect. Authentication and access controls follow because they determine who can reach the enclave. Monitoring and logging come next because they need to capture activity across the controls already in place.

Documentation development runs in parallel with technology deployment. CMMC Level 2 requires a System Security Plan that describes every in-scope system and the controls applied to each. It requires policies and procedures for each of the 14 security domains. It requires a Plan of Action and Milestones for any requirement not yet fully implemented. These documents must reflect the actual environment, not generic templates with the organization's name inserted. Assessors evaluate whether documentation matches the operating reality.

Process implementation addresses requirements that are not purely technical. Access review procedures, incident response plans, change management processes, vulnerability management programs, and personnel screening procedures all require definition, documentation, testing, and training. Process implementation also includes CUI handling training for all personnel who access controlled information and security awareness training for the broader workforce.

The training component of remediation deserves specific attention because it requires coordination across departments that do not normally interact on cybersecurity matters. The organization's CMMC consultant should be working directly with human resources and the corporate training function during this phase to develop the employee training program. The consultant brings the subject matter expertise on what CMMC requires employees to know and how assessors will evaluate training effectiveness. HR and corporate training bring the delivery infrastructure, the scheduling authority, and the institutional knowledge of how to reach every employee in the organization. CUI handling training in particular must be tailored to the organization's

specific environment, its marking conventions, its storage locations, its transmission rules, and its destruction procedures. This is not a generic awareness module purchased off the shelf. It is training that reflects how this organization handles controlled information in its actual operations, and building it takes time.

Physical security remediation is a fourth track that organizations frequently overlook during this phase because it falls outside the IT budget and outside the IT team's authority. Some facilities simply do not meet the physical protection standards required for areas where CUI is processed or stored. Discovery may have identified the need for access control systems on doors to CUI areas, visitor management procedures and logs, secure storage for CUI media, document destruction equipment, or controlled areas that prevent unauthorized visual access to screens and documents. In manufacturing environments, this may extend to controlled parts storage, prototype areas, and secure handling of technical drawings on the shop floor. Physical security improvements often require facilities management involvement, contractor coordination, and lead times for equipment procurement and installation. Organizations that defer physical security remediation to the final months of the program discover that construction timelines and equipment delivery schedules do not compress to meet certification deadlines. Chapter 6 examines these physical security requirements in detail.

By the end of month six, the majority of remediation work should be complete. Controls should be implemented and operational. Documentation should be drafted and under review. Processes should be defined and personnel should be

trained. The organization should be approaching a state where it is ready to begin demonstrating consistent operation of its security program.

Months Seven Through Nine: The Evidence Window

CMMC certification requires more than demonstrating that controls exist at the moment of assessment. It requires demonstrating that controls have been operating consistently over a sustained period.

This is the evidence window, and it is the phase that most frequently surprises organizations that have not planned for it. An assessor will expect to see evidence of control operation spanning at least 90 days. Audit logs must show continuous monitoring over that period. Process records must demonstrate consistent execution of required procedures. Training records must show that personnel were trained and operating within the security program, not that training occurred the week before the assessment.

The evidence window cannot be compressed. Ninety days of logs require ninety days. There is no shortcut, no workaround, and no substitute. Organizations that complete remediation in month eight instead of month six face a corresponding delay in their certification timeline because the evidence window must still run its full duration.

During this phase, the organization must maintain disciplined execution of every implemented control and process. Audit logs must be generated, collected, and retained according to documented retention policies. Verify early in the evidence window that logging is configured correctly and retention periods are sufficient. A common failure is discovering during final preparation that logging

was enabled but retention was set too short, leaving the organization without evidence for the required period.

Process execution records must demonstrate that operational processes function as documented. If the vulnerability management procedure requires monthly scanning, there must be records of monthly scans. If the access review process requires quarterly reviews, there must be documentation of those reviews. If the incident response plan requires annual testing, there must be evidence of that test. Create a calendar of required process activities and verify that each one is executed and documented on schedule. Assign responsibility for each activity to a specific individual. A single missed process cycle during the evidence window creates a gap that assessors will identify.

Training records should show that personnel completed required training early in the evidence window, demonstrating that trained personnel were operating within the security program throughout the period. Training completed immediately before Assessment Certification suggests a compliance exercise rather than a genuine security culture.

By the end of month nine, the organization should have at least 90 days of evidence demonstrating control operation. Logs should show continuous monitoring. Process records should document consistent execution. Training and acknowledgment records should demonstrate organizational awareness. This evidence portfolio is what positions the organization for successful Assessment Certification.

Months Ten Through Twelve: Mock Audit and Assessment Certification

The final phase of the compliance program includes mock audits to verify readiness, remediation of any identified weaknesses, and the formal C3PAO Assessment Certification.

Organizations should plan for more than one mock audit during this phase. The first mock audit, conducted early in month ten, establishes the current state of readiness and identifies gaps that require attention. After those findings are addressed, a second mock audit verifies that remediation was effective and that the organization is genuinely prepared for the formal Assessment Certification. A single mock audit leaves the organization guessing about whether its corrections actually resolved the identified issues. Multiple iterations provide the confidence that comes from verified improvement.

Each mock audit simulates the formal Assessment Certification experience. The evaluator reviews documentation, examines technical configurations, interviews personnel, and evaluates evidence using the same methodology a C3PAO will employ. Mock audits identify remaining gaps before the formal certification, when the consequences of findings are substantially greater. They familiarize personnel with the assessment experience, reducing anxiety and improving performance during the actual evaluation. They validate that evidence is complete, organized, and accessible. Chapter 7 examines the mock audit process in detail.

Mock audits should be conducted by a contracted third party consultant, not by internal personnel. Internal staff do not have the objectivity to evaluate their own work, and they will not replicate the experience of having an outside set of eyes scrutinize the program the way a C3PAO assessor will. Specifically, mock audits should be conducted by a Registered Practitioner Advanced who is trained and credentialed on the Level 2 controls and the assessment procedure. The RPA credential requires demonstrated knowledge of both the 110 NIST SP 800-171 security requirements and the methodology that C3PAO assessors use to evaluate them. That combination of control expertise and assessment procedure knowledge is what enables the mock audit to accurately predict how the organization will perform during the formal Assessment Certification.

There is an important principle embedded in this structure. A Registered Practitioner who has been advising the organization through Discovery and Remediation should never have been directly implementing controls or performing hands-on remediation work in the environment. The practitioner's role is advisory. The organization's team implements. This separation is not administrative formality. It is what preserves the objectivity required for the mock audit to have value. A practitioner who implemented the controls and then evaluates those same controls during the mock audit is auditing their own work. The result lacks the independent scrutiny that the exercise is designed to provide. The value of the practitioner relationship depends on maintaining this boundary throughout the engagement.

The first mock audit should occur early in month ten, with findings documented at the same rigor as a formal

assessment. Budget two to four weeks for each mock audit depending on organizational complexity. After findings from the first mock audit are remediated, the follow-up mock audit should occur in month eleven, providing a final verification of readiness before the formal Assessment Certification is scheduled.

Remediation of mock audit findings addresses any gaps that surface. Findings typically fall into three categories: documentation gaps where evidence exists but is not properly organized or accessible, minor control weaknesses requiring adjustment or enhancement, and significant deficiencies requiring substantial remediation. Documentation gaps and minor weaknesses can usually be addressed within a few weeks. Significant deficiencies may require timeline adjustment. It is far better to delay Assessment Certification than to proceed with known deficiencies that will result in failed certification.

C3PAO scheduling should begin early in this phase. C3PAO availability varies, and preferred dates may require scheduling weeks or months in advance. Begin communicating with potential C3PAOs in month ten to understand availability and reserve tentative dates. Select a C3PAO based on experience with organizations similar in size and industry, assessor qualifications, availability, and cost. Request references and speak with organizations they have previously assessed.

The formal Assessment Certification occurs in months eleven or twelve, depending on mock audit timing and C3PAO availability. The assessment typically spans three to five days for a mid-sized organization, though duration

varies based on scope and complexity. Final preparation in the weeks before Assessment Certification should focus on evidence organization, personnel readiness, and logistics. Ensure all evidence is accessible and well organized. Conduct final preparation sessions with personnel who will participate in assessor interviews. Arrange appropriate facilities for assessor work and interviews. Chapter 8 examines what to expect during Assessment Certification day itself.

Why the Timeline Resists Compression

Organizations under contract pressure frequently ask whether the twelve month timeline can be shortened.

Certain phases can be compressed under specific conditions. Organizations with mature security programs may complete Discovery in weeks rather than months. Organizations with existing technology infrastructure may require less remediation time. But two constraints are effectively irreducible.

The evidence window requires at least 90 days. This is a function of time, not effort. No amount of additional resources or parallel activity can produce 90 days of operational evidence in 60 days.

There is a structural reason the evidence window is not merely a best practice but a dependency for the Assessment Certification itself. Phase 1 of the C3PAO assessment begins with a review of the organization's System Security Plan and SPRS score. The SSP is the central document that describes every in-scope system, the controls applied to each, and the evidence that demonstrates those controls are operating. The 90 day evidence window produces the artifacts, the audit logs, the process execution records, the training documentation, that populate the SSP and substantiate the SPRS score. Until those artifacts exist, the SSP cannot be technically complete. An SSP submitted without sustained operational evidence is a description of intent, not a description of a functioning security program. The C3PAO will identify this in Phase 1, before the assessment team ever

arrives on site, and the organization will be directed to complete its evidence before the assessment can proceed.

Remediation has dependencies that resist acceleration. Network segmentation must precede endpoint configuration. Policy development must precede training. Process definition must precede process execution records. Attempting to run these activities in parallel when they have sequential dependencies produces rework and errors that ultimately extend rather than compress the timeline.

Organizations that attempt to compress a twelve month program into six months typically encounter one of several outcomes: they arrive at Assessment Certification without adequate evidence and must delay, they pass the evidence window but discover during the mock audit that controls were implemented hastily and do not function as documented, or they achieve certification but find that the controls cannot be sustained because the implementation was built for speed rather than durability. In each case, the compressed timeline produces higher cost and greater risk than a properly paced program.

Maintaining Momentum

A twelve month compliance program requires sustained leadership attention and organizational commitment.

Regular progress reviews keep the program on track. Monthly reviews with the compliance team should evaluate progress against plan, identify emerging risks, and address

obstacles. Quarterly reviews with executive leadership maintain visibility and reinforce organizational priority.

Communication keeps the organization informed and engaged. Regular updates to affected personnel maintain awareness of program status and upcoming requirements. Communication also surfaces issues that might otherwise remain hidden until they become problems during Assessment Certification.

Executive visibility demonstrates organizational commitment. When leadership visibly engages with the compliance program, attending reviews, participating in training, and allocating resources without delay, it signals that compliance is a genuine priority rather than a delegated burden. The organizations that navigate CMMC most effectively are the ones where executive leadership treats the program as a business priority from the first month through the last.

The twelve month roadmap provides structure for a complex undertaking. Following it while remaining flexible enough to address emerging challenges positions the organization for successful certification. The next chapter examines the expertise required to navigate this process and why internal IT teams, however capable they may be in their domain, cannot do it alone.

Chapter 5: The Expertise Gap

There is a moment in nearly every CMMC compliance program when an executive realizes that technical competence is not enough.

The organization may have talented IT professionals who understand networks, servers, and security tools. They may have implemented sophisticated technical controls. But when they encounter the documentation requirements, evidentiary standards, and assessment methodology of CMMC, technical expertise alone proves insufficient.

This realization often arrives too late. Organizations invest months in remediation activities guided by IT staff who understand technology but not compliance frameworks. They create documentation that satisfies internal stakeholders but fails under outside scrutiny. They implement controls that function operationally but cannot be demonstrated to external assessors. When the C3PAO arrives, they discover that much of their work must be revised or repeated.

The expertise gap in CMMC compliance is not a reflection of the IT team's capabilities. It reflects the fundamental nature of the program. CMMC is roughly 70 percent documentation and process, and only 30 percent technology. Internal IT excels at the 30 percent. The other 70 percent requires a different kind of expertise: understanding of federal compliance frameworks, experience with assessment methodology, knowledge of evidentiary standards, and familiarity with how C3PAOs actually evaluate organizations.

Why Internal IT Is Not Enough

The IT department plays an essential role in CMMC compliance, but several factors limit its effectiveness as the leader of a compliance program.

Perspective limitations affect how IT professionals approach compliance challenges. IT teams are trained to solve technical problems. When presented with a compliance requirement, their instinct is to find a technical solution. But many CMMC requirements are not primarily technical. They require policies, procedures, training programs, and documented evidence of consistent execution. An IT professional tasked with addressing access control requirements may implement excellent technical controls while overlooking the policy documentation, access review procedures, and training records that assessors will expect to see.

Assessment inexperience creates blind spots about what assessors actually examine. IT professionals who have not participated in federal compliance assessments do not know what C3PAOs look for, how they conduct interviews, what evidence they consider sufficient, or how they evaluate documentation. This inexperience leads to preparation that addresses the wrong concerns or inadequately addresses the right ones.

Objectivity challenges arise when internal teams evaluate their own work. IT staff who implemented controls have difficulty assessing those controls critically. They understand what they intended to accomplish but may not recognize the

gaps between their intentions and their actual implementation. They may also face organizational pressure to minimize findings or present an optimistic picture of readiness.

Bandwidth constraints are a practical reality. IT staff have operational responsibilities that do not pause during a compliance program. Networks must be maintained, users must be supported, incidents must be addressed, and projects must be delivered. Adding a twelve month compliance program to an already full operational workload produces one of two outcomes: compliance activities receive inadequate attention, or operational responsibilities suffer. Neither outcome serves the organization.

Documentation expertise is a distinct skill that most IT professionals have not developed. Writing a System Security Plan that accurately describes an environment, maps controls to requirements, and withstands C3PAO scrutiny is not the same as writing a technical configuration document. The documentation required for CMMC must be precise, comprehensive, and aligned with a specific assessment methodology. IT professionals who have never written compliance documentation often produce materials that are technically accurate but structurally inadequate for assessment purposes.

CMMC Is a Whole Business Problem

The expertise gap extends beyond IT into areas of the business that technology teams do not typically manage.

CMMC compliance encompasses physical security, personnel security, facilities management, manufacturing processes, and organizational governance. An IT department is not responsible for who has physical access to the building, how visitors are managed, whether the cleaning crew has been vetted, how technical drawings are handled on the shop floor, or whether CNC machines running controlled specifications are appropriately protected. These are compliance requirements that fall outside the IT domain entirely.

In a typical defense manufacturing environment, the CMMC scope includes door access control systems, camera and surveillance infrastructure, visitor management procedures, CUI handling on the production floor, controlled parts storage, and document destruction processes. An IT team focused on the network, the endpoints, and the cloud tenant sees one dimension of a multidimensional compliance problem. The physical environment, the operational technology, the manufacturing processes, the people, and the documentation all require evaluation and remediation by someone who understands the full scope of what CMMC requires.

This is why the compliance program described in Chapter 4 identifies four remediation tracks, not one. Technology deployment is the IT team's strength. Documentation development, process implementation, and physical security remediation require expertise that spans the organization. The gap between what IT can cover and what CMMC demands is the expertise gap this chapter addresses.

The Tool Versus Program Confusion

One of the most consequential misunderstandings in the defense industrial base is the belief that CMMC compliance can be achieved by purchasing the right software tool.

Vendors in the governance, risk, and compliance space have positioned their platforms as CMMC solutions, implying or in some cases stating directly that purchasing and deploying their product will produce compliance. Organizations that accept this framing invest in technology, configure the platform, and believe they are making progress toward certification. In practice, they are addressing one component of a multifaceted program while the other components, the policies, the procedures, the training, the physical security, the evidence of sustained operation, remain unaddressed.

A GRC platform can be a useful tool for organizing documentation, tracking remediation progress, and managing evidence. It is not a compliance program. The platform does not write the System Security Plan. It does not develop policies that reflect the organization's actual operating environment. It does not train employees on CUI handling procedures. It does not evaluate whether physical security controls meet assessment standards. It does not conduct mock audits or prepare personnel for assessor interviews.

Organizations that have spent months and significant budget on a software tool before engaging qualified compliance expertise often face a difficult realization: the tool addressed the platform but not the program, and much of the work still lies ahead. The distinction matters because every month spent on a tool-first approach is a month not spent on the

governance, documentation, and operational changes that produce actual certification.

The Registered Practitioner and Registered Practitioner Advanced

The CMMC ecosystem includes a credential specifically designed to fill the expertise gap between what organizations can do internally and what Assessment Certification requires.

The Registered Practitioner and Registered Practitioner Advanced are credentials issued through the CyberAB, the accreditation body authorized by the Department of Defense to oversee the CMMC ecosystem. These credentials require demonstrated knowledge of the NIST SP 800-171 security requirements, the CMMC assessment methodology, and the evidentiary standards that C3PAOs apply during formal Assessment Certification. The RPA credential requires additional depth of knowledge in both the Level 2 controls and the assessment procedure itself.

Practitioners credentialed through the CyberAB serve an advisory role. They guide organizations through Discovery, advise during Remediation, develop documentation, build training programs, and conduct mock audits. They bring the compliance framework expertise, assessment methodology knowledge, and outside perspective that internal teams lack. What they do not do is conduct official CMMC assessments, which can only be performed by authorized C3PAOs. They do not implement controls directly or assume operational responsibilities within the organization's environment. And they do not guarantee certification outcomes, which depend

on the organization's actual compliance posture as evaluated by an independent C3PAO.

The advisory boundary described in Chapter 4 bears repeating here because it defines the value of the practitioner relationship. A practitioner who maintains separation between advising and implementing preserves the objectivity required to evaluate the organization's readiness honestly. A practitioner who crosses into implementation compromises that objectivity and diminishes the value of every subsequent evaluation, including the mock audits that the organization depends on for its readiness determination.

What a Qualified Practitioner Provides

The practitioner's contribution spans the entire compliance lifecycle described in Chapter 4.

Think of an RPA as the glue for the entire project. IT handles technology. HR handles training logistics. Facilities handles physical security. Operations handles process execution. But no single department owns the compliance program as a whole, and without someone connecting these efforts into a coherent program, the work happens in silos that do not produce a unified result. The practitioner is the person who ensures that the technology deployment, the documentation, the training, the physical security improvements, and the evidence collection all align with what the C3PAO will evaluate. That connective function is what makes the difference between an organization that has completed a list of tasks and an organization that has built a compliance program.

During Discovery, the practitioner conducts the scoping analysis and gap evaluation that defines the compliance boundary and identifies every gap against the applicable requirements. As discussed in Chapter 3, this includes the physical security walkthrough that internal teams are structurally unable to perform objectively.

During Remediation, the practitioner advises on control implementation, reviews documentation for assessment readiness, works with HR and corporate training to develop the employee training program, and manages the remediation project plan. The practitioner coordinates activities across IT, operations, human resources, and

facilities, functioning as the compliance program's coordinator across departments that do not normally interact on cybersecurity matters.

During the evidence window, the practitioner monitors whether evidence collection is proceeding on schedule, verifies that logging and process execution records meet the standards that assessors will apply, and identifies any gaps in the evidence portfolio before they become findings.

During mock audits, the practitioner, specifically an RPA with training in both the Level 2 controls and the assessment procedure, evaluates the organization using the same methodology a C3PAO will employ. This includes documentation review, technical configuration examination, personnel interviews, and evidence evaluation. The mock audit is where the practitioner's accumulated knowledge of the organization's environment, combined with assessment methodology training, produces the most direct value: an honest, informed prediction of how the organization will perform during formal Assessment Certification.

The Training Mandate

CMMC requires that personnel be trained, and the training program is an area where the practitioner's involvement is most visible to the broader organization.

Security awareness training applies to all personnel and covers the fundamentals of cybersecurity hygiene, threat recognition, and organizational security policies. Commercial training platforms can deliver baseline

awareness content, but the practitioner supplements this with organization-specific material that connects general concepts to the organization's actual practices and environment.

CUI handling training applies to all personnel who access, process, or handle Controlled Unclassified Information. This training covers CUI identification and marking conventions, authorized storage locations and systems, permitted transmission methods, physical handling requirements, and destruction procedures. CUI handling training must be tailored to the organization. Generic training cannot address the organization's specific marking standards, storage systems, transmission rules, or destruction protocols. The practitioner develops this content in coordination with HR and the corporate training function, as described in Chapter 4, to ensure it reflects the actual CUI handling environment.

Role-specific training addresses responsibilities particular to certain positions. Personnel with incident response duties need training on response procedures. Personnel who administer access controls need training on access management procedures. Personnel who monitor security events need training on monitoring tools and escalation protocols.

Interview preparation is a specialized form of training that prepares personnel for C3PAO assessment interviews. Assessors interview personnel across multiple organizational roles to verify that documented policies and procedures reflect actual practice. Personnel who cannot articulate their responsibilities or who provide inconsistent answers create doubt about compliance validity. The practitioner conducts

practice interviews that simulate assessment conditions, helping personnel become comfortable with the experience and identifying individuals who may need additional preparation before Assessment Certification.

Selecting a Practitioner

Not all practitioners offer equivalent value. The credential establishes baseline qualification, but experience, expertise, and approach vary significantly.

When evaluating a practitioner, consider several factors. How many organizations has the practitioner guided through the CMMC compliance process? Experience with organizations similar in size, industry, and complexity to yours is more relevant than total engagement count. Does the practitioner have experience in defense manufacturing environments where physical security, operational technology, and shop floor CUI handling are part of the compliance scope? Does the practitioner arrive with a project template and structured engagement methodology, or are they inventing the approach as they go?

Verify credentials through the CyberAB marketplace, which confirms active credential status. Ask for references from organizations the practitioner has supported and speak with those references about the practitioner's communication style, responsiveness, depth of knowledge, and the outcomes their organizations achieved.

Be cautious of practitioners who promise specific outcomes, guarantee certification, or position themselves as able to do it all. A qualified practitioner is direct about what they can and cannot control. They can improve the organization's readiness substantially. They cannot control the C3PAO's independent evaluation. Be equally cautious of technology vendors or managed service providers who present their

products as CMMC solutions and offer practitioner services as an add-on to a software sale. The compliance program should drive tool selection, not the other way around.

Engaging a qualified practitioner early in the compliance process improves outcomes, reduces cost, and increases the likelihood of successful certification. The investment in expertise pays for itself through avoided rework, accurate scoping that controls the compliance boundary, and preparation that produces genuine readiness rather than optimistic assumptions. In the next chapter, we examine the physical security blind spots that catch many organizations by surprise and that represent one of the clearest examples of why the expertise gap exists.

Chapter 6: Blind Spots

Most executives understand the technology requirements of CMMC. They know they need firewalls, encryption, and multi-factor authentication. They have budgeted for security software and engaged expertise to close the technical gaps.

But when asked about their cleaning crew's background checks, what happens to the paper in their recycling bins, or who has unescorted access to the building after hours, the conversation typically stops.

This is the category of CMMC compliance that derails otherwise well-prepared organizations: physical security controls that live outside the IT department's jurisdiction. These are not theoretical risks buried in an obscure appendix of NIST 800-171. They are practical, everyday vulnerabilities that assessors will examine during Assessment Certification. Organizations that have spent months configuring access controls and documenting incident response procedures can fail on a janitor with unrestricted building access or a recycling bin full of technical drawings.

CMMC assessors know this. They have seen it repeatedly. They will look for it.

The Cleaning Crew

The most common physical security blind spot in defense contractor facilities is the janitorial service.

Consider the typical arrangement. A cleaning crew of three or four people from a local service company has master key access to the entire facility five nights a week. They work unsupervised from 7 PM to midnight, long after the last employee has left. The service agreement contains no requirements for background checks, no training on CUI handling protocols, and no acknowledgment that the crew is working in a controlled environment.

This is NIST 800-171 controls PE-2 and PE-3 in practice. Physical Access Authorizations and Physical Access Control do not distinguish between engineers and cleaning staff when it comes to access to areas where CUI is processed, stored, or transmitted. Any individual with unescorted access to CUI areas must be authorized, and that authorization requires a basis for granting it.

The implications for external cleaning companies are significant. Any cleaning company employee who will have unescorted access to CUI areas must receive the same CUI awareness training that the contractor's own employees receive. They must undergo the same background screening. They must sign the same nondisclosure acknowledgments. And the cleaning company must guarantee that no substitute employee, no untrained or unscreened person filling in for an absent crew member, will set foot on a CUI floor. That last requirement is the one that makes external cleaning arrangements impractical for most defense contractors. Cleaning companies operate on thin margins with high turnover, and guaranteeing that every person who enters the facility on every shift has been screened, trained, and documented to the same standard as the contractor's own

workforce is a commitment most janitorial service providers are neither equipped nor willing to make.

This is why most contractors handling CUI at Level 2 ultimately hire an internal employee to clean CUI areas. An internal cleaning person is subject to the same onboarding process, the same background screening, the same CUI training, and the same organizational accountability as every other employee. There is no substitution risk. There is no question about whether the person on the floor tonight is the same person who was trained last month. The organization controls the hiring, the training, the scheduling, and the access. An external cleaning company can still handle common areas, lobbies, restrooms, and non-CUI spaces. But CUI floors should be cleaned by someone the organization employs directly.

The cost of adding an internal cleaning position is modest relative to the compliance risk it eliminates. Compared to the potential loss of contracts worth millions of dollars or the False Claims Act exposure described in Chapter 1, it is one of the most straightforward investment decisions in the entire compliance program.

The cleaning crew example is detailed here to give the reader an idea of how something that appears simple in CMMC can become complicated quickly. Who cleans the building is not a question most executives have ever considered a compliance matter. Under CMMC, it requires analysis of access controls, training requirements, background screening, substitution risk, contractual obligations, and ultimately a staffing decision. This pattern repeats throughout the program. The physical security requirements

that follow in this chapter each carry similar layers of complexity beneath what initially appears to be a straightforward question.

Third Party Maintenance: No Escort, No Entry

The cleaning crew represents the most common blind spot, but janitorial services are not the only external personnel who access the facility.

Consider the full range of third parties who may enter the building in a typical month: HVAC technicians servicing heating and cooling equipment, vending machine servicers restocking machines, copier and printer maintenance personnel, electricians and plumbers, fire suppression and alarm system technicians, elevator maintenance personnel, telecommunications technicians, and pest control services. Each of these individuals potentially has access to areas where CUI is processed or stored. Each represents a physical security consideration under CMMC.

The governing principle is straightforward. No unescorted access to CUI areas for any individual who has not been properly authorized. This does not mean every vendor who enters the building requires a background check and CUI training. It means the organization must control where they go and ensure they cannot access CUI during their visit.

Designate specific personnel as authorized escorts for third party visitors. These escorts must maintain visual contact with visitors, ensure visitors access only authorized areas, and prevent any interaction with CUI or CUI systems. Establish visitor management procedures that document who enters, when they arrive, the purpose of the visit, who escorted them, and when they departed. This log becomes evidence of the physical access control program.

Where possible, configure the facility to enable escorted access to necessary areas without traversing CUI zones. If the HVAC equipment is in a mechanical room accessible without passing through engineering spaces, the escort requirement becomes simpler to implement. If the vending machine is located inside a CUI area, consider relocating it. These are not expensive changes, but they require someone to think about physical access paths with a compliance perspective, which is precisely the kind of analysis that Chapter 5 describes as part of the practitioner's contribution.

The Trash Can Test

Media sanitization is one of the most commonly failed controls in CMMC assessments, and the failure almost always involves paper rather than digital media.

This is NIST 800-171 control MP-6. The requirement is that CUI must be destroyed in a manner that makes it unreadable and unrecoverable. The implementation is where most organizations stumble.

The typical failure pattern is predictable. The organization has shredders. Employees have been told that CUI needs to be shredded. Signs have been posted. Emails have been sent. But a walkthrough of the facility reveals mixed-use recycling bins next to every desk, unlocked dumpsters in the parking lot, and a general paper box near the copier full of marked-up technical drawings.

During Assessment Certification, the assessor will conduct what amounts to a trash can test. They will walk through the

facility and look in waste receptacles. They will check the dumpster. They will ask employees what they do with sensitive papers. If they find a single piece of CUI in a standard trash bin or recycling container, the control is failed.

The solution requires both infrastructure and culture change. Separate, clearly marked receptacles for CUI destruction versus general waste are the starting point. The most effective approach is to eliminate general paper bins from CUI areas entirely. Every piece of paper generated in a CUI environment should be treated as potentially sensitive until proven otherwise. This means lockable destruction consoles, secure bins that cannot be accessed without a key, stationed in strategic locations throughout the facility.

Standard office shredders typically produce strip-cut results, which can be reconstructed. For CUI, cross-cut or micro-cut shredding is required to render documents truly unrecoverable. Many organizations use certified destruction services that provide certificates of destruction and chain-of-custody documentation, which also serve as evidence during Assessment Certification.

If the organization uses a destruction service that picks up locked bins, someone must be designated as the qualified sorter. This person verifies that only appropriate materials go into the destruction bins before they are locked and scheduled for pickup. Once the bin leaves the facility, the organization loses control of the chain of custody. If an employee accidentally places personal documents or unrelated company records in with the CUI, they cannot be retrieved. The qualified sorter, typically an administrative

staff member trained on CUI identification, performs a visual inspection before bins are sealed.

External waste containers must be locked and located in an area that is either under surveillance or inaccessible to the public. Dumpster access is a documented intelligence gathering technique, and an unlocked dumpster containing technical drawings is a compliance failure regardless of whether anyone actually accesses it.

The culture component is where executive leadership matters most. Technology and procedures only work if people follow them. When leadership talks about media sanitization in organizational meetings, when the CEO picks up a piece of paper on the floor and walks it to the destruction console, it becomes part of the organizational culture rather than a rule that people ignore when nobody is watching. One aerospace components manufacturer failed a mock audit because the practitioner found three pieces of CUI-marked documentation in general waste bins: a supplier email about specifications, a redlined drawing, and a meeting agenda listing contract names and values. The organization had spent $140,000 on IT infrastructure. A $3 recycling bin nearly derailed the entire certification.

Printers, Whiteboards, and Monitors

Several other physical security areas catch organizations off guard during Assessment Certification.

Multifunction printers and copiers store documents in internal memory. Print jobs may sit in output trays for

extended periods where anyone walking by can read them. The solution is secure print release, which requires authentication at the device before the document prints. The person who sent the job must be standing at the machine and authenticate before output is produced. This is a standard feature on most enterprise printers and costs nothing additional to enable, but it must be configured and enforced.

Information on whiteboards or displayed on monitors is visible to anyone with a line of sight. A technical drawing on a whiteboard in an engineering bay, a spreadsheet open on a monitor near a window, a specification displayed during a production meeting where visitors are present: all of these represent potential CUI exposure. Clean board policies require that whiteboards in CUI areas be erased when not actively in use. Monitor positioning should prevent viewing from outside controlled areas, and privacy screens should be used where repositioning is not practical.

Laptops, tablets, phones, and USB drives can physically transport CUI outside the controlled environment. Policies governing which devices may contain CUI, combined with encryption requirements for any that do, are required at Level 2. Policy alone is not sufficient. Enforcement, monitoring, and regular reinforcement through the training program described in Chapter 5 are what make the policy effective in practice.

After-Hours Building Access

Physical access controls must align with CUI authorization.

Not every employee who has badge access to the building should have after-hours access to CUI areas. If the enclave described in Chapter 2 is physically separated, access control to that space should reflect the authorization list for CUI access, not the general building access list. Employees who do not handle CUI have no reason to access CUI areas outside normal business hours, and their access should be restricted accordingly.

Review building access logs periodically to verify that after-hours access patterns are consistent with authorized personnel. Unexplained access by unauthorized individuals, or unusual access patterns by authorized personnel, should be investigated. These logs also become evidence of the organization's physical access monitoring program during Assessment Certification.

The Pattern Behind the Blind Spots

What makes these physical security controls so easy to overlook is a pattern shared across all of them.

First, they are administratively owned, not IT owned. The IT director is not responsible for janitorial contracts, waste management, or building access systems. These fall under facilities, HR, or operations. In organizations where CMMC compliance has been delegated to IT, these areas receive no attention because they are outside IT's scope of authority.

Second, they are contextually invisible to executives. Leadership is not in the building when the cleaning crew arrives. They are not watching what employees do with printed documents at the end of the day. They do not observe who walks through which doors or whether the visitor log is being maintained.

Third, they require the cross-functional coordination described throughout this book. Addressing the cleaning crew requires coordination between facilities management, the janitorial service provider, and the compliance program. Addressing media sanitization requires coordination between facilities, procurement, and every department that handles CUI. Addressing third party access requires coordination between facilities, reception, and every department that schedules vendor visits.

This is precisely the pattern that Chapter 5 identifies as the expertise gap. Internal teams do not see these issues because they live inside the environment every day. An outside practitioner walking the facility for the first time will identify

physical security gaps in the first hour that internal staff have not noticed in years. The rock holding the side door open, the recycling bin next to the printer, the visitor log that has not been reviewed in months: these findings are the reason Discovery includes a physical security walkthrough and the reason that walkthrough should not be conducted by internal personnel alone.

In the next chapter, we examine the mock audit process in detail, where every blind spot described here, along with every technical and documentation requirement covered in the preceding chapters, faces its first real test under conditions that simulate the formal Assessment Certification.

Chapter 7: The Dress Rehearsal

The organization has spent months preparing for CMMC certification. Technology is implemented, documentation is complete, the evidence window has accumulated 90 days of logs and records, and personnel have been trained.

The question is whether all of that work actually holds up under scrutiny. Believing the organization is ready and being able to demonstrate readiness to an independent evaluator are two different things. The difference matters substantially when the formal Assessment Certification carries a cost of $60,000 or more and a failed result means the investment does not produce certification until deficiencies are remediated and reassessment is scheduled.

This is the purpose of the mock audit. It is the dress rehearsal before the performance. The organization runs through the entire Assessment Certification experience under realistic conditions, with an outside evaluator applying the same methodology a C3PAO will use. Problems found during the dress rehearsal can be corrected. Problems found during the formal Assessment Certification become findings that delay certification, increase cost, and put contracts at risk.

What the Mock Audit Reveals

The mock audit serves multiple purposes beyond identifying individual compliance gaps.

The most valuable function is finding the say-do gap. Organizations frequently have documented policies and procedures that do not reflect actual practice. The policy says access reviews occur quarterly, but the last review was eight months ago. The procedure says incidents are reported within 24 hours, but no one can describe how to report an incident. The plan says backups are tested monthly, but testing records do not exist. This gap between what the organization says it does and what it actually does is the most common source of Assessment Certification findings. An experienced mock auditor will probe for the say-do gap at every opportunity, because the C3PAO assessor will do exactly the same.

Evidence completeness is the second major function. The organization may have implemented controls correctly, but the question is whether it can prove it. The mock audit evaluates whether the evidence portfolio is complete, organized, and sufficient to satisfy an assessor. Missing logs, incomplete records, and disorganized documentation all create problems during formal Assessment Certification. It is far better to discover these gaps during the dress rehearsal.

Personnel readiness is the third function. Many employees have never experienced a compliance assessment. They do not know what to expect, how to respond to questions, or how their answers affect certification outcomes. The mock audit gives personnel realistic interview experience, reducing anxiety and improving performance during the formal evaluation.

Readiness validation is the ultimate function. The mock audit provides the objective information required for the

most important decision in the compliance program: is the organization ready to proceed with formal Assessment Certification, or should it delay to address what was found?

Who Conducts the Mock Audit

As discussed in Chapter 4, mock audits should be conducted by a Registered Practitioner Advanced who is trained and credentialed on the Level 2 controls and the assessment procedure.

The RPA credential requires demonstrated knowledge of both the 110 NIST SP 800-171 security requirements and the methodology that C3PAO assessors apply during formal evaluation. That combination is what makes the mock audit predictive rather than merely observational. A general cybersecurity consultant may identify technical gaps, but without knowledge of how assessors evaluate evidence, conduct interviews, and apply the assessment methodology, the mock audit will not replicate the actual Assessment Certification experience.

The advisory boundary established in Chapter 4 applies directly here. The practitioner who conducts the mock audit should not have been directly implementing controls or performing hands-on remediation in the environment. If the same person built the controls and then evaluates them, the mock audit loses its independence. The value of the exercise depends entirely on the evaluator's willingness and ability to identify problems honestly, including problems with work that the organization's team performed based on the practitioner's own advice. Maintaining the separation between advising and implementing is what preserves that objectivity.

Multiple Iterations

Chapter 4 established that the organization should plan for more than one mock audit, and the reasoning is worth examining in detail here.

The first mock audit, conducted early in month ten of the timeline described in Chapter 4, establishes the current state of readiness. It identifies gaps in documentation, weaknesses in controls, evidence that is missing or insufficient, and personnel who are not prepared for assessor interviews. The findings from the first mock audit drive a focused remediation effort.

The second mock audit, conducted after those findings are addressed, verifies that the remediation was effective. It confirms that documentation gaps were closed, that control weaknesses were corrected, that evidence was collected and organized, and that personnel who struggled in the first round are now prepared. Without this second iteration, the organization proceeds to formal Assessment Certification hoping that its corrections resolved the issues. With it, the organization proceeds knowing they did.

The cost of two mock audits is a fraction of the cost of a failed Assessment Certification followed by remediation and reassessment. The additional investment in verification is one of the most cost effective decisions in the entire compliance program.

Mock Audit Scope and Methodology

A thorough mock audit covers every dimension that the formal Assessment Certification will examine.

Documentation review evaluates the System Security Plan, policies, procedures, and the Plan of Action and Milestones for completeness, accuracy, and alignment with the actual operating environment. The evaluator verifies that the SSP describes every in-scope system, that policies address each of the 14 security domains, that procedures are specific enough to be followed, and that the POA&M accurately reflects any requirements not yet fully implemented.

Technical verification examines whether implemented controls function as documented. This includes reviewing configurations, testing access controls, verifying encryption, examining logging and monitoring systems, and confirming that network segmentation is effective. The evaluator is looking for gaps between what the documentation describes and what the systems actually do.

Evidence examination evaluates the completeness and quality of the evidence portfolio. Are audit logs present for the required period? Do process execution records demonstrate consistent operation? Are training records complete? Can the organization produce evidence for each requirement in a timely manner, or does locating evidence require extended searching? The organization of the evidence matters as much as its existence. Assessors have limited time, and evidence that cannot be produced efficiently creates doubt about the program's maturity.

Personnel interviews are conducted across multiple organizational roles to verify that documented policies and procedures reflect actual practice. The evaluator asks employees to describe their responsibilities, explain how processes work, and demonstrate that they understand the security requirements relevant to their roles. The interview process is where the say-do gap is most clearly exposed.

Physical security evaluation covers every blind spot described in Chapter 6: access controls, visitor management, media sanitization, printer security, monitor visibility, and all the operational elements that exist outside the IT department's domain. The evaluator walks the facility with the same eye that a C3PAO assessor will bring.

Interview Preparation

The interview component of the mock audit doubles as a training exercise for personnel who will face C3PAO assessor interviews during the formal Assessment Certification.

Several principles govern effective interview performance. Personnel should answer the question that was asked and only the question that was asked. Volunteering information beyond what the assessor requested opens lines of inquiry that may not serve the organization's interests. If the assessor asks how often access reviews occur, the answer is the frequency. It is not the frequency plus a detailed explanation of a time the review was late plus a description of the remediation that followed.

Personnel should never guess. If they do not know the answer, they should say so and offer to connect the assessor with the person who does. An honest acknowledgment of uncertainty is always preferable to an incorrect answer. Assessors are trained to follow inconsistencies, and an inaccurate answer creates more problems than an incomplete one.

Personnel should understand that it is acceptable to defer. Not every person in the organization is expected to know the answer to every question. An assessor asking a system administrator about the incident response plan is testing whether the administrator knows the plan exists and understands their role in it, not whether the administrator can recite every section. If the question goes beyond the person's role, deferring to the appropriate colleague demonstrates organizational awareness rather than weakness.

The mock audit provides the opportunity to practice these principles under realistic conditions. The evaluator conducts interviews using the same approach and questions that C3PAO assessors employ, then debriefs each participant on what went well and what needs improvement. Personnel who demonstrate uncertainty or provide problematic responses receive additional preparation before the formal Assessment Certification.

The Mock Audit Report

The mock audit report is an action document, not a narrative summary.

The executive summary provides a high level readiness determination and identifies the most significant concerns requiring attention. This section enables executive decision making without requiring detailed technical review.

The findings section documents specific gaps, deficiencies, or concerns identified during the evaluation. Each finding identifies the relevant control, describes the issue, explains why it matters for Assessment Certification, and provides a recommendation for remediation. Findings should be prioritized so the organization knows which require immediate attention and which can be addressed in sequence.

The observations section covers items that are not formal findings but warrant attention. Controls that are implemented but where the evidence could be stronger. Personnel who demonstrated some uncertainty that additional preparation could address. Documentation that is technically complete but could be improved. These are items that may not fail the organization individually but could contribute to a finding if left unaddressed.

The evidence evaluation assesses the completeness and quality of the evidence portfolio as a whole, identifying gaps, organizational issues, and documentation that may not survive the scrutiny of a formal assessor.

The personnel readiness section summarizes how individuals performed in interviews and identifies anyone or any topic area that needs additional preparation.

The recommendation section provides the evaluator's honest professional judgment on whether the organization is ready to proceed with formal Assessment Certification. This recommendation must be frank. If significant gaps exist, the report should say so plainly regardless of organizational pressure to stay on schedule. That frankness is the entire reason the mock audit is conducted by an outside practitioner rather than by internal staff.

The Go or No-Go Decision

With the mock audit report in hand, executive leadership faces the most important decision in the compliance program: proceed with formal Assessment Certification or delay to address what was found.

If findings are limited to minor documentation gaps, evidence organization issues, or personnel preparation concerns that can be resolved before the scheduled date, proceeding is appropriate. These are the kinds of items that the second mock audit is designed to verify.

If findings reveal significant control gaps, systematic documentation failures, or evidence that is insufficient and cannot be meaningfully addressed within the available time, delay is the correct decision regardless of schedule pressure. A failed Assessment Certification does not produce a partial result. It produces a list of findings, a requirement to remediate, and the need to schedule and pay for a reassessment. The total cost of failure, including the wasted assessment fee, the remediation effort, and the reassessment

cost, almost always exceeds the cost of delaying for adequate preparation.

If findings fall somewhere between minor and significant, the decision requires judgment. Weigh the severity of what was found against the remediation timeline, the cost of a failed Assessment Certification, and the consequences of delay. The practitioner who conducted the mock audit has seen this pattern across multiple organizations and can provide an informed perspective on where the real risk lies.

Do not allow organizational momentum or sunk-cost reasoning to drive the organization into a premature Assessment Certification. The investment already made is not a reason to add a failed certification fee to it. The goal is to achieve certification, not merely to attempt it.

From Rehearsal to Performance

The mock audit marks the transition from preparation to execution.

The organization has built the compliance program, implemented the controls, accumulated the evidence, and validated readiness through independent evaluation. What remains is the formal Assessment Certification itself.

Use the time between the final mock audit and the formal Assessment Certification to address every finding and observation in the report. Conduct additional interview preparation with anyone who showed uncertainty. Review and organize the evidence portfolio one final time. Verify that all logistics are arranged: facilities for the assessor team,

access to systems and documentation, availability of personnel who will participate in interviews, and clarity on roles for every participant.

Approach the formal Assessment Certification with confidence grounded in preparation. The work has been done. The mock audits verified that it holds up. The team understands their responsibilities. The evidence demonstrates compliance. In the next chapter, we examine the formal Assessment Certification from the executive perspective: the role of leadership in setting the right tone, what the assessment week actually looks like, and how to handle whatever the outbrief brings.

Chapter 8: Assessment Day

The C3PAO assessment team arrives on Monday morning.

After twelve months of preparation, substantial investment, and sustained effort across the organization, the moment has arrived. The next three to five days will determine whether that investment produces the certification the organization needs to compete for Department of Defense contracts.

For many executives, this moment brings anxiety. The outcome matters enormously to the business, yet the process itself is largely outside executive control. The assessors will examine systems, review documentation, and interview personnel. The executive cannot take the test for the organization. The executive can only observe as the team demonstrates what they have learned and the systems prove what they can do.

This chapter addresses the executive role during formal Assessment Certification. Executive presence and conduct matter more than most leaders expect. How leadership sets the tone, how it interacts with assessors, and how it handles whatever emerges all influence the assessment experience and its outcomes.

Tone at the Top: The Opening Meeting

The Assessment Certification begins with an opening meeting where the C3PAO lead assessor introduces the assessment team, reviews scope and

methodology, confirms logistics, and addresses preliminary questions.

Executive participation in this meeting is expected and important. The CEO's presence signals organizational commitment to the assessment process. It demonstrates that CMMC compliance is a business priority, not merely an IT initiative. Assessors notice when executives engage personally with the compliance program. That engagement suggests a mature security culture that takes its obligations seriously.

Welcome the assessment team and express genuine appreciation for their role. They are not adversaries. They are professionals conducting an evaluation that, if successful, validates the organization's security posture and enables continued participation in the defense industrial base. Affirm the organization's commitment to cybersecurity and to honest assessment. Make clear that the organization wants the assessors to see it accurately, including any areas that need improvement. This posture of transparency builds credibility and reduces any perception that the organization might be concealing problems. Confirm that organizational resources are available to support the assessment and that any barriers to access should be reported immediately so they can be resolved.

There are several things to avoid during the opening meeting. Do not attempt to influence assessment outcomes through personal appeals or by emphasizing the business consequences of findings. Do not overstate the organization's capabilities or readiness. Do not make preemptive excuses for areas where the organization may be

weak. Assessors are trained to evaluate what they find, and attempts to frame the narrative before the evaluation begins rarely achieve their intended effect.

What the Assessment Week Looks Like

The formal Assessment Certification typically spans three to five days for a mid-sized organization, though duration varies based on scope and complexity.

The assessment team will conduct several parallel activities throughout the week. Documentation review examines the System Security Plan, policies, procedures, the Plan of Action and Milestones, and supporting documentation against the 110 requirements. The assessors are evaluating whether documentation is complete, accurate, and reflective of the actual operating environment.

Technical examination involves direct observation and testing of implemented controls. Assessors will review system configurations, test access controls, verify encryption, examine logging and monitoring infrastructure, and confirm that network segmentation functions as documented. They may request live demonstrations of specific capabilities.

Evidence review evaluates the evidence portfolio that the organization has accumulated during the evidence window described in Chapter 4. Assessors will request specific evidence for each requirement and evaluate whether it demonstrates sustained operation of the controls, not merely implementation at a point in time.

Personnel interviews are conducted across multiple organizational roles. Assessors will interview system administrators, security personnel, management, and end users. The interviews verify that documented policies and

procedures reflect actual practice and that personnel understand their security responsibilities.

Physical observation occurs throughout the assessment. Assessors will walk the facility, observe physical access controls, examine media sanitization practices, and evaluate the physical security measures described in Chapter 6. The trash can test, the visitor log, the door access system, the printer output tray: all of it is subject to observation.

The Staff Speak Principle

The most important thing an executive can understand about Assessment Certification interviews is that the assessors want to hear from the organization's staff, not from consultants or leadership.

When an assessor asks a system administrator how access reviews are conducted, the assessor wants the system administrator to describe the process in their own words. When an assessor asks an engineer what happens when CUI needs to be destroyed, the assessor wants the engineer to explain the procedure as they understand and practice it. The assessor is not testing whether the organization has someone who can recite the correct answer. The assessor is testing whether the people who actually perform the work understand what they are doing and why.

This is why the interview preparation described in Chapter 7 matters so much. Personnel who have practiced answering questions under realistic conditions will perform substantially better than personnel encountering the

assessment experience for the first time. The mock audit provides that practice. The formal Assessment Certification is not the place to discover that a key employee cannot articulate the incident response procedure or that a department head does not know what CUI stands for.

Executives should not intervene during staff interviews. If an employee pauses or provides an incomplete answer, allow the assessor to follow up. Assessors are skilled at drawing out information through follow-up questions, and a natural exchange between the assessor and the employee is far more credible than a polished answer prompted by executive intervention.

The Practitioner's Role on Assessment Day

The practitioner who has guided the organization through Discovery, Remediation, and the mock audit process has a specific and limited role during the formal Assessment Certification.

During the assessment, the practitioner serves as an advisor sitting at the elbow of the organization's staff, not as a participant in the assessment itself. The practitioner may help locate evidence when staff cannot immediately find what the assessor has requested. The practitioner may clarify terminology if an assessor uses language that staff do not recognize. These supporting functions are appropriate and expected.

What is not appropriate is the practitioner answering substantive questions about the organization's controls, practices, or compliance status. Those answers must come

from the organization's personnel. A practitioner who tries to manage the assessment, who fills silence during interviews, or who corrects incomplete answers from staff creates a negative impression. Assessors interpret consultant intervention as a signal that the organization's personnel do not understand the program, which undermines exactly the demonstration of organizational competence that the assessment is designed to evaluate.

Brief the practitioner on their assessment role before the C3PAO arrives. Ensure they understand the boundaries and will maintain them throughout the week. The practitioner's instinct to help, particularly after months of close work with the organization, must be tempered by the reality that the assessment belongs to the organization and its people.

The practitioner plays a more active role in debriefs at the end of each assessment day. They can help leadership understand what occurred, interpret assessor questions and reactions, and identify areas that may need attention on subsequent days. If certain interview topics revealed weakness, additional preparation that evening may help. If evidence requests suggested assessor concerns, ensuring relevant documentation is readily accessible the next day demonstrates responsiveness. This interpretation and preparation function is where the practitioner's value is highest during assessment week.

Executive Presence Throughout the Week

The executive's role after the opening meeting is less defined but still important.

Be visibly present during the assessment week, available if needed and clearly engaged with the process. This does not mean hovering over assessors or sitting in every interview. It means being in the office, checking in periodically with the assessment coordinator, and demonstrating that the assessment has executive attention. Visible presence reinforces the tone set in the opening meeting and provides reassurance to staff that leadership stands behind them during a demanding week.

Resist the urge to intervene. There will be moments that trigger the instinct to step in: an employee struggling with a question, an assessor pursuing a line of inquiry that feels unfair, a conversation heading in a direction that causes concern. Let the staff handle questions, even difficult ones. Let assessors pursue their methodology, even when the focus seems misdirected. Trust the preparation that has been done and the team that has been built. If something genuinely requires executive attention, the assessment coordinator or practitioner will bring it forward.

Take care of the team practically. Assessment week is stressful for the people being interviewed and supporting technical examinations. Ensure meals are available for staff working through lunch. Provide flexibility for breaks. Express appreciation for the effort regardless of how specific interactions went. After difficult interview sessions, resist the temptation to critique or second-guess performance. There will be time for lessons learned once the week is over. During the assessment, the team needs confidence and support.

The Closing Meeting and Outbrief

The Assessment Certification concludes with a closing meeting where the lead assessor presents preliminary findings.

This outbrief is the first indication of outcomes, though the final determination comes after the C3PAO completes its internal review. The lead assessor will summarize the week's activities and present any findings identified during the evaluation. Findings are categorized by severity and type. Some may require remediation before certification can be issued. Others may be addressable through the Plan of Action and Milestones process.

Preliminary findings are exactly that: preliminary. The assessment team may revise findings after completing their documentation and review. Findings presented in the outbrief may be removed if additional evidence surfaces during the review. New findings may emerge if issues are identified that were not discussed on site. The outbrief provides direction, not a final determination.

Receive findings professionally and without defensiveness. Even where disagreement exists, the outbrief is not the time for extended debate. Thank the assessor for the information, ask clarifying questions where genuinely needed, and note any evidence that might address a concern. The organization will have the opportunity to respond formally through the assessment process. Calm, evidence-supported responses are far more effective than emotional arguments during the outbrief.

If the assessment identifies findings that require remediation, the POA&M process provides a structured path.

The organization documents each finding, develops a remediation plan with specific milestones and target dates, and executes the remediation within the timeframe established by the assessment. The POA&M is not a penalty. It is a mechanism that allows certification to proceed while identified items are corrected under documented accountability.

If the assessment identifies no findings, express appreciation and confirm next steps for receiving formal certification. Clean assessments happen, particularly for well-prepared organizations that invested in thorough mock audits and took the readiness process seriously.

After the Assessment

The formal Assessment Certification concludes, but the path to certification does not end when the assessors leave the building.

What many organizations do not anticipate is the review process that follows the on-site assessment. After the assessment team departs, the lead assessor conducts a quality review of the assessment package, reconciling findings, verifying evidence references, and ensuring the assessment documentation meets C3PAO internal standards. This review can result in adjustments to findings, including findings being added or removed based on the lead assessor's evaluation of the complete record. The organization has limited visibility into this process while it is underway.

Once the C3PAO's internal review is complete, the assessment results are submitted into the Enterprise Mission Assurance Support Service, known as eMASS, which is the Department of Defense's system of record for cybersecurity authorization and assessment data. The Department of Defense then conducts its own review of the submitted assessment. This review evaluates whether the C3PAO's assessment was conducted properly and whether the results support the certification determination. The timeline for these post-assessment reviews varies, and the organization should plan for a period of weeks to months between the on-site assessment and the final certification determination. During this period, the organization should continue operating its security program as documented, because certification has not yet been granted and the

representations made in the SPRS score and SSP remain in effect.

The practical consequence for executive planning is that the Assessment Certification on-site week is not the finish line. It is the last major milestone before a review process that the organization cannot accelerate. Certification is valid for three years from the date it is issued, and the three year maintenance perspective described in Chapter 3 applies immediately upon receiving it.

Conduct a lessons learned review within two weeks of the assessment conclusion, while observations are still fresh. What went well? Where did the organization struggle? Which interviews were strong and which revealed gaps in personnel understanding? What evidence was difficult to locate? Were there findings that could have been prevented with better preparation? The lessons learned inform the ongoing compliance maintenance program and improve preparation for the eventual recertification.

Recognize the team. CMMC certification represents a sustained organizational achievement. The IT staff who implemented controls, the operations personnel who changed processes, the administrative staff who maintained evidence, the employees who completed training and performed well in interviews: every one of them contributed to the outcome. Recognition reinforces the compliance culture that produced certification and sustains it through the three year maintenance period.

The work described throughout this book, from the enforcement context in Chapter 1 through the data

categories, cost planning, timeline, expertise, physical security, mock audits, and this assessment week, was never about the assessment itself. The assessment is a measurement. The work was building an organization capable of protecting the information entrusted to it by the Department of Defense. That capability, demonstrated and verified, is what the certification represents.

In the next chapter, we examine a specific compliance risk that many organizations carry without realizing it: the accuracy of the SPRS score they have already submitted and the consequences of discovering it is wrong.

Chapter 9: Your SPRS Score

> *Disclaimer: This chapter is provided for informational purposes only and does not constitute legal advice. The author is a CMMC Registered Practitioner Advanced, not an attorney. Nothing in this chapter should be construed as legal counsel or guidance on any specific legal matter. If the issues described here are relevant to your organization, consult a qualified attorney who understands both the False Claims Act and CMMC compliance before taking any action.*

Every industry has its elephant in the room. In the defense industrial base, it is the SPRS score.

Everyone involved knows the problem exists. The IT managers know their organization's reported score does not match the technical reality. The consultants who walk into new engagements and run their first gap analysis know it within days. The Department of Defense knows it, which is precisely why CMMC replaced self-attestation with third party verification. The problem has been standing in the middle of the room for years, and the collective response has been to work around it, avoid eye contact with it, and hope that nobody forces the conversation.

CMMC is about to force the conversation.

In many cases, the SPRS score is wrong. Not slightly wrong. Not off by a few points due to a difference in interpretation. Wrong by 50, 75, sometimes 100 points or more from the actual security posture of the organization. A company

reports a score of 90 to the Department of Defense, wins contracts based on that representation, and the technical reality of its environment is a negative 10. That is not a rounding error. That is not a matter of interpretation. It is a chasm between what was represented to the federal government and what actually exists. Every day that score sits in a federal database attached to an active contract, the legal exposure grows.

What SPRS Is and Why It Matters

The Supplier Performance Risk System is a Department of Defense managed database where defense contractors submit a self-assessed score reflecting their implementation of the 110 security requirements in NIST SP 800-171.

That score, which ranges from 110 for full implementation down to negative 203 for nothing implemented, is directly tied to the organization's eligibility for defense contracts. The Department of Defense uses it to evaluate cybersecurity posture before awarding work.

Under CMMC, the SPRS score and the System Security Plan behind it become the baseline that everything else is measured against. When a C3PAO begins a formal Assessment Certification, it starts by reviewing the SSP and the SPRS score. The assessment team will compare what the score claims against what the systems actually do. That comparison has legal consequences that are described throughout this chapter.

How Scores Get This Wrong

Some of the inflation is intentional. A significant amount of it is not.

Much of the inaccuracy comes from organizations that used an internal checklist, relied on an underqualified consultant, or simply did not understand what NIST SP 800-171 was actually requiring. They reviewed 110 requirements, checked the ones they believed applied, gave themselves credit for controls that were partially implemented or planned but never executed, and arrived at a number that appeared reasonable. Some were told by their IT provider that they were compliant. Some used a template found online. Some estimated based on assumptions rather than evidence.

The result is the same regardless of intent. Scores that are off by 50, 75, sometimes 100 points or more from reality. And every one of those scores is a representation to the federal government that specific security controls are in place when they are not.

The False Claims Act Standard

Chapter 1 described the False Claims Act framework and its application to cybersecurity misrepresentations. That framework applies directly to inaccurate SPRS scores.

The False Claims Act does not require proof of intent to defraud. It requires only that the organization knew, or should have known, that its representation was false. An executive who signed off on a compliance attestation without verifying the technical accuracy of the underlying work can be found to have known that the representation was

inaccurate. An organization that reported a 90 when the reality was a negative 10 will not be treated as having made a reasonable mistake. The gap is too large for any court to accept ignorance as a credible defense.

The per-claim penalties described in Chapter 1, currently $14,308 to $28,619 per false claim plus treble damages, apply to every invoice submitted against a contract where the SPRS score was a condition of award or continued performance. A multi-year contract with monthly invoicing can generate dozens of individual claims, each carrying its own penalty.

The C3PAO Creates Documented Proof

The implementation of CMMC Assessment Certification across the defense industrial base is about to change the enforcement landscape for inaccurate SPRS scores.

Before CMMC, the government had limited visibility into the actual security posture of its contractors. Self-assessment meant self-reporting, and verification was rare. As C3PAOs begin conducting assessments at scale, they are generating documented, independent proof of exactly where organizations stand against the 110 requirements. When a C3PAO assessment reveals that an organization's actual posture is 100 or more points below its reported SPRS score, that documentation becomes available evidence in any subsequent enforcement action.

The MORSECORP settlement described in Chapter 1 illustrates this dynamic precisely. The company reported an

SPRS score of 104. A subsequent third party evaluation produced a score of negative 142. That is a gap of 246 points. The documented proof of the discrepancy was central to the $4.6 million settlement.

The Whistleblower Factor

The qui tam provisions described in Chapter 1 apply with particular force to SPRS score inaccuracies.

The person most likely to know that an organization's SPRS score does not reflect reality is someone inside the organization. The system administrator who knows the controls are not implemented. The IT manager who raised concerns that were overridden. The compliance officer who documented gaps that were never addressed. The former employee who left knowing the score was inflated.

Each of these individuals has a direct financial incentive to report the discrepancy under the False Claims Act's qui tam provisions. Whistleblowers in cybersecurity cases received more than $4.5 million in collective awards in fiscal year 2025 alone. Five of the nine cybersecurity settlements that year were initiated by whistleblowers. The financial incentive, combined with the ease of demonstrating that a reported score does not match the actual environment, makes SPRS score inaccuracy one of the most accessible qui tam opportunities in the defense industrial base.

Personal Liability

The executive accountability standard described in Chapter 1 applies with particular clarity to SPRS scores because someone had to sign the attestation.

The SPRS self-assessment requires an executive with authority to bind the organization to certify the accuracy of the reported score. That signature creates personal accountability. The standard is not whether the executive personally evaluated every control. The standard is whether the executive should have known that the score was inaccurate. If the executive signed a certification for a score of 90 without any independent verification that the score was accurate, a court can find that the executive should have known. Willful blindness is not a defense under the False Claims Act.

GRC Platforms and Discoverable Records

Many defense contractors have adopted automated governance, risk, and compliance platforms to manage CMMC compliance. From a legal risk perspective, that decision deserves careful consideration.

These platforms create a permanent, discoverable record of every known vulnerability and every internal deficiency the organization has identified and documented. Data stored in a standard commercial platform is not protected by attorney-client privilege. A subpoena to the GRC vendor is sufficient to place every gap analysis, every acknowledged deficiency, and every red flag in front of a Department of Justice investigator or a whistleblower's attorney.

The practical effect is that the organization may be paying a software company to build a comprehensive database of everything it knows it is doing wrong, fully accessible to anyone with a subpoena. That is worth understanding before populating one of these systems with candid assessments of compliance gaps.

What to Do If the Score Is Wrong

If there is reason to believe that the organization's SPRS score does not accurately reflect its actual security posture, the most important step is to involve qualified legal counsel before taking any other action.

Not after running a new gap analysis. Not after updating the SSP. Not after correcting the score in the system. Before any of those actions.

An attorney who understands both the False Claims Act and CMMC compliance can help the organization understand its exposure, structure the remediation in a way that provides legal protection, and advise on how to bring the score into alignment with reality without creating additional liability in the process. The sequence in which these steps are taken matters substantially. Getting the order wrong can turn a correctable problem into a documented admission.

The organization's outside compliance advisor, whether a Registered Practitioner Advanced or another qualified consultant, plays a role in this process, but that role should be defined and directed by legal counsel given the stakes involved. The technical expertise the advisor brings is essential for determining what the actual score should be. But the legal structure around how that expertise gets applied and how findings get documented is something only an attorney can properly advise on.

The Enforcement Trajectory

The enforcement cases described in Chapter 1 occurred before CMMC assessments were widespread across the defense industrial base.

Aerojet Rocketdyne settled for $9 million. MORSECORP settled for $4.6 million with a 246 point SPRS discrepancy. A major defense contractor settled for $8.4 million over a failure to implement a system security plan. Swiss

Automation, a small precision machining company, settled for $421,234. Georgia Tech Research Corporation settled for $875,000. In December 2025, a former senior manager at a defense contractor was criminally indicted for cybersecurity fraud exceeding $29 million.

Total cybersecurity related False Claims Act recoveries exceeded $52 million in fiscal year 2025, more than tripling for the second consecutive year. The Department of Justice has named cybersecurity fraud as a key enforcement priority. Whistleblower filings reached an all time high of 1,297 new qui tam suits in fiscal year 2025.

The defense industrial base is now entering a period where C3PAO assessments are generating documented, independent proof of compliance postures across thousands of organizations. Every assessment that reveals a significant discrepancy between a reported SPRS score and actual implementation creates a potential enforcement matter. The volume of documented evidence available to the Department of Justice and to qui tam relators will increase substantially as CMMC assessments scale.

For executives reading this chapter, the question is straightforward. Is the organization's SPRS score accurate? If the answer is yes, with confidence grounded in independent verification rather than assumption, the enforcement framework described here is not a concern. If the answer is uncertain, the time to address that uncertainty is now, through legal counsel, before a C3PAO assessment, a whistleblower, or a Department of Justice investigation resolves the question on less favorable terms.

In the concluding chapter, we examine the strategic opportunity that CMMC certification creates for organizations that have invested in genuine compliance and what that certification means for competitive positioning in a changing defense market.

Chapter 10: Taking CMMC Forward

The Assessment Certification is complete. The C3PAO has submitted its findings. The certification has been issued. The organization can now compete for Department of Defense contracts that require CMMC Level 2.

For many executives, this moment feels like the finish line. The investment has been substantial, the effort has been sustained, and the team has earned the result. The natural instinct is to exhale, turn attention back to operations, and move on.

That instinct is understandable. It is also the beginning of a three year problem if the organization acts on it.

Why Certification Is Not the Finish Line

CMMC certification is valid for three years. The security posture that earned that certification must be maintained for every one of those three years.

The Department of Defense did not create CMMC to produce a point-in-time snapshot of an organization's security. It created CMMC to ensure that organizations protecting controlled information maintain effective security programs on a sustained basis. The certification represents a verified baseline. The expectation is that the organization will operate at or above that baseline from the day certification is issued through the day the next assessment begins.

The enforcement framework described in Chapter 1 does not pause after certification. The False Claims Act applies to every invoice submitted against a contract where CMMC certification is a condition of performance. If the organization's security posture degrades after certification and the organization continues to accept contract payments, the same legal exposure that existed before certification exists again. The signature on the attestation represents an ongoing commitment, not a historical statement about what the organization looked like on assessment day.

How Security Postures Degrade

Security postures do not fail catastrophically. They erode gradually, in ways that are difficult to detect from inside the organization.

Staff turnover is the most common driver. The system administrator who understood the security architecture leaves and is replaced by someone who was not part of the compliance program. The new hire inherits the systems but not the institutional knowledge of why configurations are set the way they are. Within months, well-intentioned changes begin to drift from the documented baseline. Access controls are adjusted to accommodate operational requests. Logging configurations are modified to reduce storage costs. Network segmentation rules are relaxed to solve a connectivity problem. Each change is small and seemingly reasonable. Collectively, they erode the posture that earned certification.

Process discipline fades when the pressure of an upcoming assessment is no longer present. Quarterly access reviews that were conducted rigorously during the evidence window

become semiannual, then annual, then overdue. Vulnerability scans that ran monthly during remediation become sporadic. Training that was delivered on schedule before certification falls off the calendar when competing priorities take precedence. The processes still exist on paper. The execution no longer matches the documentation. This is the say-do gap described in Chapter 7, and it develops invisibly over time.

Technology changes accumulate. New systems are added to the environment. Cloud services are adopted. Software is upgraded. Hardware is replaced. Each change has the potential to affect the compliance boundary, the control implementations, and the evidence that supports them. Without someone evaluating whether each change affects the organization's CMMC posture, the environment documented in the SSP slowly diverges from the environment that actually exists.

Physical security controls receive less attention once the assessment pressure is gone. The visitor log that was maintained rigorously during the assessment month is completed less consistently. The destruction console that was emptied on schedule starts to overflow. The clean desk policy that was enforced before the C3PAO walked the facility becomes a suggestion rather than a requirement. The blind spots described in Chapter 6 do not reappear suddenly. They creep back in as the organizational attention that held them in check shifts elsewhere.

The Cost of Rebuilding Versus Maintaining

Organizations that allow their security posture to degrade after certification face a familiar and expensive problem when the three year reassessment approaches.

They must effectively repeat the remediation process described in Chapter 4. Controls that drifted from baseline must be reconfigured. Documentation that no longer reflects the environment must be rewritten. Training that lapsed must be delivered again. Evidence must be accumulated through another 90 day window. The cost of rebuilding a compliance program that was allowed to decay is not substantially different from the cost of building it the first time. The organization ends up paying for CMMC compliance twice in a six year period when it could have maintained it continuously for a fraction of the remediation cost.

Chapter 3 estimated ongoing annual maintenance costs at $30,000 to $60,000 for a mid-sized organization. That estimate assumed the organization was actively maintaining its program. The cost of rebuilding after three years of neglect can approach or exceed the original certification investment of $150,000 to $275,000. The financial argument for continuous maintenance is not close.

The RPA Support Plan

The most effective mechanism for maintaining a CMMC security posture between assessments is retaining the Registered Practitioner Advanced who guided the organization through certification on an ongoing support engagement.

A support plan typically involves the RPA making regular visits, whether monthly or quarterly depending on the organization's size and complexity, to verify that the security program continues to operate as documented. During these visits, the practitioner reviews whether controls remain configured to baseline, whether process execution records demonstrate continued compliance with documented procedures, whether training is current, whether personnel changes have been properly addressed, and whether any technology or operational changes have affected the compliance boundary.

The practitioner also serves as the first point of contact when the organization faces a compliance question between visits. A system administrator considering a configuration change can consult the practitioner before making the change rather than discovering months later that the modification affected a control. A hiring manager onboarding a new employee into a CUI role can confirm the training and access provisioning requirements. An operations manager evaluating a new vendor or cloud service can assess the compliance implications before the contract is signed. The practitioner functions as a standing resource, available when questions arise, rather than an emergency response engaged after problems have developed.

The cost of an RPA support plan is typically $2,000 to $4,000 per month depending on the scope of the engagement and the frequency of visits. Over a year, that represents $24,000 to $48,000 in support fees. Measured against the cost of rebuilding a degraded compliance program, which can run $100,000 or more in remediation

alone plus the risk of a failed reassessment, the support plan is inexpensive insurance.

Measured against the cost of trying to maintain the program entirely in-house, the support plan is also the more practical option. The expertise gap described in Chapter 5 does not disappear after certification. The organization's IT team still has operational responsibilities that compete with compliance maintenance. Internal staff still lack the assessment methodology training required to evaluate whether controls meet the standard that a C3PAO will apply. The practitioner brings the same outside perspective and domain expertise to ongoing maintenance that made the initial Discovery and mock audit process effective. The organization gets an expert watching over its security posture on a continuous basis, someone who will identify drift before it becomes a finding and address emerging issues before they compound into remediation projects.

What the Support Plan Covers

A well-structured RPA support plan addresses every category of degradation described earlier in this chapter.

Configuration verification confirms that technical controls remain at their documented baseline. The practitioner reviews access control configurations, logging settings, encryption status, network segmentation rules, and endpoint protection to identify any changes that have been made since the last review. Deviations are flagged and corrected before they accumulate.

Process compliance monitoring verifies that required processes are being executed on schedule. Access reviews, vulnerability scans, backup tests, incident response exercises, and all other recurring activities documented in the organization's policies are checked against actual execution records. Missed activities are identified and the organization is directed to complete them.

Personnel and training review confirms that new employees have completed required training, that annual refresher training is on schedule, and that personnel changes have been reflected in access controls and system documentation. When an employee who handled CUI departs, the practitioner verifies that access was revoked, credentials were disabled, and any CUI in the departing employee's custody was properly transferred or destroyed.

SSP and documentation maintenance ensures that the System Security Plan continues to reflect the actual environment. When systems are added, removed, or modified, the SSP must be updated. When policies or procedures change, the documentation must be revised. The practitioner ensures that the documentation package remains current rather than gradually diverging from reality.

Physical security review includes periodic walkthroughs to verify that the controls described in Chapter 6 remain in place. Visitor logs, media destruction procedures, access controls, and facility security measures are evaluated against the same standard that the C3PAO will apply during reassessment.

Regulatory change management is an increasingly important component of the support plan. The Department of Defense continuously evolves its cybersecurity requirements, and the standards that underpin CMMC do not stand still. NIST SP 800-171 Revision 3 is forthcoming as this book goes to print, and when it is adopted for CMMC, every certified organization will need to understand what changed, how those changes affect their existing controls, and what new requirements must be addressed before reassessment. An organization attempting to track these changes internally, without someone whose professional practice is built around the CMMC ecosystem, risks missing a revision that alters the compliance landscape between certification cycles. The RPA on a support plan is monitoring these developments as part of their practice and can translate regulatory changes into specific action items for the organization well before the reassessment timeline creates urgency.

Approaching Reassessment with Confidence

The organizations that approach their three year reassessment with confidence are the ones that never stopped operating their compliance program.

With an RPA support plan in place, the reassessment preparation is fundamentally different from the initial certification effort. There is no remediation phase because controls have been maintained continuously. There is no documentation overhaul because the SSP has been kept current. There is no training surge because training has been delivered on schedule throughout the cycle. The evidence

window is not a special phase because evidence has been accumulating through normal operations for three years.

The mock audit before reassessment becomes a verification exercise rather than a diagnostic one. The practitioner who has been monitoring the program for three years already knows its strengths and its areas of attention. The mock audit confirms readiness rather than discovering problems. The reassessment itself becomes a validation of ongoing practice rather than a reconstruction under deadline pressure.

The cost savings are substantial. Chapter 3 estimated recertification costs at 60 to 75 percent of initial certification for organizations that maintain their programs. For organizations that allow programs to degrade, recertification costs can approach or exceed the original investment. The difference between these two outcomes is the difference between continuous maintenance and periodic rebuilding.

The Strategic Position

Throughout this book, CMMC has been examined as a compliance requirement. It is also a competitive reality.

CMMC certification creates a qualification requirement that will reduce competition in the defense market. Organizations that cannot achieve certification or that allow certification to lapse will lose access to contracts they may have held for decades. Organizations that maintain active certification compete in a smaller, more qualified field.

The organizations that gain the most from this dynamic are not just the ones that achieve initial certification. They are the ones that maintain it without interruption. A three year gap in certification while an organization rebuilds a degraded program is a three year period of lost contract eligibility. Competitors who maintained their programs continuously will capture that work.

The investment in CMMC compliance, from the Discovery described in Chapter 3 through the Assessment Certification described in Chapter 8 and the ongoing maintenance described here, is an investment in sustained market access. The certification is the entry requirement. Maintaining it is the cost of staying in the market. And the organizations that treat maintenance as a continuous discipline rather than a periodic crisis are the ones that will compete most effectively in the defense industrial base for years to come.

That is the decision this book was written to inform. Not whether to comply, but how to comply intelligently, sustain that compliance efficiently, and lead an organization through a complex regulatory requirement to a position of genuine competitive strength.

Glossary

Assessment Certification

The formal third party evaluation conducted by a C3PAO that determines whether an organization has met CMMC requirements at the applicable level. Assessment Certification is the final phase of the compliance process, following Discovery and Remediation. The term is used throughout this book to distinguish the formal C3PAO evaluation from internal assessments and mock audits.

C3PAO (CMMC Third Party Assessment Organization)

An independent organization authorized by the CyberAB to conduct formal CMMC assessments and make certification recommendations. C3PAOs evaluate whether organizations meet certification requirements. The resulting certification is valid for three years, after which reassessment is required.

Civil Cyber-Fraud Initiative

A Department of Justice enforcement initiative announced in October 2021 that uses the False Claims Act to pursue government contractors and grant recipients who knowingly misrepresent their cybersecurity practices, provide deficient cybersecurity products or services, or violate obligations to monitor and report cybersecurity incidents.

CMMC (Cybersecurity Maturity Model Certification)

A Department of Defense cybersecurity certification program that replaces contractor self-assessment with structured verification. CMMC establishes three certification levels based on the sensitivity of the information being protected.

The program became part of federal regulation with 32 CFR Part 170.

CMMC Level 1

The baseline certification tier requiring implementation of 17 security practices outlined in FAR 52.204-21. Level 1 applies to organizations handling only Federal Contract Information and is verified through annual self-assessment with executive affirmation.

CMMC Level 2

The certification tier requiring implementation of all 110 security requirements specified in NIST SP 800-171. Level 2 applies to organizations handling Controlled Unclassified Information and, for most contracts, requires formal assessment by a C3PAO every three years.

CMMC Level 3

The certification tier for organizations working on the most sensitive national security programs. Level 3 builds on Level 2 requirements and adds enhanced controls from NIST SP 800-172. Assessments are conducted by the Defense Contract Management Agency rather than private C3PAOs.

Compliance Boundary

The defined scope of systems, networks, facilities, and personnel subject to CMMC requirements. Every system that processes, stores, or transmits CUI falls within the boundary and must meet applicable security requirements. Controlling the size of the compliance boundary is the most effective mechanism for controlling compliance cost.

CUI (Controlled Unclassified Information)

Sensitive federal information requiring protection due to national security, competitive, or operational concerns. CUI includes technical data, engineering specifications, designs, research findings, and operational information designated by the government through contract language and marking requirements. Organizations handling CUI must achieve CMMC Level 2 certification.

CUI Enclave

A segregated network environment where Controlled Unclassified Information is processed, stored, and transmitted under Level 2 controls. The enclave approach limits the compliance boundary to reduce cost and operational complexity while the broader business network operates at Level 1.

CyberAB

The CMMC Accreditation Body authorized by the Department of Defense to oversee the CMMC ecosystem. The CyberAB credentials Registered Practitioners and Registered Practitioners Advanced, authorizes C3PAOs, and establishes assessment standards and methodology.

DFARS 252.204-7012

The Defense Federal Acquisition Regulation Supplement clause that requires contractors to provide adequate security for covered defense information, report cyber incidents, and flow down security requirements to subcontractors. The presence of this clause in a contract indicates the organization is handling CUI.

Discovery

The diagnostic phase of CMMC compliance where the organization determines its actual security posture against applicable requirements. Discovery encompasses scoping, data flow analysis, control-by-control gap evaluation, and physical security walkthrough. The term is used throughout this book to distinguish internal diagnostic work from the formal C3PAO Assessment Certification.

EDR (Endpoint Detection and Response)

Advanced security software that monitors endpoints for threats beyond what traditional antivirus detects. EDR platforms provide real-time threat detection, investigation capabilities, and automated response to security incidents. EDR is a common technology investment during CMMC Level 2 remediation.

eMASS (Enterprise Mission Assurance Support Service)

The Department of Defense system of record for cybersecurity authorization and assessment data. After a C3PAO completes an Assessment Certification, results are submitted into eMASS for Department of Defense review before final certification is issued.

Evidence Window

The period during which an organization demonstrates sustained operation of its security controls by accumulating audit logs, process execution records, training documentation, and other evidence. Assessors expect a minimum of 90 days of operational evidence. The evidence window cannot be compressed because 90 days of logs require 90 days of time.

False Claims Act

A federal statute prohibiting the knowing submission of false claims for payment to the United States government. The Act applies to cybersecurity misrepresentations when contractors certify compliance they have not achieved. Civil penalties as of July 2025 range from $14,308 to $28,619 per false claim, in addition to treble damages. The Act's knowledge standard includes deliberate ignorance and reckless disregard for the truth.

FAR 52.204-21

The Federal Acquisition Regulation clause establishing basic safeguarding requirements for Federal Contract Information. It specifies 17 security practices that form the basis for CMMC Level 1.

FCI (Federal Contract Information)

Information provided by or generated for the government under a contract that is not intended for public release. FCI includes contract terms, delivery schedules, pricing information, and administrative correspondence. Organizations handling only FCI require CMMC Level 1 compliance.

FedRAMP Moderate Equivalency

The security standard that cloud services processing CUI must meet under CMMC Level 2. Cloud platforms that do not meet FedRAMP Moderate baseline requirements or demonstrate equivalent security require migration to compliant alternatives.

GRC Platform (Governance, Risk, and Compliance)

Software tools used to manage compliance programs, track controls, and document security activities. GRC platforms create permanent, discoverable records. Data stored in standard commercial GRC platforms is generally not protected by attorney-client privilege and may be subject to subpoena.

MFA (Multi-Factor Authentication)

An access control mechanism requiring two or more verification factors to authenticate a user. MFA is required for all personnel accessing CUI environments under NIST SP 800-171.

Mock Audit

A simulated Assessment Certification conducted before the formal C3PAO evaluation to identify remaining gaps, test evidence completeness, and prepare personnel for assessor interviews. Mock audits should be conducted by a Registered Practitioner Advanced with training in both the Level 2 controls and the assessment procedure, not by internal staff.

MSP (Managed Service Provider)

A third party organization that manages IT infrastructure, security, or other technical services on behalf of a client. If an MSP has administrative access to systems within a CUI environment, the MSP's infrastructure falls within the compliance boundary and must meet applicable CMMC requirements.

NIST SP 800-171

National Institute of Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. It

specifies 110 security requirements across 14 control families that form the foundation for CMMC Level 2 certification. Revision 2 is the current basis for CMMC. Revision 3 is forthcoming.

NIST SP 800-172

National Institute of Standards and Technology Special Publication 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information. It provides additional requirements beyond NIST SP 800-171 for CMMC Level 3 certification, addressing advanced persistent threats.

Physical Security Controls

Measures addressing physical access to facilities, systems, and information. These include access controls for CUI areas, visitor management and escort requirements, media destruction procedures, secure storage, and controls governing cleaning crews, third party vendors, and maintenance personnel.

Plan of Action and Milestones (POA&M)
A structured document identifying security deficiencies, planned remediation activities, required resources, and completion timelines. Organizations may receive conditional certification with POA&M items that must be closed within specified timeframes.

Qualified Sorter
A designated individual responsible for verifying that only appropriate materials are placed in locked destruction bins before pickup by a destruction service. The qualified sorter performs a visual inspection to prevent non-CUI materials from entering the destruction chain of custody where they cannot be retrieved.

Qui Tam
A provision of the False Claims Act that allows private individuals, known as relators, to file lawsuits on behalf of the federal government alleging fraud. Successful whistleblowers may receive between 15 and 30 percent of any government recovery. In fiscal year 2025, 1,297 new qui tam suits were filed and more than $5.3 billion was recovered through whistleblower actions.

Registered Practitioner (RP)
A CMMC credential issued through the CyberAB for individuals qualified to provide advisory services to organizations preparing for CMMC certification. RPs conduct Discovery, advise during Remediation, and support readiness but do not conduct formal certification assessments.

Registered Practitioner Advanced (RPA)

An advanced CMMC credential issued through the CyberAB requiring demonstrated knowledge of both the NIST SP 800-171 security requirements and the assessment methodology used by C3PAOs. RPAs conduct mock audits, advise on complex compliance matters, and provide the depth of expertise required for Level 2 readiness evaluation.

Remediation

The implementation phase of CMMC compliance where identified gaps are closed through technology deployment, documentation development, process implementation, physical security improvements, and personnel training. Remediation follows Discovery and precedes the evidence window.

Say-Do Gap

The discrepancy between what an organization's documentation says it does and what it actually does in practice. The say-do gap is the most common source of Assessment Certification findings and is the primary target of mock audit evaluation.

SIEM (Security Information and Event Management)

A platform that collects, aggregates, and analyzes security event data from across an organization's IT environment. SIEM systems support the audit logging, monitoring, and incident detection requirements of NIST SP 800-171.

SPRS (Supplier Performance Risk System)

A Department of Defense managed database where defense contractors submit self-assessed scores reflecting their implementation of NIST SP 800-171 security requirements.

The score ranges from 110 for full implementation to negative 203 for no implementation. SPRS scores are tied to contract eligibility and are reviewed by C3PAOs during Assessment Certification.

SSP (System Security Plan)

The central compliance document that describes every in-scope system, the security controls applied to each, and the evidence demonstrating those controls are operating. The SSP is reviewed by the C3PAO in Phase 1 of Assessment Certification and must reflect the actual operating environment, not a generic template.

System Security Plan

See SSP.

For additional information: davidkoran.com

About the Author

David W. Koran is a CMMC Registered Practitioner Advanced with over 30 years of experience in information technology and cybersecurity. He is the Managing Partner of David Koran & Associates Inc., where he serves Defense Industrial Base contractors and their legal counsel on CMMC readiness, compliance implementation, and sustained certification maintenance. He is an Associate Member of the American Bar Association Section of Public Contract Law.

David served as a United States Marine from 1983 to 1987, including duty as an 0311 Rifleman, Marine Security Force, and Marine Detachment aboard the USS Constellation CV-64. After his military service, he entered the technology industry designing and implementing systems for financial services clients in New York City during the Y2K era, when protecting systems and data was simply part of building them correctly because cybersecurity as a discipline did not yet have a name. His career expanded internationally when he spent six years as Director of Security, both physical and cybersecurity, for multiple companies within the Clark Development Industrial Park in the Philippines, where he built a security training program from scratch in an operational environment with real and active threats.

That combination of military discipline, financial services rigor, and international security leadership informs the approach to CMMC compliance described throughout this book. David's work now centers on helping defense contractors navigate certification from initial Discovery through Assessment Certification and the sustained maintenance that follows, delivered without unnecessary jargon and without a product to sell.

Semper Fidelis