GOVDATAHOSTING
POWERED BY IT-CNP, INC.
FEDRAMP HIGH (CLASS D) CERTIFIED CLOUD PLATFORM

NIST 800-171 / CMMC LEVEL 2
ROADMAP

The Defense Contractor's Playbook to a Passing Score & C3PAO Certification

2026 EDITION • **ALIGNED TO 32 CFR PART 170 & DFARS 252.204-7021**

WHAT YOU'LL LEARN

CMMC levels & rollout timeline • CUI scoping & asset categories • SPRS scoring methodology • The fastest path to a passing score • POA&M strategy • C3PAO assessment prep • Progress tracker

FOR

Defense Contractors • Primes & Subcontractors • The Defense Industrial Base

GovDataHosting

FedRAMP High (Class D) Certified • NIST 800-53 High • DoD IL2 Authorized

www.govdatahosting.com | 800-967-1004

What's Inside

01 Executive Summary
The stakes, the deadline, and what this playbook delivers

02 Understanding CMMC 2.0
The program, the three levels, and who must comply

03 The Implementation Timeline
The four-phase rollout and the date that matters

04 NIST SP 800-171: The 110 Requirements
The 14 control families and assessment objectives

05 SPRS Scoring Explained
The DoD Assessment Methodology, point weights, and the 88 threshold

06 CUI Scoping & Asset Categories
Defining your boundary and the five asset categories

07 The Fastest Path to a Passing Score
Prioritized remediation and POA&M strategy

08 C3PAO Assessment Preparation
The CAP process, your evidence bundle, and selecting an assessor

09 Your CMMC Progress Tracker
Track families, milestones, and your SPRS score

10 CMMC Readiness Checklist
Scope to certification, step by step

11 How GovDataHosting Accelerates Your Path
A FedRAMP-certified enclave and inherited controls

Executive Summary

For more than a decade, the cybersecurity obligations on defense contractors ran largely on the honor system. Under DFARS 252.204-7012, contractors handling Controlled Unclassified Information (CUI) were required to implement the 110 controls of NIST SP 800-171 and self-attest to their compliance. The Cybersecurity Maturity Model Certification (CMMC) program exists to replace that self-attestation with independent verification.

With the CMMC acquisition rule (48 CFR) effective November 10, 2025, CMMC is now a legally enforceable condition of contract award. The single most important date for most contractors handling CUI is November 10, 2026—the start of Phase 2, when a third-party (C3PAO) Level 2 certification becomes a standard requirement on applicable solicitations and contracts.

This roadmap is a practical, contractor-focused playbook for getting there: how CMMC is structured, how SPRS scoring works, how to scope your CUI environment, the fastest path to a passing score, how to prepare for a C3PAO assessment, and a progress tracker to manage it all.

WHY THIS MATTERS NOW

The DoD estimates roughly 80,000 contractors will need a Level 2 C3PAO certification, and that 70–75%+ of CUI handlers will require third-party verification rather than self-assessment. Preparing typically takes 6–12 months—so for a Phase 2 contract, the planning clock is already running.

Key Takeaways

- CMMC Level 2 maps directly to the 110 requirements of NIST SP 800-171 (Rev. 2)—the same controls you already owe under DFARS 7012.
- Your SPRS score (range –203 to 110) is the gate: most contracts expect movement toward 110, and a minimum of 88 is required to earn a Conditional certification.
- Scoping your CUI environment correctly is the highest-leverage decision you will make—it drives cost, risk, and timeline.
- Hosting CUI in a FedRAMP-certified enclave lets you inherit controls, shrink your assessment boundary, and accelerate your path to a passing score.
- Self-attestation is ending. An affirming official must attest annually in SPRS—and inaccurate affirmations carry False Claims Act exposure.

Understanding CMMC 2.0

CMMC is the Department of Defense's program for verifying that contractors and subcontractors in the Defense Industrial Base (DIB) adequately protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). It is established in two parts of the Code of Federal Regulations: the program rule at 32 CFR Part 170 (effective December 16, 2024), and the acquisition rule at 48 CFR—which inserts the contract clause DFARS 252.204-7021 (effective November 10, 2025).

FCI vs. CUI

The level you need is driven by the type of information your systems handle. Federal Contract Information (FCI) is non-public information provided by or generated for the government under a contract. Controlled Unclassified Information (CUI) is information the government (or an entity acting for it) must safeguard under law, regulation, or government-wide policy—contracts, statements of work, technical data, source code, and proposals are common examples.

The Three CMMC Levels

Level	Information	Security Requirements	Assessment	Cadence
Level 1	FCI only	15 basic requirements (FAR 52.204-21)	Self-assessment	Annual
Level 2	CUI	110 requirements (NIST SP 800-171 Rev. 2)	C3PAO (most); self for a limited subset	Every 3 years
Level 3	CUI (highest priority)	Level 2 + 24 enhanced requirements (NIST SP 800-172)	Government (DIBCAC)	Every 3 years

WHERE MOST CONTRACTORS LAND

If your contract involves CUI, you are almost certainly targeting Level 2. Under Phase 2, the DoD expects the majority of CUI handlers to undergo a C3PAO certification assessment rather than a self-assessment—so plan for third-party verification unless your contracting officer specifies otherwise.

Who Must Comply

CMMC requirements flow down from primes to subcontractors that handle FCI or CUI (32 CFR 170.23). The DoD estimated that roughly 338,000 prime and subcontractors are affected, including approximately 230,000 small businesses. If your information systems process, store, or transmit CUI in the performance of a DoD contract, CMMC applies to you—and to the relevant suppliers below you.

The Implementation Timeline

CMMC rolls out over a three-year, four-phase schedule defined in 32 CFR 170.3(e). Each phase begins one year after the last. The obligations escalate on fixed dates, so the right way to plan is to work backward from the phase that will apply to your contracts.

Phase	Begins	What Applies
Rule effective	Nov 10, 2025	48 CFR acquisition rule in effect; DFARS 252.204-7021 begins appearing in solicitations and contracts.
Phase 1	Nov 10, 2025	Level 1 (Self) or Level 2 (Self) required on applicable contracts. DoD may require Level 2 (C3PAO) at its discretion.
Phase 2	Nov 10, 2026	Level 2 (C3PAO) certification becomes a standard requirement on applicable contracts. DoD may require Level 3 (DIBCAC) at its discretion.
Phase 3	Nov 10, 2027	Level 3 (DIBCAC) added to applicable contracts; Level 2 (C3PAO) applied more broadly.
Phase 4	Nov 10, 2028	Full implementation—CMMC required on all applicable DoD contracts as a condition of award.

THE DATE THAT MATTERS: NOVEMBER 10, 2026

Phase 2 is when self-attestation stops being enough for most CUI work. If a Phase 2 contract is in your pipeline, count backward: 6–12 months to prepare, plus roughly 90 days to build an operational track record your assessor can verify. For many contractors, that means the work needs to be underway now.

A Note on NIST 800-171 Rev 2 vs. Rev 3

CMMC Level 2 is currently assessed against NIST SP 800-171 Revision 2 (110 requirements), and the DoD Assessment Methodology and SPRS scoring are built for Rev 2. NIST published Revision 3 in May 2024, but the DoD has not adopted it for CMMC and has signaled no near-term change. Build to Rev 2 today—while keeping an eye on fedramp.gov, dodcio.defense.gov, and the Federal Register for any transition guidance.

NIST SP 800-171: The 110 Requirements

Level 2 is built on the 110 security requirements in NIST SP 800-171, organized into 14 control families. Each requirement is further broken into assessment objectives—320 in total—that an assessor evaluates using the methods in NIST SP 800-171A. Your System Security Plan (SSP) must document how you meet each requirement across all 14 families.

The 14 Control Families

ID	Control Family	Reqs	Focus
AC	Access Control	22	Who and what can reach CUI
AT	Awareness & Training	3	Security awareness for staff
AU	Audit & Accountability	9	Logging and traceability
CM	Configuration Management	9	Hardened, controlled baselines
IA	Identification & Authentication	11	Identity, MFA, credentials
IR	Incident Response	3	Detect, report, respond
MA	Maintenance	6	Safe system maintenance
MP	Media Protection	9	Protecting & sanitizing media
PS	Personnel Security	2	Screening and transfers
PE	Physical Protection	6	Facility and device access
RA	Risk Assessment	3	Vulnerability & risk management
CA	Security Assessment	4	Control assessment & POA&M
SC	System & Communications Protection	16	Boundary defense, encryption
SI	System & Information Integrity	7	Flaw remediation, monitoring
Total	**14 families — 320 assessment objectives**	**110**	

DOCUMENTATION IS THE DELIVERABLE

Implementing a control is not enough—you must be able to prove it. The SSP is the primary assessment artifact, supported by policies, procedures, and evidence for each of the 320 objectives. Assessors will challenge any requirement marked “not applicable” without a documented justification.

SPRS Scoring Explained

Before you can be considered for most CUI contracts, you must submit a self-assessment score to the DoD's Supplier Performance Risk System (SPRS) via the PIEE portal. The score is calculated using the NIST SP 800-171 DoD Assessment Methodology and is the single number contracting officers and primes use to gauge your posture.

How the Score Works

You start at a perfect 110 and subtract the weighted value of every requirement you have not fully implemented. The score ranges from a maximum of 110 down to a minimum of –203. Each requirement is worth 1, 3, or 5 points based on its security impact.

Weight	Count	What it covers
5 points	~42	Highest-impact controls (including the basic FAR 52.204-21 safeguards) whose absence would allow exploitation of the network and its data.
3 points	~14	Controls with a specific, confined effect on the security of the network and its data.
1 point	~54	Remaining controls with a more limited individual impact.

There is no partial credit—with two exceptions. Multi-factor authentication (3.5.3) and FIPS-validated cryptography (3.13.11) allow a partial deduction:

- **MFA (3.5.3):** –3 if MFA covers only remote and privileged users; –5 if MFA is not implemented for any users.
- **FIPS crypto (3.13.11):** –3 if encryption is used but not FIPS-validated; –5 if encryption is not employed.

Worked Example

Suppose you have implemented everything except five 5-point controls and MFA only for privileged users. That is (5 × 5) + 3 = 28 points of deductions, for a score of 110 – 28 = 82. Because that falls below 88, it would not yet qualify for a Conditional certification—closing two of those 5-point gaps would.

> **THE 88 THRESHOLD**
>
> A minimum score of 88 out of 110 (80%) is required to earn a Conditional Level 2 status, with up to 180 days to close the remaining gaps and reach Final. The long-term expectation, however, is a full 110—a perfect score is the goal, not the floor.

Submitting and Maintaining Your Score

- Your self-assessment must be current (no older than three years) and maintained in SPRS for the life of the contract.
- An affirming official must complete an annual affirmation of continuous compliance in SPRS for each CMMC UID.

- Inaccurate scores or affirmations carry serious consequences—contract suspension, debarment, and False Claims Act liability under the DOJ Civil Cyber-Fraud Initiative.
- For medium and high DoD-led assessments, a fully virtual assessment caps at 100 rather than 110, because physical controls cannot be verified remotely.

CUI Scoping & Asset Categories

Scoping is the most consequential decision in a CMMC Level 2 assessment. Define the boundary too broadly and you pay to secure systems that never touch CUI; define it too narrowly and you risk a failed assessment. The goal is to identify every system, person, facility, and process that handles CUI or Security Protection Data and place each into the correct category—before a C3PAO arrives. Importantly, you propose the boundary; the assessor can challenge a scope that leaves obvious gaps.

The Five Asset Categories

Asset Category	Definition	Assessment Treatment
CUI Assets Process, store, or transmit CUI.	Core systems that handle CUI directly.	Fully assessed against all applicable 110 requirements.
Security Protection Assets Provide security functions for the CUI environment.	Firewalls, SIEM, identity providers, endpoint tools.	Assessed against the requirements relevant to the protection they provide.
Contractor Risk Managed Assets Can access CUI but are not intended to, and are not separated from CUI assets.	Managed by risk-based policy; documented in the SSP.	Not assessed unless documentation is weak—then a limited spot-check.
Specialized Assets OT, IoT, ICS, test equipment, and Government-Furnished Equipment that cannot fully implement the controls.	Inventoried and documented; may qualify for an Enduring Exception.	Limited check only; must be documented and segregated.
Out-of-Scope Assets No CUI interaction and provide no protection for CUI; physically or logically separated.	Sales/marketing systems with no CUI access.	Not assessed; no documentation required (be ready to justify).

External Service Providers (ESPs) and the Cloud

If you use a cloud or external provider that stores, processes, or transmits CUI—or that holds Security Protection Data such as logs and configuration—that provider is an External Service Provider (ESP) within your scope. Under DFARS 252.204-7012, a cloud provider handling CUI must meet the FedRAMP Moderate baseline (or equivalent). You must document the ESP relationship in your SSP and rely on the provider's Customer Responsibility Matrix (CRM) to show which control objectives the provider satisfies and which remain yours.

SCOPING MISTAKE THAT DERAILS ASSESSMENTS

Misclassifying a Contractor Risk Managed Asset is a common, expensive error. If CUI actually flows to it—or your documentation is thin—an assessor can reclassify it as a CUI Asset, pulling it (and everything connected to it) fully into scope. Document the rationale and data-flow boundaries for every in-scope asset, and keep network diagrams labeled accordingly.

Scoping in Five Steps

1. Identify all CUI and Security Protection Data, and where each enters, lives, and leaves your environment.
2. Map the data flow and produce a labeled network diagram of the assessment scope.
3. Categorize every asset (people, technology, facilities) into one of the five categories.
4. Document each asset and the classification rationale in your SSP and asset inventory.
5. Shrink the boundary where you safely can—segregation and an external CUI enclave reduce cost and risk.

The Fastest Path to a Passing Score

Once you know your scope and your current SPRS score, remediation becomes a prioritization problem. Because requirements are weighted 1, 3, or 5 points, the fastest score gains come from closing high-value gaps first—and from the handful of controls that carry partial-credit rules.

Prioritize in This Order

6. **Close 5-point gaps first.** Each fully implemented 5-point control returns the most score per unit of effort and is required for certification (5- and 3-point items cannot sit on a POA&M).
7. **Fix MFA and FIPS encryption.** Moving MFA to all users and adopting FIPS-validated cryptography can swing up to 10 points and addresses two of the most-cited findings.
8. **Knock out the 3-point controls.** These also cannot be deferred to a POA&M, so they must be done before certification regardless.
9. **Sweep the 1-point controls.** Individually small, collectively decisive—and a limited set of 1-point items are the only requirements eligible for a POA&M.
10. **Document as you go.** Update the SSP with each control's implementation so your evidence is assessment-ready, not reconstructed later.

Highest-Impact Control Areas

In practice, the biggest score movements come from access control, audit and accountability, identification and authentication, and system and communications protection—strong MFA and least privilege, centralized logging with retention, FIPS-validated encryption for CUI in transit and at rest, and hardened, patched, baseline-configured endpoints.

Conditional vs. Final, and POA&M Rules

Rule	What it means
Minimum to POA&M	You must score at least 88 (80%) to be eligible for a Conditional status with a POA&M.
Not POA&M-eligible	All 5-point and 3-point requirements must be fully implemented; they cannot be deferred.
POA&M-eligible	Only a limited set of 1-point requirements may be deferred (FIPS crypto, 3.13.11, is handled under specific conditions).
Closeout window	A Conditional status lasts a maximum of 180 days; a closeout assessment confirms the POA&M is resolved to reach Final.

THE SINGLE BIGGEST ACCELERATOR

Move CUI into a FedRAMP-certified enclave. By hosting CUI on infrastructure that already implements and evidences the underlying controls, you inherit a large share of the technical requirements through the provider's Customer Responsibility Matrix, shrink your in-scope footprint, and focus your remaining effort on the application and process layer—the fastest route from a low score to 110.

C3PAO Assessment Preparation

A CMMC Third-Party Assessment Organization (C3PAO) is an independent organization authorized by the Cyber AB to conduct Level 2 certification assessments. C3PAOs evaluate your environment using the methods in NIST SP 800-171A, determine whether you achieve Conditional or Final Level 2 status (32 CFR 170.4), and submit results to the DoD, which issues the certification and a CMMC Unique Identifier (UID) in SPRS.

The CMMC Assessment Process (CAP)

The assessment follows the published CMMC Assessment Process. Early in the process (Step 1.3), the assessor validates your assessment scope—so the quality of your scoping documentation directly affects how smoothly the engagement runs. Your evidence bundle should include:

- A current System Security Plan (SSP) covering all 110 requirements and 320 objectives
- A CUI data-flow diagram showing how CUI enters, moves through, and leaves your environment
- A complete, labeled logical network diagram of the assessment scope
- A technical asset inventory mapping each asset to its category
- A physical layout map identifying non-public areas that protect CUI
- Plans of Action & Milestones (POA&Ms) and any External Service Provider CRMs

Selecting a C3PAO

Marketplace authorization is the floor, not the ceiling. Look for assessors with broad federal assessment experience, relevant industry familiarity, and a track record of well-run engagements. C3PAOs must achieve and maintain ISO/IEC 17020:2012 accreditation, and assessments are conducted by a lead assessor plus one or more team members—so plan for scheduling lead time and, for onsite work, assessor travel costs.

> **COST & DURATION DRIVERS**
>
> The size and complexity of your CUI environment is the primary cost driver—another reason tight scoping pays off. Poorly scoped engagements create evidence churn, rework, and extended timelines. The more of your environment that sits outside the CUI boundary (or inside an inherited, FedRAMP-certified enclave), the faster and less expensive the assessment.

Conditional vs. Final Certification

If you meet the 88 threshold but have a small number of eligible gaps, the C3PAO can issue a Conditional Level 2 status. You then have up to 180 days to close the POA&M, after which a closeout confirms Final status. A Final Level 2 certification is valid for three years, with an annual affirmation of continuous compliance required in SPRS throughout.

Your CMMC Progress Tracker

Use the three trackers below to manage your journey. Print this section or copy it into your project tooling. Fill the blank columns as you work—family by family, milestone by milestone—and log your SPRS score over time to show momentum toward 110.

1. Control-Family Readiness

Control Family	Reqs	Status	Owner	Target Date
AC Access Control	22			
AT Awareness & Training	3			
AU Audit & Accountability	9			
CM Configuration Management	9			
IA Identification & Authentication	11			
IR Incident Response	3			
MA Maintenance	6			
MP Media Protection	9			
PS Personnel Security	2			
PE Physical Protection	6			
RA Risk Assessment	3			
CA Security Assessment	4			
SC System & Communications Protection	16			
SI System & Information Integrity	7			

Status legend: Not Started • In Progress • Implemented • Documented & Evidenced

2. Milestone Tracker

Milestone	Target	Status	Notes
Assessment scope & asset inventory defined			
CUI data-flow & network diagrams complete			
System Security Plan (SSP) drafted			
Initial self-assessment & SPRS score submitted			
POA&M built for remaining gaps			
High-value (5- & 3-point) gaps remediated			
MFA (all users) & FIPS encryption in place			
Score ≥ 88 achieved			

Milestone	Target	Status	Notes
C3PAO selected & engagement scheduled			
Pre-assessment readiness review passed			
C3PAO assessment completed			
Conditional → Final status (POA&M closed)			

3. SPRS Score Log

Date	Score (/110)	Change	Notes

CMMC Readiness Checklist

A condensed, phase-by-phase checklist to track the whole journey from scoping to certification.

Phase 1: Scope

- ☐ Identify all CUI and Security Protection Data
- ☐ Map CUI data flows across people, technology, and facilities
- ☐ Categorize every asset into one of the five categories
- ☐ Produce a labeled network diagram and asset inventory
- ☐ Decide what to host in an external FedRAMP-certified enclave

Phase 2: Document

- ☐ Draft the System Security Plan (SSP) across all 14 families
- ☐ Write supporting policies and procedures
- ☐ Document External Service Providers and obtain their CRMs
- ☐ Justify any “not applicable” requirements in writing

Phase 3: Remediate & Score

- ☐ Run a gap assessment against all 110 requirements
- ☐ Close 5-point and 3-point gaps (not POA&M-eligible)
- ☐ Implement MFA for all users and FIPS-validated encryption
- ☐ Calculate your SPRS score and submit it via PIEE
- ☐ Build a POA&M for any remaining eligible 1-point gaps

Phase 4: Assess

- ☐ Confirm your score is ≥ 88
- ☐ Assemble the full evidence bundle (SSP, diagrams, inventory, POA&M)
- ☐ Select an authorized C3PAO and schedule the assessment
- ☐ Complete a pre-assessment readiness review

Phase 5: Certify & Maintain

- ☐ Complete the C3PAO assessment (Conditional or Final)
- ☐ Close any POA&M within 180 days to reach Final status
- ☐ Record your CMMC UID and certification in SPRS
- ☐ Complete the annual affirmation of continuous compliance
- ☐ Re-assess every three years and track changes to scope

How GovDataHosting Accelerates Your Path

GovDataHosting operates a FedRAMP High (Class D) Certified cloud platform purpose-built for government workloads. For defense contractors pursuing CMMC Level 2, it serves as a ready-made CUI enclave that meets—and exceeds—the FedRAMP Moderate baseline DFARS 252.204-7012 requires for cloud handling CUI.

Inherit Controls, Shrink Your Scope

When your CUI lives in our certified enclave, a large share of the underlying technical requirements are already implemented, assessed, and evidenced at the platform layer. Through our Customer Responsibility Matrix (CRM), you document exactly which control objectives we satisfy and which remain yours—so your assessment focuses on the application and process layer instead of rebuilding infrastructure controls from scratch.

What You Get	Why It Accelerates CMMC
FedRAMP High (Class D) Certified enclave	Exceeds the FedRAMP Moderate baseline DFARS 7012 requires for CUI; controls are pre-assessed.
Customer Responsibility Matrix (CRM)	Maps inherited vs. customer control objectives for your SSP—reducing documentation effort.
Reduced assessment boundary	Hosting CUI externally moves infrastructure out of your in-scope footprint, lowering cost and risk.
U.S. citizen support staff	U.S. persons supporting U.S. Cloud Data Centers Only—aligned to federal handling expectations.
Continuous monitoring (24/7 SOC)	Run by our 24/7 U.S.-based SOC—logging, vulnerability scanning, POA&M, and reporting that support your ongoing affirmations.
Single-source accountability	One partner for infrastructure, security, and compliance support—no multi-vendor finger-pointing.

THE BOTTOM LINE

The fastest contractors to a passing score are the ones who stop trying to secure everything themselves. By placing CUI in a FedRAMP-certified enclave and inheriting controls, you cut the most expensive and time-consuming part of CMMC—the infrastructure layer—and concentrate your effort where it earns the most score, the fastest.

Next Steps

Ready to map your fastest path to CMMC Level 2? Start with a conversation about your scope.

FREE CMMC SCOPING ASSESSMENT

Schedule a complimentary 30-minute consultation. We'll help you define your CUI boundary, estimate your SPRS score, and map the fastest path to a passing Level 2 assessment.

800-967-1004

www.govdatahosting.com/contact-us • **info@govdatahosting.com**

Additional Resources

Explore these companion guides from GovDataHosting:

- **FedRAMP Certification Playbook** — the step-by-step guide to FedRAMP Certification and 20x
- **Complete FISMA Authorization Guide** — NIST RMF, system categorization, and the ATO process
- **DFARS & CUI Compliance Checklist** — a quick-reference for 7012/7019/7020/7021 obligations

A Division of IT-CNP, Inc. • Founded 2001

FedRAMP High (Class D) Certified • NIST 800-53 High • DoD IL2 Authorized • SOC 2 Type II

© 2026 IT-CNP, Inc. All rights reserved.

DISCLAIMER

The information in this roadmap is accurate as of the date of publication. CMMC and DFARS requirements—including phase dates, scoring methodology, and the applicable revision of NIST SP 800-171—are evolving and subject to change. Always verify the latest requirements at authoritative sources, including dodcio.defense.gov/cmmc, sprs.csd.disa.mil, and nist.gov, before making compliance decisions. This document is informational and does not constitute legal or assessment advice.