ESPRESSO LABS

CONQUERING CMMC

A Comprehensive Guide to the Cybersecurity Maturity Model Certification

ADI RUPPIN

ESPRESSO LABS

Table of Contents

Introduction: A Vision to Secure the Defense Industrial Base

Why This Book Exists

The United States defense industrial base is one of the most strategically important ecosystems in the world, and one of the most under-protected. More than 300,000 companies, ranging from major aerospace primes to two-person machine shops in the American heartland, collectively design, build, and sustain the platforms, systems, and technologies that underpin American military superiority. They share sensitive technical data, operational specifications, and program details that adversaries spend enormous resources trying to steal. And for decades, far too many of them have done so without the cybersecurity infrastructure to keep that information safe.

This is not a story of negligence. Most defense contractors are small businesses run by engineers, operators, and entrepreneurs who are extraordinarily skilled at what they do: building things, solving hard technical problems, delivering for the warfighter. Cybersecurity compliance has historically been a domain that required specialized expertise, significant budget, and sustained organizational attention that few small and mid-size companies could realistically sustain alongside the demands of running a business. The result has been a gap. Not from indifference, but from inaccessibility.

CMMC was created to close that gap. This book was written to help every defense contractor, regardless of size, technical sophistication, or prior compliance experience, understand what CMMC requires, what it costs, how to build a program that actually works, and how to use modern tools to make compliance achievable without breaking the business in the process.

Our Vision: Security as a National Imperative

At Espresso Labs, we believe that securing the defense industrial base is not merely a regulatory exercise — it is a national security

imperative. Every piece of controlled technical information that leaks through an unsecured contractor network is a gift to an adversary. Every stolen design, every compromised specification, every exfiltrated test result shortens the distance between our adversaries' capabilities and our own. The cost of these losses is measured not just in dollars but in the strategic advantage that American defense technology is meant to provide: an advantage that, once lost, takes years and billions of dollars to rebuild.

We built Espresso Labs because we believe the defense industrial base deserves better than the compliance tools and services it has historically had access to. The traditional model consisting of expensive consultants, a hodgepodge of tools, annual assessments with months of manual evidence gathering in between, was designed for large enterprises with dedicated security and compliance teams. It was never designed for the 80% of the DIB that is a small business. It was never designed for the speed of the threat environment we operate in today. And it was never designed to make compliance genuinely sustainable rather than a painful, recurring scramble before each assessment cycle.

Our vision is simple: every defense contractor in America, regardless of size or resources, should be able to achieve and maintain world-class cybersecurity compliance, and do so without sacrificing the energy and attention that makes their core business run. That vision requires a fundamental rethinking of how compliance works, who it is designed for, and what tools make it possible.

The Stakes

The DoD Inspector General estimated that inadequate cybersecurity among defense contractors costs the United States hundreds of billions of dollars in lost intellectual property annually. Nation-state actors — China, Russia, Iran, North Korea — target the DIB specifically because contractor networks are the softest path to the most sensitive defense technology. Securing the DIB is not bureaucratic box-checking. It is defending the technological edge that American national security depends on.

Making Compliance Accessible to All

One of the most troubling dynamics in the CMMC rollout is the risk of compliance becoming a barrier that consolidates the defense industrial base around large, well-resourced primes. Not because they are better at the actual work of defense, but because they can absorb compliance costs that smaller companies cannot. A small precision manufacturer in Ohio or a specialized electronics firm in Texas that has served the DoD faithfully for twenty years should not lose its place in the defense supply chain because it cannot afford a team of compliance consultants and a six-figure GRC platform.

Accessibility is not about lowering the security bar. The 110 requirements of NIST SP 800-171 exist because the threat is real and the information is genuinely sensitive. Accessibility is about making the tools and expertise required to meet that bar available to organizations that have traditionally been priced out through smarter automation, more efficient processes, and service models calibrated to the reality of small business operations rather than the assumptions of enterprise IT departments.

This is a strategic goal. A defense industrial base that loses its small and mid-size suppliers to compliance attrition is a less resilient, less innovative, and less competitive one. The specialized capabilities, the niche expertise, and the manufacturing diversity that small DIB companies provide are national security assets. Protecting those companies' ability to participate in defense work is part of what it means to secure the DIB.

AI and Automation as the Great Equalizer

The technology that makes our vision possible is artificial intelligence. Not as a buzzword, but as a genuine operational capability that changes the economics of compliance in favor of smaller organizations. For the first time in the history of cybersecurity compliance, AI allows a small defense contractor to access the same quality of continuous monitoring, evidence generation, threat detection, and compliance management that

previously required a dedicated security operations center and a team of specialists.

AI does not replace human judgment in compliance. It amplifies it. The security professional who previously spent 60% of their time manually collecting evidence, maintaining documentation, and preparing for assessments can instead focus on the decisions that genuinely require human expertise: evaluating risk, building relationships with assessors, making architectural decisions, and responding to the incidents that matter. AI handles the volume; humans handle the judgment.

Automation compounds this effect. When a security control is not just documented but enforced by an automated system, when MFA is not merely required by policy but mandated by the identity platform and verified continuously, the control becomes structural rather than behavioral. It does not depend on every employee remembering to follow a procedure. It does not degrade when the compliance team is busy, when a staff member leaves, or when the organization goes through a period of rapid growth. Automated controls are more reliable, more auditable, and ultimately less expensive to maintain than their manual equivalents.

The Espresso Labs Model — AI Augments, Humans Decide

What AI and Automation Specifically Eliminate

The CMMC compliance burden has historically been dominated by three categories of work that consume enormous time and cost without adding meaningful security value: manual evidence collection, repetitive documentation maintenance, and periodic assessment scrambles. These are exactly the categories that AI and automation eliminate most completely.

Traditional Compliance Burden	What AI/Automation Replaces It With	Impact
Manual evidence collection: pulling log samples, taking configuration screenshots, exporting access control lists before each assessment	Continuous, automatic evidence capture tied to every control action the platform takes — always current, always organized, always mapped to the right requirement	Eliminates weeks of pre-assessment preparation; evidence is assessment-ready 365 days a year
SSP and policy maintenance: updating documents manually when the environment changes, hoping someone remembers to revise the right section	Platform-driven SSP that flags sections requiring update when asset inventory, control status, or configuration changes are detected	Eliminates documentation drift — the gap between what the SSP says and what the environment actually does
Vulnerability management: scheduling scans, reviewing reports, tracking remediation in spreadsheets, writing status updates	Automated scanning on risk-based schedules, AI-prioritized findings, automated patch deployment, ticket-tracked remediation with evidence attached	Reduces remediation cycle time by 60–80%; eliminates the spreadsheet tracking that creates no security value
Incident detection and response: reviewing SIEM alerts manually, triaging false positives, assembling timelines from disparate log sources	AI-powered alert correlation, automated playbook response for known patterns, pre-assembled IR case files with evidence already gathered	Compresses detection-to-response time from hours to minutes; ensures 72-hour DoD reporting is achievable on every incident
Assessment preparation: gathering evidence, organizing folders, briefing staff, running through control checklists in the weeks before a C3PAO visit	On-demand evidence package generation from the platform's continuously maintained evidence library — organized by requirement, by domain, or by assessor request	Reduces assessment prep from weeks to days; improves assessment outcomes by presenting organized, complete evidence rather than reconstructed fragments

Compliance expertise gap: small companies cannot afford a CISO or compliance team with the depth to manage a full CMMC program	AI-native platform embeds compliance expertise into the system itself — gap detection, control scoring, POA&M management, and SPRS tracking require no specialized knowledge to operate	Democratizes access to expert-level compliance management; a company with one part-time IT administrator can sustain a CMMC Level 2 program

How to Use This Book

This book is designed to be useful regardless of where you are in your CMMC journey. If you are starting from zero, not sure whether CMMC applies to you, not sure what FCI and CUI are, not sure where to begin, the early chapters provide the foundational knowledge you need to make those determinations and start building a compliance roadmap.

If you are further along, already working through NIST SP 800-171 implementation, preparing for a C3PAO assessment, or managing a supply chain with CMMC flowdown obligations, the middle and later chapters provide detailed practical guidance on the specific challenges you are facing. The assessment chapter (Chapter 6) is particularly useful for organizations in the final stages of preparation. The business considerations chapter (Chapter 11) provides the ROI framework that helps justify the investment to leadership and boards.

The final chapter covers how Espresso Labs can help compress your timeline, reduce your cost, and give you a compliance program that works as hard as your business does. We are not pitching a product — we are offering a partnership in a mission we believe matters. If that resonates, we would be glad to talk.

A Note on Currency

CMMC is a living regulatory framework. Requirements, assessment procedures, timelines, and guidance documents are updated periodically by the DoD and the Cyber AB. This book reflects the framework as of June

2026, including the CMMC 2.0 Final Rule (32 CFR Part 170) and the DFARS companion rule. Readers should verify current requirements against official DoD and Cyber AB publications before making compliance decisions. Where specific requirements, thresholds, or procedures are cited, the source regulation or guidance document is identified so readers can confirm currency independently.

Chapter 1: What Is CMMC and Why Was It Enacted?

1.1 The Threat Landscape Facing the Defense Industrial Base

The United States Department of Defense (DoD) relies on a vast ecosystem of commercial contractors, known collectively as the Defense Industrial Base (DIB), to design, manufacture, and sustain nearly every platform, weapon system, and service the military depends on. This network spans more than 300,000 companies, ranging from prime contractors with tens of thousands of employees to small machine shops and sole proprietors in rural America. What unites them all is access to sensitive government information: blueprints, technical data packages, acquisition strategies, and operational parameters that adversaries would pay a great deal to obtain.

Nation-state actors — most prominently China, Russia, Iran, and North Korea — have identified the DIB as a soft underbelly of American military capability. Rather than attacking hardened DoD networks directly, they target contractors whose cybersecurity posture is often far weaker. The result has been a sustained and damaging campaign of intellectual property theft, operational disruption, and supply-chain compromise that cost the United States an estimated hundreds of billions of dollars in lost competitive advantage over the past two decades.

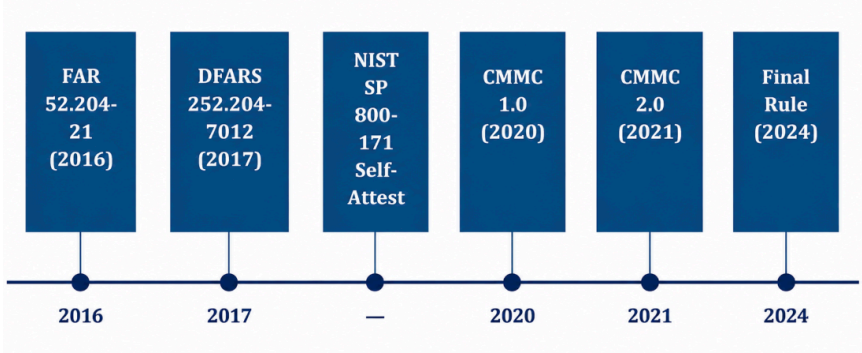
High-profile breaches have illustrated the stakes with painful clarity. The 2015 OPM breach exposed the personnel records of 21.5 million cleared individuals. Separate intrusions into defense contractors yielded designs for the F-35 Joint Strike Fighter, missile defense systems, and advanced radar technologies. In each case, the initial foothold was gained not through the government's own networks but through a contractor's under-defended systems. The adversary did not need to crack the Pentagon. It only needed to find the subcontractor making a single component who stored sensitive files on an unencrypted laptop.

The F-35 Joint Strike Fighter — design data compromised via contractor network breaches.

1.2 The Regulatory History: From DFARS to CMMC

The DoD's effort to impose cybersecurity discipline on contractors did not begin with CMMC. The regulatory journey started years earlier and evolved as each generation of controls proved insufficient on its own.

Regulatory Timeline — From FAR to CMMC



Federal Acquisition Regulation (FAR) clause 52.204-21, effective June 2016, established the first baseline: fifteen basic safeguarding requirements applying to any contractor system that processes, stores, or transmits Federal Contract Information (FCI). These requirements, things like limiting system access to authorized users and sanitizing media before disposal, were commonsense controls but deliberately minimal.

DFARS clause 252.204-7012, updated in October 2016 and made mandatory in December 2017, raised the bar significantly. It required contractors and subcontractors handling Controlled Unclassified Information (CUI) to implement all 110 security requirements in NIST Special Publication 800-171 and to report cyber incidents to the DoD within 72 hours. The 2017 rule was groundbreaking in scope but fatally flawed in enforcement: compliance was based entirely on self-attestation. A contractor only had to assert that it met the requirements; no independent verification was required.

Predictably, the self-attestation model failed. A 2018 DoD Inspector General report found widespread non-compliance across the DIB, with many contractors either misunderstanding the requirements or simply misrepresenting their posture to win contracts. The problem was not purely bad faith as NIST SP 800-171 is genuinely complex, and smaller companies often lacked the expertise to implement it correctly. However, the combination of no verification and significant contractual risk created perverse incentives for checked-box compliance over real security.

1.3 The Birth of CMMC

In January 2020, Under Secretary of Defense for Acquisition and Sustainment Ellen Lord announced CMMC 1.0. The core innovation was third-party verification: rather than self-attesting, contractors at certain maturity levels would need to be assessed by a certified third-party assessment organization (C3PAO) and receive a formal certification before they could bid on certain contracts. CMMC 1.0 defined five maturity levels, each requiring increasingly

sophisticated cybersecurity practices and process institutionalization.

The model drew heavily on established frameworks, particularly NIST SP 800-171 and NIST SP 800-172, but added a process maturity dimension that required organizations not only to implement controls but to demonstrate that they had documented, reviewed, and institutionalized those controls into repeatable organizational processes. The approach borrowed from the Software Engineering Institute's Capability Maturity Model Integration (CMMI), which gave CMMC its name.

1.4 CMMC 2.0: Streamlining Without Sacrificing Security

In November 2021, the DoD announced a significant revision, CMMC 2.0, following an internal review that heard concerns from industry about complexity, cost, and the feasibility of third-party assessments for small businesses. CMMC 2.0 made three major changes:

1. Reduced the five maturity levels to three, eliminating the intermediate Levels 2 and 4 from 1.0.
2. Eliminated unique CMMC-specific practices and processes, aligning directly with NIST SP 800-171 and 800-172.
3. Allowed self-attestation for most Level 2 contracts on a "non-prioritized acquisition" basis, with third-party assessments required only for "prioritized" contracts and all Level 3 work.

Critics noted that these changes — particularly the expansion of self-attestation — risked recreating the exact problem CMMC was meant to solve. Supporters argued that maintaining the C3PAO requirement for the most sensitive work, combined with the threat of False Claims Act liability for contractors who mis-attest, would provide meaningful accountability without crushing small businesses with assessment costs.

1.5 The Final Rule and Current Status

The CMMC 2.0 Final Rule (32 CFR Part 170) was published in October 2024, completing the rulemaking process that had begun

years earlier. A companion DFARS rule (48 CFR Parts 202, 212, 215, 219, 234, 239, and 252) governs how CMMC requirements flow into contracts. As of 2025, the DoD began phasing CMMC requirements into contracts, with full implementation expected across new solicitations by 2026.

Understanding why CMMC was enacted and the regulatory failures that preceded it is essential context for understanding everything that follows. CMMC is not merely another compliance checkbox. It is the DoD's answer to a decade of evidence that voluntary cybersecurity controls in the defense supply chain are insufficient to protect national security. Every requirement in the framework, every assessment procedure, and every penalty provision traces back to the fundamental lesson of those years: without verification and accountability, contractors will not invest adequately in security, and adversaries will exploit the resulting gaps.

Key Takeaway — Chapter 1
CMMC exists because voluntary, self-attested cybersecurity requirements failed to stop nation-state actors from stealing sensitive defense technology through contractor networks. The framework introduces mandatory, verifiable controls aligned with NIST standards, backed by the False Claims Act and contract exclusion for non-compliant companies.

Chapter 2: What Exactly Are FCI and CUI?

2.1 Two Categories, Two Regulatory Regimes

The entire CMMC framework is organized around two categories of sensitive government information: Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Understanding the distinction between them and what each category requires is the single most important conceptual building block in CMMC compliance. Organizations that confuse the two, or that fail to identify which category applies to their work, will build programs calibrated to the wrong requirements.

2.2 Federal Contract Information (FCI)

FCI is defined in FAR 4.1901 as "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government." The definition is broader than it might initially appear.

Any information the government provides to a contractor in the course of contract performance — and any information the contractor generates in performing that work — is FCI, so long as it was not intended for public release. This means that a company installing IT equipment for a federal agency may be handling FCI even if it never touches a classified network. A landscaping contractor managing grounds at a federal facility may store FCI in its contract administration records.

Common examples of FCI include:

- Contract terms, pricing, and performance requirements
- Government-furnished property lists and specifications
- Correspondence with contracting officers about scope or schedule
- Deliverables produced under the contract before government acceptance
- Personnel information related to contract performance

FCI does not include information that is publicly available, information provided by the contractor to the government (rather than the reverse), or information that the government has explicitly authorized for public release. The key regulatory hook is FAR 52.204-21, which imposes fifteen basic safeguarding requirements on any contractor system that processes, stores, or transmits FCI. CMMC Level 1 is the certification that corresponds to these requirements.

2.3 Controlled Unclassified Information (CUI)

CUI is a category established by Executive Order 13556 (2010) to standardize the way the executive branch handles sensitive but unclassified information. Before EO 13556, different agencies used dozens of different labels, such as Sensitive But Unclassified (SBU), For Official Use Only (FOUO), Law Enforcement Sensitive (LES), and many more, with inconsistent handling rules. The CUI program replaced this patchwork with a single framework administered by the National Archives and Records Administration (NARA) through the CUI Registry.

CUI is defined as "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls." The key phrase is "that a law, regulation, or Government-wide policy requires or permits". CUI must have an explicit legal or regulatory basis, not merely an agency preference for limiting distribution.

2.4 The CUI Registry

The CUI Registry (cui.archives.gov) is the authoritative source for CUI categories and subcategories. It organizes CUI into twenty broad categories, each with multiple subcategories, and specifies the handling requirements and legal authorities for each. For defense contractors, the most commonly encountered categories include:

CUI Category	Common Subcategories	Typical Defense Context
Critical Infrastructure	Chemical, Defense Industrial Base, Energy	Facility vulnerability data, infrastructure plans
Defense	Naval Nuclear Propulsion, Controlled Technical Information (CTI)	Technical data packages, engineering drawings, specifications
Export Control	Export Administration Regulations (EAR), ITAR	Technology with export restrictions, defense articles
Intelligence	Finished Intelligence, Foreign Government Info	Intelligence assessments shared with contractors
Law Enforcement	Controlled Technical Information, Investigative Records	Security investigation data, personnel security
Privacy	Health Information, Personnel Records	Employee and beneficiary data, medical information
Procurement and Acquisition	Source Selection, Budget	Pre-award source selection data, program budgets
Technical	Controlled Technical Information (CTI)	Drawings, models, specifications under DoD contracts

2.5 CUI Basic vs. CUI Specified

Within the CUI framework, there is an important further distinction between "CUI Basic" and "CUI Specified."

CUI Basic is information whose handling is governed by the baseline CUI policy, 32 CFR Part 2002 and the CUI Registry. When no specific handling instructions are given, the baseline requirements apply. Most CUI that defense contractors encounter is CUI Basic.

CUI Specified is information for which the authorizing law, regulation, or government-wide policy provides specific handling requirements that deviate from, or layer on top of, the baseline. Export-controlled technical data under the International Traffic in

Arms Regulations (ITAR) is an example: ITAR imposes requirements beyond the CUI baseline, and those additional requirements govern when ITAR-controlled information is involved.

2.6 CUI Markings and Handling

One of the most operationally significant aspects of CUI is the marking requirement. Properly identified CUI should be marked with the "CUI" designation at the top and bottom of each page of a physical or electronic document. Subcategory markings (e.g., "CUI//CTI" for Controlled Technical Information) provide additional specificity. Dissemination limitation markings (e.g., "CUI//CTI//FEDCON" for Federal Employees and Contractors Only) further restrict sharing.

Sample CUI marker

In practice, marking compliance in the DIB is inconsistent. Government agencies themselves frequently fail to properly mark CUI before sharing it with contractors. Contractors therefore need documented processes for identifying likely CUI even when it arrives without proper markings — a significant organizational challenge that the best CMMC programs address explicitly.

NOTE: Physical Media Marking — CUI Labels for Hardware and Storage

The marking requirement extends beyond paper documents and digital files to physical hardware and storage media. Any physical item: hard drives, USB drives, SD cards, optical discs, printed circuit boards containing embedded firmware with CUI, and even equipment enclosures, that stores or processes CUI must be visibly labeled with the CUI designation.

The most practical way to meet this requirement is with purpose-made CUI labels. **CUISupply.com**) is a widely used source for the official CUI purple tamper-evident labels that match the marking standards specified in 32 CFR Part 2002 and NARA guidance. Their label stock comes in multiple sizes to accommodate everything from 2.5" hard drives to full server chassis, and the purple color is the recognized industry standard that assessors and auditors expect to see.

Practical guidance for physical CUI labeling:
• Apply a CUI label to every removable storage device that stores CUI (USB drives, external hard drives, tapes, optical media).
• Label server equipment or rack units in your CUI environment.
• Use tamper-evident label stock so that unauthorized removal of the label is detectable.
• Maintain an inventory log correlating labeled media/equipment to the CUI it contains.
• Include your physical labeling procedure in your Media Protection Policy and SSP.

Assessors will physically inspect your environment. Unlabeled CUI media sitting in a desk drawer or equipment room — even if it is technically protected — is a finding. A small investment in proper labels eliminates a common and easily avoidable gap.

2.7 Why the FCI/CUI Distinction Drives Your CMMC Level

Information Type	Applicable Regulation	CMMC Level Required	Controls Framework
FCI only (no CUI)	FAR 52.204-21	Level 1	17 practices (FAR basic safeguarding)
CUI (non-prioritized acquisitions)	DFARS 252.204-7012	Level 2 (self-attestation)	NIST SP 800-171 (110 requirements)

CUI (prioritized/critical programs)	DFARS 252.204-7012	Level 2 (C3PAO assessment)	NIST SP 800-171 (110 requirements)
CUI + advanced persistent threat risk	DFARS 252.204-7012 + 7021	Level 3 (DCSA-led assessment)	NIST SP 800-171 + 800-172 (110+ requirements)

The practical implication: every contractor's first CMMC task is to determine what type of information flows through its systems. That determination drives everything else: scope, controls, assessment path, and cost. Organizations that handle only FCI have a dramatically simpler compliance path than those handling CUI, and organizations that handle CUI on high-priority programs face the full weight of third-party assessment requirements.

Practical Tip — Identifying CUI in Your Environment

1. Review contract clauses: DFARs 252.204-7012 in your contract is the clearest signal that CUI is expected.
2. Examine attachments and PWS: Performance Work Statements and Contract Data Requirements Lists (CDRLs) often describe what data you will receive or generate.
3. Ask the contracting officer: If in doubt, request a CUI identification from the Government. Document the response.
4. Check DD Form 1423 (CDRLs) for data items that may carry CUI markings.
5. Review all government-furnished information (GFI) packages for marking.

Chapter 3: Who Needs to Be CMMC Compliant?

3.1 The Scope of the DIB

CMMC applies to all companies of any size, in any industry, that are parties to DoD contracts or subcontracts where the performance involves processing, storing, or transmitting FCI or CUI. The breadth of this definition catches many organizations by surprise. CMMC is not limited to traditional defense primes or aerospace manufacturers. It can apply equally to:

- A university research lab receiving DoD-funded research grants that involve CUI
- A staffing firm placing cleared personnel on DoD programs
- A cloud service provider hosting DoD contractor data
- A healthcare company providing occupational health services to a prime contractor's employees under a DoD contract
- An accounting firm auditing a defense contractor's cost accounting system under a DoD contract
- A logistics company managing supply chain for a defense prime

3.2 Determining Your CMMC Level

The CMMC level that applies to an organization is determined by the type of information it handles, the sensitivity of the programs it supports, and the specific contract clauses the DoD includes in its solicitations. The three-level structure works as follows:

Level 1 — Foundational applies when:

- The contract involves FCI but not CUI.
- FAR clause 52.204-21 is included but DFARS 252.204-7012 is not.
- The contractor does NOT receive, generate, or process CUI.

Level 1 requires implementation of 17 basic practices drawn directly from FAR 52.204-21. Self-attestation is sufficient. No third-party assessment is required. The company must have a senior official affirm compliance annually in the Supplier Performance Risk System (SPRS).

Level 2 — Advanced applies when:

- The contract involves CUI.
- DFARS clause 252.204-7012 is included in the contract.
- The program is part of the DoD's acquisition universe handling sensitive defense information.

Level 2 requires all 110 security requirements from NIST SP 800-171 Rev 2. For most Level 2 contracts, a triennial third-party assessment by a C3PAO is required. For a subset of "non-prioritized" contracts, DoD has indicated that self-attestation may be accepted, but contractors should not assume this without specific contract guidance. Self-assessment must be affirmed by a senior company official.

Level 3 — Expert applies when:

- The program presents heightened risk of attack by advanced persistent threats (APTs).
- The DoD has specifically designated the contract as requiring Level 3.
- Work involves the most sensitive CUI or critical DoD technologies.

Level 3 requires implementation of all NIST SP 800-171 requirements plus a subset of NIST SP 800-172 requirements (currently anticipated to be 24 additional practices). Assessments are conducted by Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), not by C3PAOs. The assessment cadence is every three years.

3.3 The CMMC Scoping Process

One of the most consequential (and most frequently mishandled) aspects of CMMC compliance is scoping. The CMMC Assessment Scope defines which of your assets are subject to CMMC requirements, and getting this right dramatically affects both your compliance burden and your assessment outcome.

CMMC defines five asset categories that must be identified during scoping:

Asset Category	Definition	CMMC Requirement
CUI Assets	Systems that process, store, or transmit CUI	Full CMMC Level 2 or 3 requirements apply
Security Protection Assets	Systems that provide security functions protecting CUI assets (firewalls, IAM, SIEM, etc.)	Full CMMC requirements apply
Contractor Risk Managed Assets	Systems that can reach CUI assets but do NOT process/store/transmit CUI	Must be documented; contractor manages risk
Specialized Assets (OT/IoT/GFE)	Operational technology, IoT devices, government-furnished equipment	Assessed against unique criteria
Out-of-Scope Assets	Systems with no path to CUI and no security function for CUI assets	No CMMC requirements

Effective scoping is the primary lever for reducing CMMC compliance costs. Organizations that segment their CUI-handling environment from the rest of their network, through network segmentation,

dedicated CUI workstations, or use of government-compliant cloud environments, can dramatically reduce the number of assets in scope. Conversely, organizations that allow CUI to flow freely across their entire enterprise find their entire IT environment in scope, multiplying assessment complexity and remediation cost.

3.4 Small Businesses and CMMC

Small businesses represent a disproportionate share of the DIB by count and face unique challenges in achieving CMMC compliance. The DoD has acknowledged these challenges and has taken some steps to accommodate small businesses, including the Project Spectrum initiative (a free resource hub), access to DoD-sponsored cybersecurity shared services, and the allowance of self-attestation for a portion of Level 2 contracts.

Nevertheless, the fundamental requirements of NIST SP 800-171 are the same regardless of company size. A five-person engineering firm handling CUI must meet the same 110 requirements as a 50,000-employee prime contractor. The practical implication is that small businesses have fewer internal resources to implement and sustain controls, making external managed security service providers (MSSPs) and purpose-built CMMC platforms an important part of the compliance toolkit for smaller DIB participants.

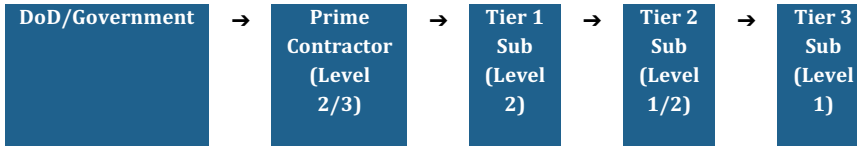
Self-Assessment Checklist — Do I Need CMMC?
Step 1: Review your DoD contracts and subcontracts for FAR 52.204-21 and DFARS 252.204-7012.
Step 2: Identify whether you receive, generate, or process CUI in contract performance.
Step 3: If CUI is involved, determine if the DoD has designated the acquisition as "prioritized."
Step 4: Check for CMMC clause DFARS 252.204-7021 in solicitations.
Step 5: If any of the above apply, you need CMMC — determine the appropriate level.

Chapter 4: The Flowdown of Primes and Subs

4.1 Why Flowdown Matters

The security of the defense supply chain is only as strong as its weakest link. Adversaries targeting a prime contractor's systems will often find that the prime has robust security — and will pivot to finding a subcontractor with access to the same sensitive data but far weaker controls. For this reason, CMMC is not limited to the prime contractor who holds the government contract. The requirements flow down through every tier of the supply chain to every subcontractor that handles FCI or CUI in performing the work.

CMMC Flowdown Through Supply Chain Tiers



4.2 The Legal Mechanism: Contract Clauses

The legal vehicle for CMMC flowdown is the contract clause. When the DoD includes DFARS 252.204-7021 in a prime contract, it requires the prime to flow down that clause — or the equivalent requirements — to all subcontractors that will handle CUI in performing the work. The prime is responsible for ensuring its subcontractors meet the applicable CMMC level before allowing them to access CUI.

This creates a legal and practical responsibility chain. If a prime contractor allows a sub to access CUI without verifying the sub's CMMC compliance, the prime may face False Claims Act liability, contract termination, and reputational damage — even if the actual breach occurred at the subcontractor level.

4.3 Prime Contractor Responsibilities

A prime contractor's CMMC supply chain obligations include:

4. Identifying which subcontractors will handle FCI or CUI in contract performance.
5. Determining the appropriate CMMC level for each subcontractor based on the type of information they will access.
6. Including appropriate CMMC contract clauses in subcontracts (the flow-down requirement).
7. Verifying that subcontractors have achieved the required CMMC level before allowing CUI access.
8. Maintaining records of subcontractor CMMC compliance status.
9. Monitoring subcontractor compliance throughout contract performance.
10. Reporting subcontractor cyber incidents that may affect prime or government systems.

The verification obligation is particularly significant. Primes cannot simply take a subcontractor's word for CMMC compliance. For Level 2 contracts requiring C3PAO assessment, the prime should obtain and retain a copy of the subcontractor's CMMC certification letter or verify the sub's status in the CMMC Enterprise Mission Assurance Support Service (eMASS) or equivalent DoD tracking system.

4.4 Subcontractor Responsibilities

Subcontractors must achieve and maintain the CMMC level required by their subcontract — which may or may not be the same level as the prime. The applicable level depends on what information the sub will actually handle. A subcontractor performing administrative support that never touches technical data may need only Level 1, while a subcontractor receiving engineering drawings or test data will likely need Level 2.

Subcontractors have an important right: they may not be required to implement CMMC requirements beyond what is necessary based on the information they actually handle. Primes cannot impose Level 3 requirements on subs that only handle standard CUI. However, subs should be cautious — primes may contractually require a higher level than strictly necessary as a risk management measure, and subcontractors accepting such requirements are bound by them.

4.5 Managing Third-Party Risk

Effective supply chain risk management under CMMC goes beyond contract clause inclusion. Best-practice prime contractors build systematic supply chain security programs that include:

- Vendor cybersecurity questionnaires and risk assessments during source selection
- Contractual rights to audit subcontractor cybersecurity practices
- Requirements for subcontractors to report cyber incidents promptly
- Periodic re-verification of subcontractor CMMC status (since certifications can be suspended or revoked)
- Incident response plan coordination across the supply chain
- Data handling agreements specifying CUI marking, storage, and transmission requirements

Warning — The Sub-to-Sub Trap
If your Tier 1 subcontractor further subcontracts work involving CUI to a Tier 2 company, your prime contract flowdown obligation extends to that Tier 2 company as well. You are responsible for ensuring appropriate CMMC requirements flow all the way down. Many primes discover this requirement only after a contract audit or incident — at which point the consequences can be severe.

Chapter 5: How to Build a CMMC Program

5.1 The Program Mindset

CMMC compliance is not a project — it is a program. A project has a defined start and end; a compliance program has no end. Controls must be sustained, documented, monitored, and continually improved. Organizations that approach CMMC as a one-time implementation effort — "get compliant, get certified, move on" — invariably fail their next assessment. The controls degrade, the documentation grows stale, and personnel turn over without transferring institutional knowledge.

Building a genuine CMMC program requires organizational commitment at the senior leadership level, dedicated resources (people, budget, technology), and governance structures that keep cybersecurity integrated with business operations rather than treated as a separate IT function. The sections that follow walk through the key phases of building that program.

CMMC Program Build Phases

5.2 Phase 1: Scoping and Gap Assessment

The first step in any CMMC program is determining what is in scope (covered in Chapter 3) and assessing the gap between your current security posture and the required CMMC level. The gap assessment is simultaneously a technical exercise, a documentation review, and an organizational analysis.

A comprehensive gap assessment should:

- Map all information flows involving FCI and CUI across your environment
- Identify all assets (hardware, software, services) that process, store, or transmit that information
- Evaluate each of the 110 NIST SP 800-171 requirements against your current controls
- Assess the maturity of your documentation (policies, procedures, SSP)
- Identify gaps where controls are absent, incomplete, or inadequately documented
- Estimate the effort and cost to remediate each gap

Gap assessments typically result in a findings report organized by the 14 NIST SP 800-171 requirement families, with each requirement scored as Met, Partially Met, or Not Met, along with evidence supporting the finding and recommended remediation actions.

5.3 The 14 NIST SP 800-171 Domains

#	Domain	Requirements	Description
1	Access Control (AC)	22	Limit system access to authorized users, processes, and devices
2	Awareness & Training (AT)	3	Ensure personnel are aware of cybersecurity risks
3	Audit & Accountability (AU)	9	Create and retain system audit logs
4	Configuration Management (CM)	9	Establish baseline configurations and manage changes

5	Identification & Authentication (IA)	11	Identify and authenticate users, processes, and devices
6	Incident Response (IR)	3	Establish operational incident-handling capability
7	Maintenance (MA)	6	Perform maintenance on organizational systems
8	Media Protection (MP)	9	Protect system media containing CUI
9	Personnel Security (PS)	2	Screen individuals prior to authorizing access
10	Physical Protection (PE)	6	Limit physical access to CUI systems
11	Risk Assessment (RA)	3	Assess risk to organizational operations from system use
12	Security Assessment (CA)	4	Periodically assess security controls
13	System & Communications Protection (SC)	16	Monitor and protect communications at system boundaries
14	System & Information Integrity (SI)	7	Identify, report, and correct information and system flaws

5.4 Phase 2: System Security Plan (SSP)

The System Security Plan (SSP) is the cornerstone CMMC document. It is a formal, written description of your information system's security controls, the environment in which those controls operate, and how each of the 110 NIST SP 800-171 requirements is implemented (or planned for implementation). The SSP is not optional — NIST SP 800-171 explicitly requires one (requirement 3.12.4), and C3PAO assessors will use it as the foundation for their assessment.

A complete SSP should contain:

- System identification and description (scope, boundaries, purpose)
- Network topology diagram showing CUI data flows and security boundaries
- Description of all hardware and software components in scope
- Interconnections with other systems (internal and external)
- For each of the 110 requirements: implementation status, description of how the control is implemented, and responsible roles
- References to supporting policies, procedures, and other artifacts
- Roles and responsibilities for system security

SSP quality is one of the strongest predictors of assessment success. Organizations with well-maintained, detailed SSPs consistently perform better in assessments than those that produce minimal, checkbox-style SSPs. The SSP should be treated as a living document, updated whenever significant changes are made to the environment or when controls change.

5.5 Phase 3: Plan of Action and Milestones (POA&M)

A Plan of Action and Milestones (POA&M) documents the security controls that are not yet fully implemented, along with the planned remediation actions, responsible parties, resource requirements, and target completion dates. The POA&M serves two purposes: it

demonstrates to assessors that you are aware of your gaps and have a credible plan to close them; and it provides an internal management tool for tracking remediation progress.

Under CMMC 2.0, a limited number of unimplemented requirements may be acceptable at the time of assessment, provided they are documented in a POA&M and closed within 180 days post-assessment. However, the specific rules for POA&M acceptance are complex — certain high-priority requirements may not be deferred, and the number of deferrable items is capped. Organizations should not rely on POA&M deferral as a substitute for genuine remediation.

5.6 Phase 4: Policies and Procedures

Controls without documentation are not controls — they are individual behaviors that may or may not be followed consistently. CMMC requires documented policies and procedures for each of the 14 security domains. These documents establish the organizational expectations, the technical and procedural requirements, and the accountability mechanisms that make controls sustainable over time.

The minimum policy documentation set for CMMC Level 2 includes:

- Access Control Policy and Procedures
- Security Awareness and Training Policy
- Audit and Accountability Policy
- Configuration Management Policy and Baseline Configuration Standards
- Identification and Authentication Policy (including multi-factor authentication requirements)
- Incident Response Plan and Procedures
- Maintenance Policy
- Media Protection Policy
- Personnel Security Policy (including hiring, departure, and transfer procedures)
- Physical and Environmental Protection Policy
- Risk Assessment Policy and Procedures
- System and Communications Protection Policy

- System and Information Integrity Policy
- CUI Handling Policy (marking, storage, transmission, disposal)

5.7 Phase 5: Technical Control Implementation

The technical controls are the actual security measures implemented in your environment to satisfy the NIST SP 800-171 requirements. Common technical implementation areas and frequently-cited deficiencies include:

Control Area	Common Gaps	Typical Solutions
Multi-Factor Authentication	Passwords-only for privileged and remote access	Authenticator apps, hardware tokens, PIV/CAC
Encryption	CUI stored unencrypted, unencrypted email	BitLocker/FileVault, S/MIME, encrypted cloud storage
Access Control	Excessive privileges, no least-privilege model	Role-based access control, PAM solutions
Audit Logging	Insufficient log retention, gaps in log collection	SIEM platforms, centralized log aggregation
Configuration Management	No documented baselines, ad-hoc changes	CIS Benchmarks, change management process
Vulnerability Management	Infrequent scanning, unpatched systems	Scheduled scans, patch management tooling
Incident Response	No documented IR plan, no 72-hour reporting capability	IR plan, tabletop exercises, IR retainer
Boundary Protection	Flat networks, CUI accessible from all systems	Network segmentation, next-gen firewalls
Media Sanitization	No formal process for retiring CUI media	NIST SP 800-88 sanitization procedures
Personnel Security	No background check requirements, no separation procedures	HR integration, access termination checklists

5.8 Phase 6: Continuous Monitoring and Sustainment

Achieving CMMC certification is the beginning, not the end, of the compliance journey. Controls must be continuously monitored to detect deviations, new vulnerabilities, and configuration drift. A sustainable CMMC program includes:

- Regular vulnerability scanning (at minimum quarterly; recommended continuous for in-scope assets)
- Annual security control assessments (internal) and triennial C3PAO assessments
- Real-time security event monitoring through a SIEM or managed detection service
- Change management processes that include security review before deployment
- Annual security awareness training with role-specific modules for privileged users
- Periodic tabletop exercises testing the incident response plan
- Regular SSP and policy reviews to reflect changes in the environment
- SPRS score updates whenever the security posture changes meaningfully

Chapter 6: The CMMC Assessment

6.1 What the Assessment Actually Is

A CMMC assessment is a structured, evidence-based examination of an organization's implementation of the security requirements corresponding to the applicable CMMC level. It is not an audit in the traditional financial sense — where an auditor reviews records to confirm historical accuracy — nor is it a penetration test that actively probes for exploitable vulnerabilities. It is closer in character to a technical compliance review: assessors examine whether controls exist, whether they function as described, and whether the organization can demonstrate through objective evidence that they are sustained over time.

For CMMC Level 2 (the level most DIB contractors will encounter), the assessment evaluates all 110 security requirements from NIST SP 800-171 Rev 2. For each requirement, the assessor must reach one of three findings: MET (the requirement is fully implemented and evidenced), NOT MET (the requirement is absent or insufficiently implemented), or NOT APPLICABLE (the requirement does not apply to this environment — a finding that must itself be justified). There is no partial credit in CMMC assessments. A requirement is either fully met or it is not.

This binary outcome structure is one of the most important things for contractors to internalize. A control that is 90% implemented — where the policy exists, the technology is deployed, but user training on that control was never completed — is a NOT MET finding, exactly the same as a control where nothing has been done. This reality drives the need for thorough pre-assessment preparation: every loose thread matters.

6.2 The CMMC Assessment Process (CAP)

The CMMC Assessment Process (CAP) is the official methodology published by the Cyber AB and DoD that governs how C3PAO assessors conduct Level 2 assessments. The CAP defines the phases of the assessment, the types of evidence assessors must examine,

and the criteria for each finding. Understanding the CAP is essential both for preparing for an assessment and for evaluating whether a C3PAO is conducting your assessment correctly.

The CAP organizes the assessment into four primary phases:

CMMC Assessment Process (CAP) — Four Phases

Phase 1 — Plan and Prepare:

- The C3PAO and the organization agree on assessment scope, schedule, and logistics.
- The organization provides the System Security Plan (SSP), network diagrams, asset inventory, and any existing POA&M.
- The C3PAO reviews pre-assessment documentation to develop the assessment plan — identifying which requirements will receive deeper scrutiny and how evidence will be examined.
- A kickoff meeting establishes the assessment team, point-of-contact structure, and communication protocols.

Phase 2 — Conduct Assessment:

- Assessors examine evidence for each of the 110 requirements using three assessment methods: examine (review documents and configurations), interview (speak with personnel who implement or manage controls), and test (observe or technically verify that controls function as described).
- Site visits (physical or virtual) allow assessors to inspect the actual environment — not just documentation about it.
- Assessors request additional evidence for any requirement where initial documentation is insufficient.

- Daily debriefs keep the organization informed of preliminary findings and give opportunities to provide clarifying evidence before the assessment closes.

Phase 3 — Report Findings:

- The C3PAO produces a formal assessment report documenting each requirement's finding (MET / NOT MET / NOT APPLICABLE) with the supporting rationale.
- For any NOT MET findings, the report identifies the specific evidence gap or control deficiency.
- If findings are within POA&M-eligible bounds (score ≥ 80, no non-deferrable gaps), a conditional certification can be issued pending POA&M closure.

Phase 4 — Close and Certify:

- The C3PAO submits assessment results to the DoD's eMASS system, which updates the organization's SPRS record.
- A full CMMC Level 2 Final Certification is issued when all 110 requirements are MET or a Conditional Certification is issued with an approved POA&M.
- The certification is valid for three years, after which a re-assessment is required.

6.3 The Three Assessment Methods — Examine, Interview, Test

The CAP specifies that assessors must use three distinct methods to gather evidence for each requirement. Organizations that prepare only for document review — and neglect interview preparation and live technical testing — consistently underperform in assessments. Understanding what each method involves is critical to comprehensive readiness.

Method	What Assessors Do	Common Evidence Requested	Preparation Implication
Examine	Review artifacts:	SSP (full), all 14 domain policies, network	Every claimed control must

	policies, procedures, SSP, configurations, logs, training records, diagrams, contracts, meeting minutes, ticket records	topology diagrams, configuration baselines, audit log samples, training completion records, incident reports, access control lists, media sanitization logs, background check records	be supported by a dated, accessible artifact. Verbal assurances without documentation are not evidence. The SSP must cross-reference each artifact so assessors can locate it quickly.
Interview	Speak with personnel who implement, manage, or oversee controls — not just the CISO. Assessors will ask employees at all levels about their understanding of and adherence to security procedures	System administrators (access control, patching, configuration management), security team (incident response, monitoring), HR (personnel security, onboarding/offboarding), end users (security awareness, CUI handling), senior leadership (program oversight, risk decisions)	All personnel who interact with in-scope systems should be briefed on what controls exist, why they exist, and how to describe them accurately. Inconsistent answers between an admin and a policy document are a red flag for assessors.
Test	Technically verify that controls function — not just that they are documented. Assessors may examine live	Live demonstration of MFA prompt, firewall rule review, log forwarding verification (does the SIEM actually receive logs from all in-scope systems?), encryption status of endpoints, vulnerability	Build a pre-assessment test checklist that mirrors what assessors will verify. Run it yourself — or have an RPO run it —

	system configurations, run queries against identity systems, review firewall rules, verify encryption state of devices, confirm MFA is enforced	scan results, network segmentation verification	before the assessment. Gaps found during testing are fixable; gaps found by the C3PAO are findings.

6.4 Who Is In Scope for the Assessment

One of the most consequential — and most frequently misunderstood — aspects of the assessment is scope. An assessment does not cover "your company." It covers your CMMC Assessment Scope: the specific set of assets, personnel, technology, and third parties that process, store, or transmit CUI, or that provide security functions protecting those assets. Getting scope right before the assessment begins is critical — scope set too broadly inflates cost and complexity; scope set too narrowly creates gaps that become findings or, worse, post-certification liabilities.

CMMC defines five asset categories. Three of them are unambiguously in scope for assessment; the other two have nuanced treatment:

Asset Category	Definition	In Assessment Scope?	Assessment Treatment
CUI Assets	Systems that directly process, store, or transmit CUI — workstations, file servers, email servers, cloud storage repositories,	Yes — fully in scope	All 110 requirements assessed against these assets. This is the core of the assessment environment.

	applications that handle CUI data		
Security Protection Assets (SPAs)	Systems that provide security functions protecting CUI assets — firewalls, intrusion detection systems, SIEM platforms, identity providers (Active Directory / Entra ID), endpoint protection platforms, MFA systems, privileged access management tools	Yes — fully in scope	SPAs are assessed against the same 110 requirements. An unpatched firewall protecting CUI is itself a material finding even if the firewall is not a CUI asset.
Contractor Risk Managed Assets (CRMAs)	Systems that can communicate with CUI assets but do not themselves process, store, or transmit CUI — a developer's personal laptop that is on the same network segment as CUI servers, a printer that could theoretically receive CUI print jobs	Partially — risk-managed by contractor	CRMAs must be documented and the contractor must demonstrate risk management for them. Assessors will review the CRMA list and the controls applied. They cannot simply be declared "out of scope" without a documented risk rationale.

Specialized Assets	Operational technology (OT), IoT devices, test equipment, government-furnished equipment (GFE) — assets that cannot feasibly implement all NIST 800-171 controls due to technical constraints	Yes — with exceptions	Assessed against purpose-specific criteria. Each specialized asset must be documented with a justification for any controls that cannot be implemented and compensating controls that mitigate the resulting risk.
Out-of-Scope Assets	Assets with no logical or physical path to CUI and no security protection function for CUI assets — a standalone invoicing system on an isolated network, a lobby kiosk with no enterprise connectivity	No — if boundary is defensible	Assessors will scrutinize the boundary between out-of-scope and in-scope assets. The segmentation must be real and verifiable, not just declared. Weak or undocumented segmentation converts out-of-scope assets to CRMAs or CUI assets.

6.5 MSPs, MSSPs, and Cloud Providers in the Assessment Scope

A critically important — and widely misunderstood — aspect of CMMC assessment scope is the treatment of external service providers. If you use a managed service provider, a managed

security service provider, or a cloud platform to handle, protect, or monitor your CUI environment, those providers' services are within your CMMC assessment scope. You cannot outsource compliance obligations by outsourcing the underlying function.

This principle has direct practical consequences. If your MSP manages your endpoints, patches your servers, and administers your identity platform, then the MSP's people and processes are part of your Security Protection Asset environment. The assessor will want to know: Is the MSP subject to a CMMC requirement themselves? How do you verify the MSP's security practices? What access does the MSP have to CUI or to systems that protect CUI, and how is that access controlled and logged?

Provider Type	Assessment Scope Implication	What Assessors Will Look For
MSP managing endpoints or servers in the CUI environment	The MSP's administrative access to your in-scope systems makes them a Security Protection Asset operator. Their people, tools, and processes are in scope.	Evidence of MSP background screening, contractual security requirements imposed on the MSP, log of MSP access to in-scope systems, MSP's own CMMC compliance status or equivalent controls, MFA enforcement for MSP remote access
MSSP providing SIEM / SOC / threat monitoring	The MSSP's monitoring platform is a Security Protection Asset. The MSSP personnel who respond to alerts from your environment are in scope.	Log forwarding configuration, MSSP access controls, contractual incident notification SLAs, evidence that MSSP alerts are reviewed and closed, MSSP's handling of CUI that may appear in log data
Cloud service provider hosting CUI workloads (e.g., Microsoft 365	The cloud platform is in scope, but FedRAMP authorization	FedRAMP authorization letter / ATO for the cloud platform, shared

GCC High, AWS GovCloud)	provides inherited control credit for the platform layer. Customer-configured controls remain the contractor's responsibility.	responsibility matrix documenting which controls are inherited vs. customer-managed, customer configuration settings (e.g., conditional access policies, retention settings, encryption configuration)
SaaS application used to process or store CUI (e.g., project management, document sharing)	The SaaS platform is in scope as a CUI asset. If it lacks FedRAMP authorization at the appropriate impact level, all controls must be implemented by the contractor.	FedRAMP status of the platform, data classification settings (does CUI flow into this app?), access control configuration, audit logging availability, encryption in transit and at rest
External IT consultant / contractor with access to CUI systems	Same as MSP — privileged access to in-scope systems makes the consultant's activities in scope.	Screening records, access authorization documentation, access logs, contractual CUI handling obligations, MFA for remote sessions

The External Provider Rule in Plain Language

If a company has access to your CUI or to systems that protect your CUI, they are in your assessment scope. You are responsible for demonstrating that their access is controlled, logged, and compliant — even if the provider is a large company with their own security program. "Our MSP handles that" is not a complete answer to an assessor. The complete answer is: "Our MSP handles that, here is our contract requiring compliant practices, here is the log of their access, and here is how we verify their controls."

6.6 Pre-Assessment Preparation — The Mock Assessment

The single most effective thing an organization can do to improve its assessment outcome is to conduct a thorough mock assessment — a full internal or RPO-led simulation of the C3PAO assessment using the official CAP methodology — before the real assessment begins. Organizations that invest in rigorous mock assessments pass their C3PAO assessments at dramatically higher rates and with fewer findings than those that rely solely on gap assessments and remediation.

A mock assessment is different from a gap assessment. A gap assessment identifies what controls are missing. A mock assessment assumes the controls are in place and asks: could we prove it to a skeptical third-party examiner using the same methods (examine, interview, test) they would use? The answer is often "not yet" — even for organizations with genuinely good security programs — because the evidence is there but not organized, or the staff can implement the controls but cannot articulate them clearly in an interview.

Pre-Assessment Activity	What It Tests	Why It Matters
Full SSP walk-through	Does the SSP accurately describe how every control is implemented? Are all 110 requirements addressed with sufficient specificity? Are cross-references to evidence correct?	The SSP is the first thing assessors read. An SSP that is vague, outdated, or inconsistent with the actual environment creates skepticism that colors the entire assessment.
Evidence library audit	Is there a specific, dated artifact supporting every MET claim in the SSP? Are artifacts organized so they can be located and presented within minutes?	Assessors have limited time. If you cannot produce evidence quickly when asked, they may score the requirement NOT MET rather than wait for a multi-day evidence search.

Interview simulation	Can your system admins, security team, HR, and end users describe their security responsibilities accurately and consistently with the SSP?	Conflicting statements between an employee interview and the SSP narrative are a major red flag. Pre-assessment coaching ensures everyone speaks the same accurate language.
Technical testing	Run the same technical checks assessors will run: MFA enforcement, log forwarding gaps, encryption state, firewall rule review, patch compliance status, network segmentation validation.	Technical findings are the hardest to remediate quickly. Finding them in a mock gives you time to fix them before the real assessment.
Scope boundary verification	Walk the network boundary between in-scope and out-of-scope assets. Is the segmentation documented and verifiable? Are there any surprise pathways from out-of-scope to in-scope systems?	Scope creep discovered during assessment — an uncatalogued system that turns out to have CUI access — can invalidate large portions of the assessment and require a scope re-do.
POA&M review	Is the POA&M current? Are all open items still accurate? Have any target dates passed without closure? Are all open items eligible for deferral (non-deferrable controls must be closed)?	An assessor reviewing a POA&M with expired dates and unclosed non-deferrable items will view the organization as lacking commitment to remediation — the opposite of the message you want to send.
Provider documentation check	Do you have contracts, access logs, and compliance evidence for every MSP, MSSP,	Provider documentation gaps are one of the most common surprise

	and cloud provider in scope?	findings at assessment. Contracts that lack security requirements, or access logs that were never configured, are easily fixed in advance and extremely hard to explain after the fact.

6.7 Assessment Timeline Planning

Organizations chronically underestimate the calendar time required to schedule and complete a CMMC Level 2 assessment. The combination of C3PAO availability constraints, documentation preparation time, and the assessment execution period itself means that contractors who wait until a contract award deadline is imminent will almost always miss it. The following timeline represents realistic planning horizons for a mid-size organization starting from a reasonably mature security posture.

Timeline Before Contract Award	Activity
18–24 months	Gap assessment and remediation roadmap. Begin technology remediation for major gaps (cloud migration, MFA deployment, SIEM implementation).
12–18 months	SSP and policy package development. Begin evidence collection framework. Complete technology remediation.
9–12 months	Internal mock assessment (first pass). Identify remaining documentation and evidence gaps.
6–9 months	RPO-led readiness review (external mock assessment). Remediate findings. Book C3PAO assessment slot — C3PAOs are booking 3–6 months out in many markets.
3–6 months	Final evidence library preparation. Interview coaching for key personnel. Provider

	documentation verification. Confirm assessment logistics with C3PAO.
0–3 months	C3PAO assessment execution (typically 1–4 weeks). Address any requests for additional evidence during assessment. Receive findings report.
Post-assessment	Close any POA&M items within 180-day window. Monitor for certification upload to eMASS / SPRS.

Recommendation — Do Not Self-Assess Your Mock Assessment

The most valuable mock assessments are conducted by someone other than the team that built the compliance program. Internal teams are blind to their own gaps — not from negligence, but because familiarity with the environment creates assumptions about what an outsider would see. An RPO or independent CMMC professional conducting the mock assessment will find gaps that internal reviewers miss every time.

At minimum, have personnel outside the security team conduct the interview simulation. An assessor interviewing a system administrator will ask basic questions that sound simple — "Walk me through what happens when a new employee needs access to a CUI system" — and a well-prepared admin will answer accurately and completely. An unprepared admin will describe what they think happens, which may not match the policy, which will not match the SSP, and the assessor will have three conflicting accounts of the same control.

Chapter 7: SPRS and the Submission Process

7.1 What Is SPRS?

The Supplier Performance Risk System (SPRS) is the DoD's authoritative enterprise application for collecting, processing, and displaying supplier and product performance information. It serves as the official repository where defense contractors submit their NIST SP 800-171 self-assessment scores and affirm their CMMC compliance status.

Before a company can be awarded most DoD contracts or subcontracts, it must have a current, valid entry in SPRS. For contracts subject to DFARS 252.204-7012, this means submitting a NIST SP 800-171 assessment score. For contracts subject to CMMC requirements, it means having either a valid self-assessment affirmation or a C3PAO-issued certification recorded in the system.

7.2 The NIST SP 800-171 Scoring Methodology

The scoring methodology for NIST SP 800-171 self-assessments was standardized by DoD in its "NIST SP 800-171 DoD Assessment Methodology" document. The system works as follows:

- The maximum score is 110 points, representing full implementation of all 110 requirements.
- Each requirement is assigned a point value based on its importance (1, 3, or 5 points).
- For each requirement that is NOT fully implemented, the point value is subtracted from 110.
- The resulting score ranges from 110 (fully compliant) to as low as -203 (nothing implemented).
- A negative score is mathematically possible because some requirements have higher point values.

Scoring Example
Maximum possible score: 110 points

If requirement 3.5.3 (Multi-Factor Authentication) is not implemented: -5 points
If requirement 3.13.8 (Encrypt CUI in Transit) is not implemented: -5 points
If requirement 3.3.1 (Audit Logs) is not implemented: -3 points

Running score after these three gaps: 110 − 5 − 5 − 3 = 97

Note: A score of 97 is not "97% compliant" — it means those specific controls are missing.
The DoD and primes will look at both the score AND which specific requirements are unmet.

7.3 Three Assessment Confidence Levels

DoD distinguishes three "confidence levels" for CMMC/NIST assessments, which affect how much weight contracting officers give to a submitted score:

Confidence Level	Who Conducts	Verification Method	Typical Use
Basic	Organization itself (self-assessment)	Internal review by company personnel	Level 1 (annual); Level 2 non-prioritized
Medium	Organization + DCSA DIBCAC spot check	DoD spot-check of self-assessment documentation	Transitional / interim before C3PAO assessment
High	Certified Third-Party Assessor (C3PAO)	Independent review of evidence by trained assessors	Level 2 prioritized contracts; Level 3 programs

7.4 Step-by-Step SPRS Submission Process

Submitting your NIST SP 800-171 assessment to SPRS involves the following steps:

11. Register in SAM.gov: Your organization must have an active registration in the System for Award Management (SAM.gov)

with a current Unique Entity Identifier (UEI). SPRS access is linked to SAM.gov registration.

12. Conduct the Assessment: Perform a comprehensive internal assessment of all 110 NIST SP 800-171 requirements against your in-scope environment. Document evidence for each requirement (Met, Partially Met, or Not Met).
13. Calculate Your Score: Using the DoD scoring methodology, calculate your total score. Document which specific requirements are not met and why.
14. Update the SSP: Ensure your SSP reflects the current assessment results. Update any requirements that have changed status since your last SSP review.
15. Update the POA&M: For any requirements that are not fully met, ensure they are documented in your POA&M with realistic target remediation dates.
16. Senior Official Affirmation: A company official — typically the CEO, CIO, or CISO — must formally affirm the accuracy of the assessment. This affirmation carries potential False Claims Act liability.
17. Access SPRS: Navigate to sprs.apps.mil. You will need a DoD-approved PKI certificate or Common Access Card (CAC) to log in, or your account must be registered through the appropriate access management portal.
18. Submit Assessment: Enter your NIST SP 800-171 assessment date, score, and plan of action details. The system will prompt for the assessment date, method (self/C3PAO), and score.
19. Record Keeping: Retain all assessment documentation, evidence, and SSP/POA&M for a minimum of three years (or longer if required by contract).

7.5 What Happens After Submission

Once your SPRS submission is complete, it becomes visible to DoD contracting officers and prime contractors through the system. When bidding on contracts, the contracting officer will verify your SPRS record. If you do not have a current record, or if your score is

very low without a credible POA&M, the contracting officer may assess your proposal as non-compliant.

Prime contractors evaluating subcontractors will similarly check SPRS records as part of supply chain risk management. A sub with a strong SPRS score gains competitive advantage in source selection for CUI-handling subcontracts.

SPRS scores must be updated whenever your security posture changes significantly — either improving (as you remediate gaps) or declining (if controls are removed or degrade). DoD guidance is to keep the SPRS record current and accurate at all times. Submitting an inaccurate score knowingly constitutes a False Claims Act violation with potential penalties of up to three times the value of contracts received on the basis of the false claim.

7.6 Minimum Score for POA&M Eligibility

A POA&M is not a blank check. The CMMC 2.0 Final Rule (32 CFR § 170.21) establishes that a company can receive a conditional CMMC Level 2 certification — allowing contract award to proceed — while carrying open POA&M items, but only if two hard conditions are met simultaneously: the SPRS score must be at or above the minimum threshold, AND none of the open items may fall on the list of non-deferrable requirements.

The minimum SPRS score required to receive a conditional certification with an open POA&M is 80 out of 110. A score below 80 means the organization cannot receive even a conditional certification — it must remediate further before being eligible for award on contracts requiring CMMC Level 2. This threshold represents the DoD's judgment that a company scoring below 80 has too many gaps across too many domains to be trusted with CUI, regardless of the remediation plan it presents.

The 80-Point Floor at a Glance

Score = 110	→	Full certification. No POA&M needed.
Score 80 – 109	→	Conditional certification permitted. POA&M required; all open items must be non-deferrable-eligible AND

closed within 180 days of conditional certification date.
Score below 80 → No certification. Contract award blocked until score is raised to at least 80 through actual remediation.

Note: Even a score of 80 with a POA&M is a business risk. Primes and contracting officers can and do use SPRS scores as a competitive factor. A score of 80 on a prioritized acquisition sends a signal that should be remediated as quickly as possible.

7.7 Non-Deferrable Controls — The Non-Negotiables

Certain NIST SP 800-171 requirements are so foundational to the security of CUI that the DoD will not allow them to be deferred to a POA&M under any circumstances. These controls must be fully implemented and evidenced before a C3PAO assessor can issue even a conditional Level 2 certification. They represent the absolute minimum security floor below which the DoD considers a contractor's environment unsafe for CUI regardless of any planned remediation.

The following table lists the non-deferrable requirements as specified in 32 CFR § 170.21(c) and the accompanying CMMC Assessment Process (CAP) documentation. Organizations should treat these as the first controls to implement — before any others — and should never allow them to lapse.

Requirement	Domain	Description	Why Non-Deferrable
3.1.20	Access Control (AC)	Verify and control/limit connections to external systems	Uncontrolled external connections are the most common initial intrusion vector; no environment is safe without this boundary control
3.1.22	Access Control (AC)	Control CUI posted or	CUI exposed on public-facing

		processed on publicly accessible systems	systems is an immediate, unacceptable disclosure
3.5.3	Identification & Authentication (IA)	Use multi-factor authentication for local and network access to privileged accounts and CUI systems	MFA is the single highest-impact control against credential theft — the leading attack method against DIB networks
3.5.4	Identification & Authentication (IA)	Employ replay-resistant authentication mechanisms	Without replay resistance, captured authentication tokens can be reused by adversaries indefinitely
3.6.1	Incident Response (IR)	Establish an operational incident-handling capability	Without IR capability the 72-hour DoD reporting requirement (DFARS 252.204-7012) cannot be met, creating immediate regulatory breach
3.6.2	Incident Response (IR)	Track, document, and report incidents to DoD	Active reporting obligation — failure is an independent DFARS violation separate from CMMC non-compliance
3.12.3	Security Assessment (CA)	Monitor security	Continuous monitoring is the mechanism

		controls on an ongoing basis	that keeps all other controls functioning; without it degradation is undetectable
3.13.8	System & Communications Protection (SC)	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission	Unencrypted CUI in transit is a de facto disclosure — adversaries capable of passive interception do not need to breach endpoints
3.13.10	System & Communications Protection (SC)	Establish and manage cryptographic keys when cryptography is employed	Weak or unmanaged key practices undermine the encryption controls that depend on them
3.13.16	System & Communications Protection (SC)	Protect the confidentiality of CUI at rest	CUI on unencrypted storage is vulnerable to physical theft, insider exfiltration, and ransomware staging
3.14.6	System & Information Integrity (SI)	Monitor organizational systems to detect attacks and indicators of potential attacks	Threat detection is the prerequisite for any meaningful incident response; blind environments cannot contain breaches

Practically speaking, if a gap assessment reveals that any of these eleven requirements is not implemented, your organization's first priority should be closing those gaps before anything else. Attempting to schedule a C3PAO assessment before resolving non-deferrable gaps is a guaranteed path to assessment failure — and to the cost of paying for a second assessment once remediation is complete.

Quick Remediation Priority Order
1. Non-deferrable controls (above) — must be complete before assessment.
2. High-point-value controls (5-pt items) — each gap costs the most SPRS points.
3. Controls that appear across multiple contract types — broader risk exposure.
4. Remaining controls by domain, working through POA&M with 180-day deadline.

Use your POA&M as a sequenced remediation plan, not a parking lot. Assessors look at whether your target dates are realistic and your resource commitments are credible — not just whether items are listed.

7.8 The False Claims Act Exposure

The Justice Department has made clear that it views CMMC and DFARS cybersecurity compliance as a False Claims Act (FCA) enforcement priority. Under the FCA, knowingly submitting false claims to the government — including false certifications of compliance — exposes companies and their officers to treble damages plus civil penalties per false claim. The government's Civil Cyber-Fraud Initiative, launched in 2021, has already produced FCA settlements involving defense contractors who misrepresented their cybersecurity posture.

This enforcement context means that CMMC compliance is not merely a matter of winning contracts — it is a matter of corporate liability. The senior official who signs the SPRS affirmation should be fully briefed on the legal exposure and should have genuine confidence in the accuracy of the underlying assessment.

Chapter 8: Available Services and Tools

8.1 The CMMC Ecosystem

A substantial and rapidly growing ecosystem of organizations and products has emerged to help defense contractors navigate CMMC compliance. Understanding the different categories of providers — and the distinct roles they play — is essential for making smart sourcing decisions. Choosing the wrong type of provider for a given need can result in wasted investment, compliance gaps, or assessment failures.

8.2 C3PAOs — Certified Third-Party Assessment Organizations

C3PAOs are organizations authorized by the CMMC Accreditation Body (Cyber AB) to conduct official CMMC Level 2 assessments. They employ Certified CMMC Assessors (CCAs) and Certified CMMC Professionals (CCPs) who have passed required training and background checks. Only a C3PAO can issue a CMMC Level 2 certification that satisfies the assessment requirement for prioritized acquisitions.

Key points about C3PAOs:

- C3PAOs must be authorized by the Cyber AB and listed in the CMMC marketplace (cyberab.org).
- A C3PAO that has helped you prepare for assessment cannot conduct your assessment — there is a conflict-of-interest prohibition.
- Assessment duration typically ranges from one to several weeks, depending on organization size and complexity.
- Assessment costs vary widely but typically range from $20,000 to over $200,000 depending on scope.
- C3PAOs submit assessment results to the DoD's eMASS system, which updates your SPRS record.

8.3 RPOs — Registered Provider Organizations

Registered Provider Organizations (RPOs) are companies that have been listed in the Cyber AB marketplace as organizations capable of providing CMMC advisory and implementation services. They employ Certified CMMC Professionals (CCPs) and/or Certified CMMC Assessors (CCAs).

Importantly, RPO status does not mean a company is authorized to conduct official CMMC assessments. RPOs help companies prepare for assessments — conducting gap analyses, building SSPs, implementing controls, developing policies, and providing readiness reviews — but the actual certification assessment must be conducted by a C3PAO (for Level 2) or DCMA DIBCAC (for Level 3).

When selecting an RPO, evaluate:

- Number of CCPs and CCAs on staff and their availability for your engagement
- Experience with organizations similar to yours in size and sector
- Ability to provide implementation support, not just advisory services
- Track record of clients who have successfully passed C3PAO assessments
- Pricing model (fixed-fee vs. time and materials) and scope clarity

8.4 Managed Service Providers (MSPs) and MSSPs

Many defense contractors — particularly small and mid-size businesses — lack the internal IT staff to implement and sustain the technical controls required by NIST SP 800-171. Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) fill this gap by taking on ongoing responsibility for specific technology functions.

There are important distinctions between general MSPs and those with genuine CMMC expertise. A general commercial MSP may handle your email and helpdesk adequately but lack the specialized knowledge to configure systems in compliance with NIST SP 800-

171. CMMC-focused MSPs understand the specific control requirements, maintain their own compliance posture (often requiring them to be assessed as well), and can provide documentation artifacts needed for your SSP.

Service Type	What They Provide	CMMC Role	Considerations
MSP	Managed IT (helpdesk, patching, device management)	Technical control implementation	Must understand CMMC requirements for services touching CUI
MSSP	Security operations: SIEM, threat detection, IR	Controls for AU, IR, SI domains	Must provide CMMC-specific logging and reporting
Cloud MSP	CMMC-compliant cloud hosting (Microsoft GCC High, AWS GovCloud)	FedRAMP-authorized environment for CUI	Understand shared responsibility model
RPO-MSP hybrid	Both advisory/implementation AND ongoing managed services	End-to-end CMMC partner	Watch for conflicts; ensure clear scope

8.5 GRC Platforms

Governance, Risk, and Compliance (GRC) platforms help organizations manage their CMMC program documentation, track control implementation, and prepare for assessments. The CMMC GRC tool market has grown substantially, with platforms ranging from general-purpose enterprise GRC tools adapted for CMMC to purpose-built CMMC-specific platforms.

Features to look for in a CMMC GRC platform:

- Pre-built NIST SP 800-171 control library with scoring methodology
- SSP generation and management capabilities
- POA&M tracking with milestone management

- Evidence collection and attachment features for each control
- SPRS score calculator and export functionality
- Policy template libraries
- Multi-user collaboration with role-based access
- Audit trail for assessment activities
- Integration with vulnerability scanners and SIEM platforms
- Reporting dashboards for executive visibility

8.6 AI-Native CMMC Services

The newest category of CMMC tools applies artificial intelligence — particularly large language models (LLMs) and AI-powered automation — to the compliance challenge. AI-native CMMC services represent a significant advance over traditional GRC platforms in several areas:

- Automated Gap Analysis: AI can analyze configuration files, system logs, and existing documentation to identify control gaps far more rapidly than manual review.
- Policy Generation: LLM-based tools can draft initial policy and procedure documents tailored to the organization's environment, dramatically reducing the time required to produce the documentation artifact set.
- SSP Drafting Assistance: AI assistants can guide personnel through SSP development, prompting for required information and generating compliant narrative descriptions of control implementations.
- Evidence Mapping: AI tools can analyze evidence artifacts (configuration screenshots, log exports, training records) and map them to specific NIST SP 800-171 requirements, reducing the manual burden of evidence organization.
- Continuous Compliance Monitoring: AI-powered systems can continuously monitor configuration state against CMMC requirements and alert on drift in near-real time.
- Assessment Prep: AI can simulate assessor questions and review documentation for common deficiencies before a C3PAO assessment.

The AI-native compliance market is evolving rapidly. When evaluating AI-based CMMC tools, assess whether the underlying AI has been trained or fine-tuned on current CMMC documentation (not just generic cybersecurity content), whether the vendor has CMMC subject matter expertise on staff to validate AI outputs, and whether the tool provides verifiable evidence artifacts rather than AI-generated attestations that cannot be substantiated.

8.7 Cloud Service Provider Compliance Environments

Where you store and process CUI matters enormously under CMMC. Using a FedRAMP-authorized cloud environment that is compliant with DoD security requirements can satisfy a large number of NIST SP 800-171 requirements through the CSP's existing authorization — provided you understand the shared responsibility model.

Cloud Environment	FedRAMP Level	CUI Suitability	Notes
Microsoft 365 GCC High	High	Authorized for CUI (ITAR/DoD)	Most common choice for DoD contractors
AWS GovCloud (US)	High	Authorized for CUI	IaaS platform; customer configures most controls
Azure Government	High	Authorized for CUI	Broad service catalog; DoD IL4/IL5 authorizations
Microsoft 365 GCC	Moderate	Suitable for most CUI	Lower cost than GCC High; some CUI types require GCC High
Standard Commercial Cloud	None/Low	NOT suitable for CUI	Using standard commercial cloud for CUI is a material control failure

Chapter 9: The Future of CMMC

9.1 The CMMC Implementation Timeline

The full rollout of CMMC into DoD contracting is happening in phases. The October 2024 final rules established the legal framework; the implementation into actual contract solicitations has been phased to allow the C3PAO ecosystem time to scale and to give contractors adequate lead time. Key milestones in the expected timeline include:

Period	Milestone
Oct 2024	CMMC 2.0 Final Rule published (32 CFR Part 170 and DFARS companion rule)
2025 (Phase 1)	Selected DoD contracts begin including CMMC requirements; assessors ramp up
2026 (Phase 2)	Broader inclusion in new solicitations; all new CUI contracts expected to include CMMC clause
2027 (Phase 3)	Full implementation across all applicable DoD contracts and re-competes
2028+	Steady-state: triennial re-assessments cycle for first cohort of certified companies

9.2 Expected Evolution of the Standard

CMMC is not a static framework. The NIST standards it builds upon — SP 800-171 and SP 800-172 — are updated periodically as the threat landscape evolves. NIST SP 800-171 Revision 3, finalized in 2024, reorganized and updated many requirements, adding new controls in areas like supply chain risk management and organizational risk management. The DoD is expected to align CMMC with Revision 3 in a future rulemaking.

Organizations should monitor for updates to the CMMC standard and plan for the transition effort when revisions are published. The transition period from SP 800-171 Rev 2 (current CMMC basis) to

Rev 3 will require SSP updates, gap reassessment, and potential remediation of new or modified requirements.

9.3 International and Reciprocity Considerations

The United States is not alone in grappling with defense supply chain cybersecurity. Allied nations — particularly those in the Five Eyes intelligence sharing community (UK, Canada, Australia, New Zealand) — have developed or are developing parallel frameworks. The UK's Cyber Essentials Plus program, Canada's Protected B / Medium Integrity / Medium Availability (PBMM) standard, and Australia's Essential Eight framework each address overlapping concerns.

DoD has expressed interest in reciprocity — the idea that a contractor certified under one framework might receive credit under another, reducing duplicative assessment burden. Some reciprocity exists today between CMMC and the Federal Risk and Authorization Management Program (FedRAMP), with CMMC giving credit for FedRAMP-authorized cloud services. Broader international reciprocity remains aspirational.

9.4 AI and the Future of Cybersecurity Compliance

Artificial intelligence is transforming both the threat landscape that CMMC is designed to address and the tools available to achieve and sustain compliance. On the threat side, AI-powered attacks are enabling adversaries to conduct reconnaissance, generate spear-phishing content, and identify vulnerabilities at scales previously impossible. This dynamic threat environment will exert upward pressure on CMMC requirements over time.

On the compliance side, AI is reducing the cost and increasing the accuracy of CMMC program management. Future CMMC programs will increasingly rely on AI-powered continuous monitoring platforms that can detect control drift in real time, AI-assisted evidence collection that reduces manual assessment prep burden, and automated compliance reporting that keeps SPRS records current without manual intervention.

The DoD is also exploring the use of automated assessment tools that could supplement or in some cases replace manual C3PAO assessments for specific control domains — particularly configuration management, where automated scanning can provide high-confidence evidence of compliance at scale.

9.5 Expanding Scope: Beyond DoD

CMMC's influence is already spreading beyond its DoD origins. Other federal agencies are watching CMMC carefully as a model for their own contractor cybersecurity requirements. The Department of Energy, the Intelligence Community, and the Department of Homeland Security have each signaled interest in similar frameworks. Some analysts expect a whole-of-government approach to contractor cybersecurity requirements to emerge in the coming years, potentially using CMMC or a CMMC-derivative as the foundation.

For defense contractors, this trajectory suggests that the investment in CMMC compliance is not merely a DoD-specific cost — it is an investment in a cybersecurity posture that will increasingly be required across the federal contracting landscape.

Chapter 10: Common Pitfalls

10.1 Scoping Too Broadly (or Too Narrowly)

Scoping errors are among the most costly mistakes in CMMC programs. Organizations that scope too broadly include systems with no path to CUI, inflating their in-scope asset count and driving up implementation and assessment costs unnecessarily. Organizations that scope too narrowly exclude systems that actually do process, store, or transmit CUI — a much more serious problem that can result in assessment failure, required remediation, and contractual penalties.

Common narrow-scoping mistakes include: treating email servers as out of scope when CUI is routinely shared via email; excluding shared drives where employees store CUI alongside non-CUI files; and failing to include laptops used by remote workers who access CUI systems from home.

10.2 Misidentifying CUI

Many organizations do not know what CUI they have, where it lives, or how it flows through their systems. This is not laziness — CUI identification is genuinely difficult when the information arrives from government customers without proper markings (which happens frequently) and when employees have not been trained to recognize it.

The consequence of misidentifying CUI — treating it as ordinary business information and storing it on unprotected systems — is exactly the kind of control failure that CMMC is designed to prevent. Organizations should invest in data discovery tooling and employee training to build reliable CUI identification processes.

10.3 Treating CMMC as a One-Time Project

As emphasized in Chapter 5, CMMC is a continuous program, not a project with a completion date. Organizations that achieve certification and then reduce their cybersecurity investment — cutting security staff, deferring patching, letting policies go stale —

will face control failures long before their next triennial assessment. Controls erode. People leave. Configurations drift. New systems are added to scope without review.

10.4 Documentation Gaps

C3PAO assessors cannot give credit for controls they cannot verify. A technically well-implemented security control with no supporting documentation — no policy requiring it, no procedure describing it, no configuration baseline capturing it, no training records showing people know how to follow it — may not receive credit in an assessment. Documentation is not bureaucratic overhead; it is the evidence that turns technical implementations into verifiable controls.

The most frequently missing documentation artifacts include:

- System Security Plan (insufficient detail, not updated, not approved)
- Configuration baselines (referenced in policy but never actually created)
- Media sanitization records (process exists but individual disposal records not kept)
- Personnel security files (background check results, access authorization records)
- Incident response test records (plan exists but never exercised)
- Audit log review records (SIEM in place but no evidence of regular review)

10.5 Inadequate Vendor and Cloud Management

Many organizations route CUI through cloud services, managed service providers, and software-as-a-service platforms without considering whether those platforms satisfy CMMC requirements. Using a consumer-grade file sharing service (Dropbox, Google Drive standard tier) to store CUI is a clear violation. Using an unvetted SaaS platform that lacks FedRAMP authorization is a common and costly mistake.

Every external service that processes, stores, or transmits CUI is a potential scope addition and must be evaluated for compliance. If the service is not FedRAMP-authorized at the appropriate impact level, your organization is responsible for implementing compensating controls — or finding a compliant alternative.

10.6 Over-Reliance on Self-Assessment

The ability to self-attest for some Level 2 contracts has led some organizations to conduct superficial assessments that bear little relationship to actual security posture. Checkbox compliance — marking requirements as "Met" based on a quick read of the requirement language without actually gathering evidence — produces inaccurate SPRS scores and false confidence.

Self-assessments should be conducted with the same rigor as an external assessment. Use the DoD's NIST SP 800-171 Assessment Methodology document as your guide, gather evidence for each requirement, and have someone other than the control implementer review the evidence. Consider engaging an RPO to conduct a readiness review before finalizing your self-assessment results.

10.7 Underestimating Cost and Timeline

Organizations routinely underestimate both the cost and the time required to achieve CMMC compliance. The most common planning errors include:

- Assuming a gap assessment alone costs a few thousand dollars (it typically costs $15,000–$75,000 for a thorough external assessment)
- Budgeting for technology but not for the ongoing personnel and process costs
- Expecting to achieve Level 2 compliance in a few months (realistic timelines range from 6 to 24 months depending on starting posture)
- Not accounting for the cost of migrating to CMMC-compliant cloud environments

- Underestimating the time required to produce quality documentation artifacts
- Not planning for assessment scheduling lead times (C3PAO availability can require 6+ months of advance booking)

Rough Budget Reference — Level 2 Compliance (Mid-Size Contractor, 100 Employees)

Gap Assessment (external RPO):	$25,000 – $75,000
Technology Remediation (MFA, endpoint, SIEM):	$50,000 – $300,000
Policy/SSP Documentation (RPO or internal):	$15,000 – $50,000
C3PAO Assessment:	$30,000 – $150,000
Ongoing Managed Security Services (annual):	$60,000 – $200,000

Total first-year investment range: $180,000 – $775,000
Actual costs vary significantly based on scope, starting posture, and cloud environment choices.

10.8 Ignoring the Human Element

Cybersecurity is fundamentally a human problem. The most sophisticated technical controls can be undermined by a single employee who clicks a phishing link, stores CUI on a personal device for convenience, shares credentials, or bypasses a security control because it is inconvenient. CMMC programs that invest heavily in technology but neglect security culture and awareness training consistently underperform in real-world incidents and assessments alike.

Effective security awareness programs go beyond annual "check the box" training. They include phishing simulations, role-specific training for privileged users, CUI handling training for everyone who touches sensitive information, and a security-aware culture where employees feel empowered to report potential incidents without fear of blame.

Chapter 11: Business Considerations — The True Cost of CMMC and the Price of Not Complying

11.1 The November 2025 Phase 1 Deadline and What It Means for Renewal

CMMC requirements are being phased into DoD contracts in waves. Phase 1, which began in late 2025, requires a subset of new solicitations and contract awards to include the CMMC clause (DFARS 252.204-7021). The pace accelerates through 2026 and 2027 as the DoD expands CMMC requirements across the full portfolio of applicable contracts. By 2027, the expectation is that essentially all new DoD solicitations requiring CUI handling will include the CMMC clause.

The mechanism that catches most contractors off guard is not new contract awards — it is contract renewals and option-year exercises. Every major DoD contract has option years. When those options come up for exercise, the contracting officer will increasingly include or re-certify CMMC requirements. A contractor that has been performing on a contract for five years without a CMMC issue could find itself ineligible to continue at the next option exercise because it cannot demonstrate the required certification.

This renewal risk is asymmetric. The contractor has already invested years building institutional knowledge, staffing the program, and developing customer relationships. Losing that work — not to a competitor who out-bid them, but to a compliance failure — is one of the most costly and preventable business outcomes in the DIB today. The cost of CMMC certification, seen in this light, is not a new expense — it is the price of protecting revenue that the contractor has already earned and expects to continue.

The Renewal Risk in Numbers
Consider a defense contractor with $5M/year in DoD contract revenue across three contracts, each with two option years remaining. Total DoD revenue at risk: $30M over the remaining option periods. The cost of CMMC Level 2 certification for a company this size: $250,000–

$500,000 over three years. The math is unambiguous: the certification investment represents 1.7%–1.6% of the revenue it protects. Not investing is not cost savings — it is a bet that regulatory enforcement will not catch up before the options expire. Increasingly, that is a bet contractors are losing.

11.2 What CMMC Certification Actually Costs

One of the most common mistakes organizations make when approaching CMMC is dramatically underestimating the true cost. They think about the C3PAO assessment fee — which is visible and easy to quote — and ignore the substantially larger investment required to build, remediate, and sustain the program that makes certification possible. The following breakdown, drawn from Espresso Labs' analysis of actual DIB compliance engagements (espressolabs.com/resources/cmmc/how-much-does-cmmc-cost/), reflects the full cost picture.

Phase	What It Covers	Typical Cost Range
1. Preparation & Gap Analysis	External gap assessment against all 110 NIST SP 800-171 requirements; scoping analysis; SPRS score calculation; risk-prioritized remediation roadmap; SSP and POA&M baseline	$40,000 – $100,000
2. Policy & Documentation Development	All 14 domain policies and procedures; SSP development; evidence framework; CUI handling procedures; personnel security documentation	$10,000 – $50,000
3. Technical Implementation	MFA deployment; endpoint encryption; SIEM/log aggregation; network segmentation;	$150,000 – $500,000

	vulnerability scanning; cloud migration to GCC High or equivalent; endpoint management; backup and recovery controls	
4. C3PAO Assessment	Formal third-party assessment by a Cyber AB-authorized C3PAO; assessment preparation support; assessor travel or remote logistics; findings review and POA&M negotiation	$30,000 – $100,000+
5. Continuous Compliance (annual)	Ongoing vulnerability management; continuous monitoring; SIEM operations; annual policy reviews; security awareness training; SPRS score maintenance; re-assessment preparation; incident response capability	$50,000 – $100,000+ per year
Three-Year Total Cost of Ownership	Initial certification + two years of continuous compliance maintenance + re-assessment in Year 3	$450,000 – $750,000+

11.3 The Hidden Costs Most Contractors Miss

The figures above represent the direct, foreseeable costs. In practice, many contractors encounter additional costs they did not anticipate when they began their CMMC journey. Being aware of these hidden costs allows for more accurate budgeting and avoids the "compliance surprise" that has derailed programs that appeared well-funded.

- Personnel costs: Building a full in-house security and compliance team — a CISO ($175,000–$250,000/year), a compliance analyst, and a security engineer — costs well over $400,000 annually in personnel expense alone, before any assessment fees or technology costs. Most small and mid-size DIB contractors cannot staff this internally.
- Cloud migration costs: Contractors storing CUI in standard commercial Microsoft 365 or Google Workspace must migrate to FedRAMP-authorized environments (Microsoft 365 GCC High, AWS GovCloud, etc.). Licensing premiums, data migration effort, and retraining costs are frequently underestimated.
- Scope creep costs: Organizations that discover mid-assessment that their CUI environment is larger than scoped — a common finding — face emergency remediation on assets that were never budgeted for inclusion.
- Re-assessment costs after POA&M: Contractors who receive a conditional certification with a POA&M must close all items within 180 days and may need to pay for a supplemental C3PAO review of remediated controls — an additional cost not included in the initial assessment quote.
- Productivity drag: Security controls — MFA, endpoint restrictions, data loss prevention — add friction to day-to-day operations. The productivity cost of implementing strong security is real, particularly during the transition period, and is virtually never included in compliance budgets.
- Training and culture change: Security awareness training, role-specific CUI handling training, and the organizational change management required to make new security procedures stick represent costs that are easy to underestimate and have long tails.

11.4 Cost Drivers — Why Two Similar Companies Can Have Very Different Bills

CMMC compliance costs are highly variable because they depend on factors that differ significantly even between organizations of similar size. Understanding the key cost drivers allows organizations to take

proactive steps to reduce their exposure before committing to an approach.

Cost Driver	Lower-Cost Scenario	Higher-Cost Scenario	Potential Impact
CUI scope size	CUI confined to a small, well-segmented environment (dedicated workstations, segregated network segment)	CUI flows freely across the entire enterprise network, reaching hundreds of devices	20–60% cost difference depending on in-scope asset count
Existing NIST 800-171 maturity	Organization already implemented DFARS 252.204-7012 controls in good faith; high SPRS score already achieved	Little to no prior implementation; SPRS score is very low or was never submitted	Existing mature programs may spend 50–70% less on remediation
Technology stack	Already using Microsoft 365 GCC High; existing endpoint management; SIEM already in place	All commercial tools; no centralized endpoint management; no logging infrastructure	Technology gap can add $100,000–$300,000 in infrastructure investment
Workforce distribution	Single office; all employees on-site; controlled physical environment	Remote or distributed workforce; employees in multiple states; BYOD environment	Remote access controls, VPN, and BYOD remediation add significant complexity and cost
Organization size	Under 50 employees; limited in-scope systems; simple network architecture	Over 500 employees; multiple sites; complex IT environment	Larger organizations may spend 50–300% more than comparable

			smaller organizations
Consultant vs. internal	Engaged RPO early; used managed services to fill security gaps efficiently	Attempted to build entirely in-house; hired expensive consultants late after failed self-assessment	Late-stage consulting engagements to rescue failing programs often cost 2–3× what early engagement would have

11.5 The Competitive Advantage Argument

Cost conversations about CMMC focus almost exclusively on the expense side of the ledger. The revenue and competitive opportunity side is equally important — and for many contractors, it represents a larger number.

The defense industrial base is undergoing a structural consolidation driven by CMMC. Contractors who cannot or will not achieve certification are being filtered out of the bidding pool for an expanding category of DoD work. This is not a gradual trend — it is an accelerating one. The contractors who achieve certification early are not just protecting their existing revenue. They are positioning themselves to capture work from competitors who could not meet the bar.

The Competitive Landscape Is Thinning
An estimated 40–60% of current DIB participants are not on track to achieve CMMC Level 2 certification by the time their contracts come up for renewal. For the contractors who are certified, this is not a crisis — it is a market opportunity. Every competitor who taps out of the DIB due to compliance costs or complexity represents contracts that must be awarded to someone else. That someone else will be a certified contractor.

Being CMMC Level 2 certified — especially with a high SPRS score — becomes a visible differentiator in source selection. Prime contractors performing supplier risk management are actively preferring certified subs. Contracting officers evaluating proposals from similarly-priced competitors will favor the one with documented, verified cybersecurity.

11.6 The Market Opportunity: DoD Contract Revenue at Stake

The scale of DoD contracting provides context for understanding what certification protects and what it enables. The DoD obligates over $400 billion annually in contract spending. The Defense Industrial Base that supports that spending has been shrinking — the number of unique DoD prime contractors has declined by more than 40% since 2000, and the small business share has fallen as compliance and program management costs price smaller companies out of the market. CMMC creates another filter — but for those who clear it, it also removes competitors.

Contractor Scenario	CMMC Decision	Business Outcome
Small manufacturer, $3M DoD revenue, Level 2 work, renewal due 2026	Does not pursue certification; cannot afford C3PAO assessment	Loses contract at renewal. Existing revenue eliminated. May exit DIB entirely.
Same manufacturer, invests in CMMC compliance	Achieves Level 2 certification; SPRS score of 105	Renews existing contracts. Eligible for new work from competitors who tapped out. Revenue grows.
Mid-size systems integrator, $25M DoD revenue, mixed Level 1 and 2 work	Achieves Level 2 for CUI-handling contracts; maintains Level 1 self-attestation for remainder	Protects full revenue base. Becomes preferred sub for primes managing supply chain compliance risk.
Defense prime, $200M revenue, manages large sub base	Achieves Level 2; requires subs to certify; drops non-compliant subs	Stronger supply chain posture reduces prime liability. Certified subs gain preferred vendor status.
Startup entering DIB market	Builds CMMC compliance into initial infrastructure design	Faster time to first contract award. No legacy remediation debt. Immediate competitive parity

		with established players.

11.7 Certification as a Business Investment: The ROI Framework

Framing CMMC certification purely as a compliance cost misses the business reality. For any contractor whose DoD revenue exceeds the certification cost — which, for a three-year $450,000–$750,000 investment, means any contractor with more than approximately $250,000/year in DoD work — the ROI of certification is positive and often dramatically so.

The correct question is not "Can we afford to get CMMC certified?" It is "Can we afford to lose the DoD contracts that certification protects?" For most contractors currently in the DIB, the answer to the second question is an unambiguous no.

Annual DoD Revenue	3-Year Revenue at Risk	Est. 3-Year Certification Cost	Cost as % of Revenue at Risk	ROI of Certification
$500,000	$1,500,000	$250,000–$400,000	17–27%	Borderline — evaluate whether work will continue post-CMMC
$1,000,000	$3,000,000	$300,000–$500,000	10–17%	Positive — certification protects 6–10× its cost
$2,500,000	$7,500,000	$350,000–$550,000	5–7%	Strong — 14–21× return on protected revenue
$5,000,000	$15,000,000	$400,000–$650,000	3–4%	Compelling — 23–37× return on protected revenue

$10,000,000	$30,000,000	$500,000–$750,000	2–3%	Undeniable — 40–60× return on protected revenue

These figures do not include the revenue growth opportunity from capturing work vacated by non-compliant competitors — which can significantly improve the actual ROI experienced by certified contractors in the 2025–2028 window when the market is actively consolidating around CMMC compliance status.

11.8 Managing Continuous Compliance Cost Over Time

One dimension of CMMC cost that is frequently underweighted in business cases is the ongoing, recurring cost of continuous compliance. The $50,000–$100,000+ annual cost of continuous monitoring, evidence maintenance, policy reviews, and re-assessment preparation does not disappear after initial certification. It is a permanent operational cost of participating in the certified DIB.

The most effective way to manage this ongoing cost is through automation and managed services that replace expensive manual processes. An organization staffing a full-time compliance analyst at $120,000/year to maintain CMMC documentation and monitor controls manually is spending more on continuous compliance than a comparable organization using an AI-native managed compliance service — while achieving less consistent results because manual processes are inherently variable and dependent on individual attention.

Continuous Compliance Cost Comparison

Traditional approach (manual / in-house):

- Compliance analyst (FTE): $100,000–$140,000/year
- GRC tool license: $15,000–$40,000/year
- SIEM / monitoring platform: $30,000–$80,000/year
- Vulnerability scanner: $10,000–$25,000/year
- Assessment prep consulting (annual): $20,000–$50,000/year

Total: $175,000–$335,000/year

AI-native managed service approach (e.g., Espresso Labs):
- Unified platform (monitoring + GRC + evidence + ticketing): consolidated
- No FTE compliance analyst required for routine operations
- Assessment package generated automatically

Estimated savings vs. traditional approach: up to 80%

Source: espressolabs.com/resources/cmmc/how-much-does-cmmc-cost/

Chapter 12: How Espresso Labs Can Help

12.1 A New Kind of MSP — One That Never Sleeps

Espresso Labs is an AI-native compliance service — a fundamentally new category of managed service provider built from the ground up for a world where cyber threats move at machine speed, regulatory clocks tick in hours (not weeks), and no human team working business hours can keep pace.

Traditional MSPs and compliance consultants operate on a familiar model: they show up, run an assessment, hand you a report, and come back in a year. In between, your environment drifts. Patches go unapplied. Configurations change. New devices appear. Log retention gaps open up. By the time anyone notices, the gap has either been exploited or it surfaces as a finding in your next C3PAO assessment — neither outcome is acceptable.

Espresso Labs works differently. Our platform runs continuously, every hour of every day, ingesting telemetry from your endpoints, cloud environments, identity systems, and network devices. AI agents compare that live state against your CMMC control baseline and fire automated playbooks the moment drift is detected — no ticket, no on-call engineer, no morning stand-up required. When a human decision is genuinely needed, we escalate with full context already assembled. When it is not, the system self-heals.

Why "AI-Native" Is Not Just a Marketing Term

A traditional MSP adds AI features on top of a human-staffed service desk.
An AI-native service inverts the model: AI is the primary responder; humans
are the escalation path. This distinction matters enormously for CMMC because:

- DFARS 252.204-7012 requires cyber incident reporting within 72 hours.
  AI detection and automated notification compresses that clock from days to minutes.

• Adversaries using AI move faster than human analysts can triage alerts.
AI-native detection matches the speed of AI-powered attacks.

• CMMC continuous monitoring (3.12.3) requires ongoing — not periodic — vigilance.
Only an always-on automated system can satisfy "ongoing" at a defensible level.

• Small and mid-size DIB contractors cannot staff a 24/7 SOC.
AI-native services deliver enterprise-grade monitoring at SMB price points.

12.2 Controls Mapped to Automated Playbooks

One of the most powerful — and most underutilized — ideas in CMMC compliance is that a large portion of the 110 NIST SP 800-171 requirements are not just verifiable by automation; they are enforceable by automation. Rather than documenting that a control exists and hoping someone follows the procedure, Espresso Labs maps controls directly to machine-executable playbooks that configure, patch, monitor, and remediate without waiting for human intervention.

This is a decisive shift in the compliance model. Instead of "we have a policy that says users must use MFA," the system enforces MFA at the identity provider level and alerts if any account bypasses it. Instead of "we patch monthly," the system deploys patches automatically within the risk-based window, logs proof of deployment, and updates your SSP evidence in real time. The control is not just documented — it is guaranteed.

The following examples illustrate how specific NIST SP 800-171 requirements are mapped to automated playbooks in the Espresso Labs platform:

NIST Req.	Control Description	Espresso Labs Automated Playbook	Evidence Generated

3.5.3 (IA)	Multi-factor authentication for privileged accounts and CUI system access	Playbook continuously audits the identity provider (Entra ID / Okta) for any account with access to CUI systems that lacks MFA enrollment. Detected accounts are automatically flagged, access is suspended pending remediation, and the account owner + admin receive immediate notification.	MFA enrollment report (timestamped), access suspension log, notification record — maps directly to IA.L2-3.5.3 evidence requirement
3.14.1 (SI)	Identify, report, and correct system flaws in a timely manner (patching)	Playbook ingests vulnerability scan results daily, cross-references against CISA KEV and CVSSv3 scores, and auto-deploys patches via endpoint management (Intune / SCCM) within risk-tiered windows: Critical ≤72h, High ≤7 days, Medium ≤30 days. Failed deployments	Patch deployment log with CVE mapping, before/after vulnerability scan comparison, exception records — maps to SI.L2-3.14.1 and RA.L2-3.11.3

		auto-retry and escalate.	
3.4.1 / 3.4.2 (CM)	Establish and maintain baseline configurations; control changes to those baselines	Playbook captures a signed configuration snapshot (OS settings, enabled services, installed software, firewall rules) for every in-scope device weekly and on every detected change. Deviations from the approved baseline trigger an alert and, for known-safe rollbacks, an automated restore.	Configuration baseline snapshots, diff reports for every detected change, change ticket cross-reference — maps to CM.L2-3.4.1 and CM.L2-3.4.2
3.3.1 / 3.3.2 (AU)	Create, protect, and retain audit logs; ensure actions are traceable to individual users	Playbook enforces log forwarding from every in-scope endpoint, server, and cloud workload to a tamper-resistant SIEM. Retention policy is enforced automatically (minimum 90 days hot, 3 years cold). Log gaps (e.g., a device going silent) trigger	Log ingestion dashboard (devices reporting vs. expected), retention policy enforcement report, gap alerts with timestamps — maps to AU.L2-3.3.1 and AU.L2-3.3.2

		an immediate alert.	
3.11.2 (RA)	Scan for vulnerabilities in systems periodically and when new vulnerabilities are identified	Playbook runs authenticated vulnerability scans against all in-scope assets on a continuous schedule (daily for internet-facing, weekly for internal). New CVEs in CISA KEV automatically trigger an out-of-cycle targeted scan of potentially affected assets within 24 hours of publication.	Scan reports (dated, scoped), asset coverage matrix, CISA KEV response log — maps to RA.L2-3.11.2 and RA.L2-3.11.3
3.6.1 / 3.6.2 (IR)	Establish incident-handling capability; track, document, and report incidents to DoD	Playbook monitors SIEM for indicators of compromise (IOCs), MITRE ATT&CK TTPs, and anomaly patterns. Confirmed incidents auto-generate a pre-populated DoD incident report (per DFARS 252.204-7012) and start the 72-hour reporting clock. The IR case file is assembled automatically from correlated log evidence.	IR case record with timeline, auto-drafted DoD incident report, clock-start timestamp — maps to IR.L2-3.6.1 and IR.L2-3.6.2

3.13.8 (SC)	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI in transit	Playbook continuously inspects TLS configurations across all in-scope web services, APIs, email gateways, and VPN endpoints. Any endpoint advertising deprecated protocols (TLS 1.0/1.1, SSL) or weak cipher suites is automatically quarantined from CUI data flows and queued for remediation.	TLS scan results, cipher suite inventory, quarantine action log — maps to SC.L2-3.13.8
3.13.16 (SC)	Protect the confidentiality of CUI at rest	Playbook queries endpoint management and cloud storage APIs to verify encryption-at-rest status across all in-scope devices and repositories. Unencrypted volumes or storage buckets containing CUI trigger automatic encryption enforcement (BitLocker,	Encryption status report (per device / per repository), enforcement action log — maps to SC.L2-3.13.16

		Azure Storage encryption) and an alert to the security team.	

These are eight examples from a library of over sixty automated playbooks in the Espresso Labs platform. Together they cover the majority of the non-deferrable controls (described in Chapter 6) and the highest-point-value requirements in the SPRS scoring methodology. Each playbook is versioned, auditable, and produces evidence artifacts in formats directly accepted by C3PAO assessors — so compliance is not just enforced, it is continuously proven.

12.3 The Espresso Labs Reference CMMC Program

One of the most time-consuming and expensive phases of any CMMC journey is the documentation build — standing up a System Security Plan, drafting fourteen domain policies, writing procedures, and mapping controls to evidence. For most contractors doing this from scratch, the documentation phase alone takes three to six months and costs $10,000–$50,000 in consulting fees, with the added risk that the resulting documents are written in a vacuum and do not reflect how the organization's actual controls work.

Espresso Labs solves this with a Reference CMMC Program: a complete, pre-built set of compliance artifacts — policies, procedures, control implementations, and a System Security Plan — engineered from the ground up to work in direct conjunction with the Espresso Labs platform and automated playbook library. Rather than generic policy templates that require wholesale customization, the Reference Program is designed around the specific controls the platform enforces, the evidence the platform produces, and the environment configurations the platform manages. The result is a documentation set that is accurate on day one because it describes what the system is actually doing — not what a policy writer imagined it might do.

12.3.1 What the Reference Program Includes

Component	Description	How It Ties to the Platform
System Security Plan (SSP)	A fully populated SSP covering all 110 NIST SP 800-171 requirements, with pre-written control narratives for every requirement the Espresso Labs platform enforces, manages, or monitors. Network topology, asset inventory, and data flow sections are populated from the platform's asset discovery output.	SSP narratives reference the specific platform playbook, integration, or dashboard that implements each control — giving assessors direct traceability from the document to the live system. As controls change, the platform flags SSP sections that need updating.
14-Domain Policy Package	All fourteen NIST SP 800-171 security domain policies (Access Control, Audit & Accountability, Configuration Management, Incident Response, etc.) plus supplemental procedures for CUI handling, media sanitization, personnel security, and vendor management.	Policies are written to reference the platform's enforcement mechanisms by name — e.g., the MFA policy cites the platform's identity provider integration; the patch management policy cites the platform's risk-tiered patching playbook. Policies are not aspirational; they describe what the system enforces.
Control Implementation Statements	For each of the 110 requirements, a concise implementation statement describing exactly how the control is satisfied — who is responsible, what system or process enforces it,	Implementation statements are auto-populated from the platform's control assessment output and updated automatically when the platform detects a change in control status. The

	where evidence is generated, and how deviations are detected.	implementation statement library is the live bridge between the SSP and the evidence library.
Evidence Framework	A structured catalog defining, for each requirement, what evidence the platform generates, where it is stored, how frequently it is refreshed, and what format it takes. Pre-mapped to the CMMC Assessment Process (CAP) evidence expectations.	Because the platform generates evidence automatically (configuration snapshots, access review exports, patch deployment logs, alert records), the evidence framework describes a system that is already producing what it promises — not a system that will produce it once someone remembers to run the report.
POA&M Template	A pre-structured POA&M aligned to the platform's gap tracking and remediation ticket workflow. Any control not yet fully implemented flows automatically from the platform's assessment engine into the POA&M with the correct requirement mapping, risk score, and evidence references.	The POA&M is not a static spreadsheet — it is a live view of the platform's open remediation tickets, exportable in the format DoD expects for SPRS submission and C3PAO review.
Incident Response Plan	A complete IR plan aligned to the platform's detection-to-notification workflow, including the 72-hour DoD reporting procedure, escalation chain, and	The IR plan's procedures map directly to the platform's automated IR playbook steps — so when an incident fires, the plan describes exactly what

	evidence collection process.	the system is already doing, and personnel know where to look for case files, timelines, and draft notifications.

12.3.2 How the Reference Program Accelerates the CMMC Journey

The acceleration effect of the Reference Program is measurable at every phase of the compliance lifecycle:

Phase	Traditional Timeline	With Reference Program	Time Saved
Gap assessment & scoping	4–8 weeks	1–2 weeks (platform auto-discovers assets and maps controls)	3–6 weeks
SSP development	8–16 weeks	1–2 weeks (pre-populated from platform output, organization reviews and approves)	7–14 weeks
Policy & procedure writing	6–12 weeks	1 week (Reference Program policies delivered; organization customizes org-specific fields)	5–11 weeks
Evidence library build	4–8 weeks (ongoing manual collection)	Continuous and automatic from day one of platform deployment	4–8 weeks initially; hundreds of hours per year ongoing
Assessment readiness review	4–6 weeks of manual evidence	2–3 days (platform generates evidence	3–5 weeks

	gathering and organization	package on demand)	
C3PAO assessment support	Days of staff time answering evidence requests during assessment	Hours — assessor evidence requests answered from pre-organized platform evidence library	80–90% reduction in staff time during assessment

Across the full compliance lifecycle, organizations using the Espresso Labs platform with the Reference CMMC Program typically reach assessment-ready status in three to five months from engagement start — compared to the nine-to-eighteen month typical timeline for organizations building programs from scratch with traditional consulting and generic GRC tools.

12.3.3 Tailoring the Reference Program to Your Organization

The Reference Program is a starting point, not a one-size-fits-all output. Every defense contractor has unique attributes — a distinctive network architecture, specialized equipment, specific CUI types, particular cloud environments, or unique organizational structures — that require the Reference Program to be tailored before it accurately describes the organization's environment.

Espresso Labs' onboarding process includes a structured tailoring workshop that adapts the Reference Program to the organization's specific context. The platform's asset discovery and control assessment output drives much of this tailoring automatically — the SSP is updated with discovered assets, the control narratives are adjusted to reflect the organization's specific tool choices, and the evidence framework is calibrated to the data sources available in the environment. Human review and approval by the organization's senior official confirms the final program before it is used in any assessment context.

Reference Program vs. Starting From Scratch

A policy written from a generic template says: "The organization shall implement multi-factor authentication for all privileged accounts."

A Reference Program policy says: "Multi-factor authentication for all privileged accounts is enforced through the Espresso Labs identity integration with Microsoft Entra ID. Enforcement is verified continuously by the platform's MFA compliance playbook (Playbook ID: IA-3.5.3). Any account with privileged access that lacks MFA enrollment is automatically flagged and access is suspended within [X] minutes. Evidence of enforcement is recorded in the compliance ticket log and exported to the evidence library under requirement 3.5.3 on a [daily] basis."

The second version is what a C3PAO assessor can actually verify. The first version is what generates a follow-up question and a request for additional evidence.

12.4 Built for the Speed of AI-Powered Risk

The cybersecurity landscape your organization operates in today is categorically different from the one that existed when DFARS 252.204-7012 was written in 2016. Adversaries — including the nation-state actors specifically targeting the DIB — now deploy AI to conduct reconnaissance at scale, generate convincing spear-phishing content in seconds, identify unpatched vulnerabilities faster than human analysts can triage scanner output, and pivot through networks with automated lateral movement tools. The speed asymmetry between AI-powered attackers and human-staffed defenses is widening every month.

The 72-hour incident reporting requirement in DFARS 252.204-7012 was designed for a world where breaches took days or weeks to detect. In an AI-powered attack, the dwell time between initial access and data exfiltration can be measured in hours. If your detection and response capability depends on a security analyst reviewing a morning dashboard, you may already be reporting a breach that is 18 hours old — and the clock has been running since hour zero.

Espresso Labs closes this gap by operating at machine speed. Our AI detection layer processes telemetry in near-real time, correlates signals across your entire environment simultaneously, and initiates both automated containment and human notification within minutes of a confirmed indicator. The 72-hour reporting window becomes a policy compliance step rather than a race against the clock.

12.5 The Compliance Ticketing System — Evidence That Builds Itself

One of the most frustrating experiences in any CMMC assessment is the evidence scramble: the C3PAO assessor asks for proof that your organization detected, investigated, and remediated a specific type of event over the past twelve months, and your team spends three days pulling emails, Slack messages, spreadsheets, and screenshots to reconstruct a timeline that was never systematically captured in the first place. The evidence existed — the work was done — but it was never organized in a way that an assessor can evaluate. Espresso Labs eliminates this problem entirely.

Built into the Espresso Labs platform is a compliance-native ticketing system designed from the ground up for the CMMC evidence lifecycle — not adapted from a generic IT helpdesk product. Every action the platform takes, every alert it fires, every automated playbook it executes, and every human decision made in response to a finding is recorded as a structured ticket in a tamper-evident log. Those tickets are not isolated records — they are first-class objects in the platform's enterprise context graph, linked to the NIST SP 800-171 requirement they address, the asset involved, the personnel who acted, and the evidence artifacts that resulted.

12.5.1 What Gets Ticketed

The ticketing system captures four categories of activity, each with its own structured schema:

Ticket Type	What It Captures	CMMC Evidence Value

Administrative / Operational	Routine compliance program activities: policy reviews and approvals, SSP updates, configuration baseline sign-offs, access re-certifications, media sanitization records, background check completions, training completions, vendor risk reviews	Produces the operational evidence trail that demonstrates ongoing program management — critical for CA.L2-3.12.1 (periodic security control assessment) and AT.L2-3.2.1 (security awareness activities)
Security Event / Alert	Every alert generated by the monitoring layer — whether auto-resolved by a playbook or escalated for human review. Captures: detection timestamp, alert source, affected asset(s), indicator details, initial classification (true positive / false positive / informational)	Demonstrates AU.L2-3.3.1 (audit log review), SI.L2-3.14.6 (attack monitoring), and IR.L2-3.6.1 (incident handling capability). False-positive tickets show the organization actively triages alerts rather than ignoring them
Incident Investigation	Full lifecycle of a confirmed security incident from detection through containment: timeline of events, forensic findings, affected systems and data, personnel involved, actions taken, external notifications made (including DoD 72-hour report). Linked to the originating alert ticket and all evidence files	Directly satisfies IR.L2-3.6.2 (track, document, and report incidents). The DoD incident report draft is auto-generated from the ticket fields and pre-populated with the required data elements — the analyst reviews and submits rather than writing from scratch

Remediation / POA&M Item	Every identified gap — whether from a gap assessment, a C3PAO finding, an internal audit, or a playbook-detected drift — has a ticket tracking: gap description, affected requirement(s), risk rating, assigned owner, planned remediation steps, target date, actual completion date, and closure evidence	Provides the living POA&M required by CA.L2-3.12.2 with full audit trail. Each closed item carries its own evidence package, making the POA&M defensible rather than declaratory

12.5.2 Enterprise Context — Tickets as Compliance Intelligence

Individual tickets are useful. A connected graph of tickets mapped to controls, assets, and people is transformative. Espresso Labs maintains an enterprise context — a structured, queryable knowledge base that links every ticket to every other relevant piece of your compliance program. This is what makes the platform fundamentally different from a ticketing system bolted onto a GRC tool.

The enterprise context enables queries that would otherwise require days of manual work:

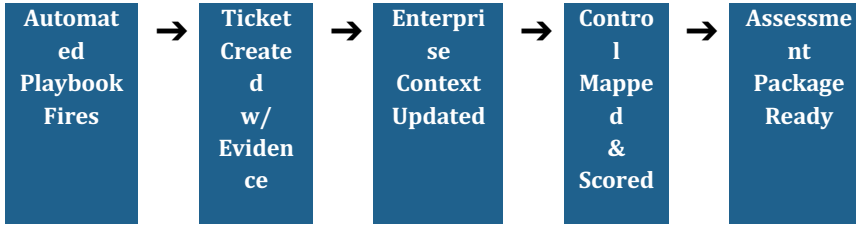
- "Show me all evidence for requirement 3.6.1 over the past 24 months" — the system returns every incident ticket, every IR test record, and every policy review associated with that control, organized chronologically with links to evidence files.
- "Which assets have had the most security events in the last 90 days?" — the system cross-references alert tickets against the asset inventory and surfaces the highest-risk devices for targeted hardening.
- "What actions did we take after the phishing campaign detected on [date]?" — the system returns the full incident ticket chain: detection alert, investigation notes, affected accounts,

remediation steps, training follow-up, and the DoD notification record.

- "Generate an evidence summary for domain 3.3 (Audit and Accountability) for our upcoming C3PAO assessment" — the system aggregates all relevant tickets, evidence files, and configuration snapshots into a structured export ready for assessor review.

This last capability — on-demand evidence package generation — is the most direct answer to the assessment evidence scramble. When your C3PAO schedules the assessment kickoff call, the Espresso Labs platform can produce a structured evidence package for every one of the 110 requirements within hours, not days. Each package contains the relevant tickets, the associated artifacts, and a narrative summary of how the evidence satisfies the requirement — in the format assessors actually want to review.

From Event to Assessment Evidence — Automated Lifecycle



12.5.3 How the Ticketing System Satisfies Specific CMMC Requirements

It is worth being explicit about the direct mapping between the ticketing system's outputs and the CMMC requirements they satisfy, because assessors will ask for exactly this evidence:

NIST Requirement	How Ticket Records Provide Evidence
3.3.1 — Create and retain audit logs	Every ticket is a timestamped, immutable record. Alert tickets capture the original log event and the response action. The system

	retains tickets for the full retention period with no manual archiving required.
3.3.2 — Ensure user actions are traceable	Every ticket records the authenticated identity of every person who viewed, commented on, or acted on the ticket — creating a complete human audit trail alongside the system log trail.
3.6.1 — Incident handling capability	The existence of the incident ticket workflow — with defined fields, mandatory escalation steps, and SLA timers — is itself evidence of an operational incident handling capability, not just a paper policy.
3.6.2 — Track, document, and report incidents	Incident tickets capture the complete documentation trail. The DoD report draft is auto-generated from ticket fields, and the submission record (timestamp, recipient, confirmation) is attached to the ticket on send.
3.12.1 — Periodically assess security controls	Administrative tickets for scheduled control reviews capture who conducted the review, when, what evidence was examined, and what the finding was — a structured record of every periodic assessment activity.
3.12.2 — Develop and implement POA&Ms	Remediation tickets are the POA&M. Each ticket carries the gap description, NIST requirement mapping, risk rating, owner, target date, and closure evidence — and the aggregate view is the live POA&M document.
3.12.3 — Monitor security controls on an ongoing basis	The continuous stream of alert tickets — including those auto-resolved by playbooks — is evidence of ongoing monitoring. Gap in ticket volume is itself a monitoring signal that the platform surfaces automatically.
3.9.2 — Ensure CUI is protected during personnel actions	Offboarding tickets capture the sequence: access revocation,

	device recovery, account disablement — each step timestamped and attributed to the responsible HR/IT actor.
3.14.6 — Monitor for attacks and indicators of compromise	Alert tickets with IOC details, MITRE ATT&CK tactic tags, and response actions provide direct, chronological evidence of threat monitoring activity across the assessment period.

Assessment Day — What Espresso Labs Delivers
When your C3PAO assessment begins, Espresso Labs provides a structured Evidence Package containing:

- Per-requirement evidence summaries (all 110 requirements) with ticket and artifact references
- Incident and event logs organized by NIST domain
- Current SSP with automated evidence cross-references populated
- POA&M (as the live remediation ticket aggregate) with closure evidence for completed items
- Configuration baseline snapshots for all in-scope assets (current and historical)
- Access review records, training completion logs, and media sanitization records
- A compliance timeline showing control status over the full assessment period

The goal: your C3PAO assessor walks into an environment where the evidence
is already organized, already mapped, and already speaks for itself.
The assessment becomes a verification exercise, not an evidence hunt.

12.6 Our Services

Service	Description	Who It's For
CMMC Readiness Assessment	Comprehensive gap analysis against all 110 NIST SP 800-171 requirements, scoping analysis, SPRS score calculation, and a	Any contractor new to CMMC or preparing for C3PAO assessment

	sequenced remediation roadmap	
SSP & Policy Package	Full System Security Plan plus all 14 domain policies and procedures — C3PAO-ready, AI-drafted, expert-reviewed	Contractors without existing documentation or needing a full refresh
Automated Playbook Deployment	Deployment of Espresso Labs control playbooks into your Microsoft 365 / Entra ID / endpoint management environment — controls enforced, not just documented	Contractors ready to move from policy to enforcement
Continuous Compliance Monitoring	24/7 AI monitoring against your CMMC control baseline with automated remediation for in-scope drift and real-time SPRS score tracking	Any contractor needing always-on compliance assurance
Incident Response — AI-Accelerated	AI-powered threat detection, auto-assembled IR case files, pre-populated 72-hour DoD report drafts, and on-call human IR support for confirmed incidents	Any contractor subject to DFARS 252.204-7012 reporting requirements
Assessment Readiness Review	Pre-C3PAO mock assessment using the official CMMC Assessment Process — AI finds gaps before the assessor does	Contractors within 90 days of a scheduled C3PAO assessment
Supply Chain Compliance	Subcontractor CMMC status tracking, flowdown clause verification, and supplier risk scoring	Prime contractors managing multi-tier supply chains

CUI Discovery & Classification	AI-powered scan of email, file shares, cloud storage, and endpoints to locate, classify, and map all CUI data flows	Contractors unsure of where their CUI lives

12.7 Why Espresso Labs

Defense contractors choosing a CMMC partner have no shortage of options. Here is why Espresso Labs is different:

- Always on: Our AI platform monitors your environment 24 hours a day, 7 days a week, 365 days a year. There is no off-hours window for adversaries to exploit.
- Speed: Automated playbooks respond to detected control drift in minutes. No ticket queue. No morning stand-up. No waiting for the next quarterly review.
- Enforcement over documentation: We do not just write policies — we deploy playbooks that enforce controls at the system level, making compliance structurally guaranteed rather than behaviorally dependent.
- Continuous proof: Every playbook execution generates a timestamped, assessor-ready evidence artifact. Your SSP evidence library is never stale.
- Right-sized for the DIB: Purpose-built for defense contractors of all sizes — from a 10-person machine shop handling CUI to a 2,000-employee systems integrator managing a multi-tier supply chain.
- Transparent: Every compliance finding, every playbook action, every SPRS score change is logged and visible. You always know exactly where you stand.

12.8 Getting Started

If you are reading this book, you are already taking the right first step: understanding what CMMC requires before investing in compliance programs. The next step is an honest assessment of where you stand today.

Espresso Labs offers a no-cost preliminary scoping consultation to help you answer:

- Does CMMC apply to my organization, and at which level?
- What is my estimated gap from current posture to required compliance?
- What are the most critical risks I need to address first?
- What is a realistic timeline and budget for my CMMC program?

To schedule your consultation, contact us at:

info@espressolabs.com

We look forward to helping you protect your place in the defense industrial base and build a cybersecurity program that genuinely safeguards the sensitive information you are trusted to protect.

Appendix A: NIST SP 800-171 Domain Reference

The following table provides a concise reference for all 14 NIST SP 800-171 security requirement families, with representative requirements and the most common assessment findings in each domain.

Domain	Key Requirements (Examples)	Common Assessment Findings
Access Control (AC) 22 requirements	3.1.1 Limit system access to authorized users 3.1.2 Limit system access to types of transactions 3.1.3 Control CUI flow 3.1.12 Monitor remote access sessions 3.1.14 Route remote access via managed access points	No least-privilege model; personal devices accessing CUI; VPN without MFA; guest accounts with CUI access
Awareness & Training (AT) 3 requirements	3.2.1 Security awareness activities 3.2.2 Insider threat awareness 3.2.3 Training for individuals with security roles	Annual training not completed for all personnel; no role-specific training for admins; no insider threat module
Audit & Accountability (AU) 9 requirements	3.3.1 Create and retain system audit logs 3.3.2 Ensure actions can be traced to users 3.3.5 Correlate audit record review and analysis	Insufficient log retention (less than 90 days); gaps in log collection; no evidence of regular log review
Configuration Management (CM) 9 requirements	3.4.1 Baseline configurations 3.4.2 Establish configuration change control 3.4.7 Restrict, disable, or prevent the use of nonessential programs	No documented configuration baselines; software installed without approval; unnecessary services enabled

Identification & Authentication (IA) 11 requirements	3.5.1 Identify system users 3.5.3 Multi-factor authentication 3.5.7 Enforce minimum password complexity	No MFA for privileged accounts; shared accounts; weak password policies; no account inactivity lockout
Incident Response (IR) 3 requirements	3.6.1 Incident handling capability 3.6.2 Track, document, and report incidents 3.6.3 Test incident response capability	No IR plan; plan not tested; 72-hour DoD reporting capability not established; no IR retainer
Maintenance (MA) 6 requirements	3.7.1 Perform maintenance 3.7.2 Provide controls for maintenance tools 3.7.5 MFA for remote maintenance	Remote maintenance without MFA; maintenance personnel with unsupervised access; no maintenance log
Media Protection (MP) 9 requirements	3.8.1 Protect system media 3.8.3 Sanitize media before disposal 3.8.9 Protect CUI during transport	No media sanitization records; CUI on unencrypted portable media; no portable media policy
Personnel Security (PS) 2 requirements	3.9.1 Screen individuals 3.9.2 Ensure CUI is protected during/after personnel actions	No background check process; access not revoked promptly at termination; no access transfer procedure
Physical Protection (PE) 6 requirements	3.10.1 Limit physical access 3.10.3 Escort visitors 3.10.6 Protect and monitor physical facility	Unlocked server rooms; no visitor log; CUI printouts left in open areas; no physical access review
Risk Assessment (RA) 3 requirements	3.11.1 Assess risk periodically 3.11.2 Scan for vulnerabilities 3.11.3 Remediate vulnerabilities in accordance with risk	No formal risk assessment; vulnerability scanning less than quarterly; no remediation prioritization process

Security Assessment (CA) 4 requirements	3.12.1 Periodically assess security controls 3.12.2 Develop and implement POA&Ms 3.12.3 Monitor security controls 3.12.4 Develop SSP	No SSP; SSP not current; no POA&M; no evidence of periodic control assessments
System & Comms Protection (SC) 16 requirements	3.13.1 Monitor, control, and protect communications 3.13.5 Implement subnetworks for public-access systems 3.13.8 Encrypt CUI in transit 3.13.10 Establish key management	Unencrypted email for CUI; flat networks; no boundary protection; outdated TLS configurations
System & Info Integrity (SI) 7 requirements	3.14.1 Identify and correct system flaws 3.14.2 Anti-malware protection 3.14.6 Monitor for attacks and indicators of compromise 3.14.7 Identify unauthorized use	No patch management process; AV not updated; no security monitoring/SIEM; no IOC detection capability

Appendix B: Glossary of Key Terms

Term	Definition
C3PAO	Certified Third-Party Assessment Organization. An organization authorized by the Cyber AB to conduct CMMC Level 2 assessments.
CCA	Certified CMMC Assessor. An individual certified to conduct CMMC assessments for a C3PAO.
CCP	Certified CMMC Professional. An individual certified to support CMMC compliance preparation (advisory/implementation, not assessment).
CMMC	Cybersecurity Maturity Model Certification. The DoD's cybersecurity certification program for defense contractors.
CUI	Controlled Unclassified Information. Sensitive government information requiring safeguarding controls under law, regulation, or policy.
Cyber AB	CMMC Accreditation Body. The non-profit organization that manages the CMMC assessor ecosystem, training, and marketplace.
DCMA DIBCAC	Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center. Conducts Level 3 CMMC assessments.
DFARS	Defense Federal Acquisition Regulation Supplement. Supplements the FAR with DoD-specific contracting rules.
DIB	Defense Industrial Base. The commercial companies that support the DoD's acquisition programs.
eMASS	Enterprise Mission Assurance Support Service. DoD system that

	receives and tracks CMMC assessment results.
FAR	Federal Acquisition Regulation. The primary set of rules governing the federal government's acquisition process.
FCI	Federal Contract Information. Information provided by or generated for the government under a contract, not intended for public release.
FedRAMP	Federal Risk and Authorization Management Program. The government-wide cloud authorization program.
GCC High	Microsoft's Government Community Cloud High environment, authorized for CUI and ITAR data.
MSSP	Managed Security Service Provider. A company providing outsourced security monitoring and operations.
NIST SP 800-171	The NIST publication defining 110 security requirements for protecting CUI in non-federal systems.
NIST SP 800-172	Enhanced NIST publication with additional requirements for high-value CUI under APT threat.
POA&M	Plan of Action and Milestones. A document tracking unimplemented security controls and remediation plans.
RPO	Registered Provider Organization. A company listed in the Cyber AB marketplace as a CMMC advisory/implementation provider.
SAM.gov	System for Award Management. The federal portal for contractor registration, required for government contract awards.
SPRS	Supplier Performance Risk System. The DoD database where

	contractors submit their NIST SP 800-171 assessment scores.
SSP	System Security Plan. The master document describing an organization's security controls and their implementation.
UEI	Unique Entity Identifier. The 12-character alphanumeric identifier assigned to organizations registered in SAM.gov.

Appendix C: Key Regulatory References

Reference	Title / Subject	Relevance to CMMC
32 CFR Part 170	Cybersecurity Maturity Model Certification (CMMC) Program	The CMMC final rule — primary regulatory authority
DFARS 252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting	Core clause requiring NIST SP 800-171 compliance and 72-hour incident reporting
DFARS 252.204-7019	Notice of NIST SP 800-171 DoD Assessment Requirements	Requires contractors to have a SPRS score before contract award
DFARS 252.204-7020	NIST SP 800-171 DoD Assessment Requirements	Allows DoD to review CMMC/assessment documentation
DFARS 252.204-7021	Cybersecurity Maturity Model Certification Requirements	The primary CMMC contract clause; triggers formal CMMC requirements
FAR 52.204-21	Basic Safeguarding of Covered Contractor Information Systems	Applies to all federal contractors handling FCI; Level 1 basis
NIST SP 800-171 Rev 2	Protecting CUI in Nonfederal Systems and Organizations	The 110 requirements forming the basis of CMMC Level 2
NIST SP 800-171A	Assessing Security Requirements for CUI	Assessment procedures corresponding to each SP 800-171 requirement
NIST SP 800-172	Enhanced Security Requirements for CUI	Additional requirements forming the basis of CMMC Level 3
EO 13556	Controlled Unclassified Information (2010)	Executive Order establishing the CUI program
32 CFR Part 2002	Controlled Unclassified Information	Implementing regulation for the CUI program

DoD Assessment Methodology	NIST SP 800-171 DoD Assessment Methodology v1.2.1	Scoring guide for calculating and submitting SPRS scores
31 U.S.C. § 3729-3733	False Claims Act	Provides civil and criminal liability for false certification of CMMC/cybersecurity compliance