# CMMC 2.0

## Penetration Testing Requirements

A guide for MSPs and defense contractors preparing for Phase 2 enforcement. Covers penetration testing requirements by level, scoping decisions, C3PAO evidence expectations, and MSP/ESP obligations under 32 CFR Part 170.

*Prepared in partnership with Secureframe*

## Contents

## 01 What Is CUI? A Key Definition

CONTROLLED UNCLASSIFIED INFORMATION

The Cybersecurity Maturity Model Certification (CMMC) 2.0 program is the DoD's framework for verifying that defense contractors and their suppliers have implemented cybersecurity requirements protecting Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). CMMC is built on NIST standards - Level 2 maps directly to the 110 controls in NIST SP 800-171 Rev 2, and Level 3 adds 24 enhanced controls from NIST SP 800-172.

Controlled Unclassified Information (CUI) is information the U.S. federal government creates or possesses - or that a non-federal entity creates or possesses on the government's behalf - that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government-wide policies, but that does not meet the standards for classified information.

The definition originates from Executive Order 13556 (2010), which established the CUI program now managed by the National Archives and Records Administration (NARA). In plain terms: CUI sits between publicly available and classified. It is sensitive but unclassified.

### Common Examples of CUI

- Technical drawings, specifications, or design data on defense contracts
- Export-controlled technical data governed by ITAR or EAR
- Law enforcement sensitive information
- Privacy Act information - Social Security numbers, personnel records, medical data
- Proprietary business information submitted to the federal government
- Critical infrastructure security information

| CUI IS NOT | CUI IS |
|---|---|
| Classified information (Top Secret, Secret, Confidential) Publicly available or uncontrolled data All company-internal information by default Information with no federal government nexus | Sensitive but unclassified - the category between public and classified Federally defined - controlled by law, regulation, or government-wide policy The specific trigger for CMMC Level 2 requirements Defined by approved category in the NARA CUI Registry at archives.gov/cui |

**WHY THIS DEFINITION MATTERS FOR SCOPING**

CUI is the boundary line for CMMC compliance. If your client's systems store, process, or transmit CUI - even temporarily - those systems fall within the CMMC assessment scope. The first step in any CMMC engagement is identifying what qualifies as CUI, where it flows, and which systems touch it. Getting this wrong means either failing the assessment for missed controls, or over-scoping and paying for compliance coverage that was not needed.

## 02 Enforcement Timeline

CMMC PHASED ROLLOUT: WHERE WE ARE NOW

CMMC implementation began November 10, 2025 with a four-phase rollout. Phase 2 - the critical deadline for most defense contractors - begins November 10, 2026, when mandatory C3PAO certification becomes required for Level 2 contracts.

| Phase | Timeline | Requirement |
|---|---|---|
| Phase 1 | Nov 10, 2025 - Nov 9, 2026 | Level 1 and 2 self-assessments in applicable solicitations. C3PAO assessments at contracting officer discretion for high-priority contracts. |
| Phase 2 | Nov 10, 2026 - you are here | Mandatory C3PAO Level 2 certification for applicable contracts involving CUI. Self-attestation no longer accepted for most CUI contracts. |
| Phase 3 | Nov 10, 2027 | Level 3 DIBCAC certification requirements introduced for critical programs and high-value assets handling the most sensitive CUI. |
| Phase 4 | Nov 10, 2028 | Full CMMC implementation across all applicable DoD solicitations. CMMC level is a mandatory condition of contract award. |

**MSP ACTION ITEM FOR NOVEMBER 2026**

Your clients handling CUI need a completed C3PAO Level 2 certification before contract renewal or new award. C3PAO booking windows are already stretching 3-6 months - some assessors are reporting 6-8 month waits for new clients. Organizations that start preparation in Q3 2026 will miss contracts. If your clients have not begun, the time is now.

## 03 Requirements by Level

WHAT CMMC REQUIRES FOR PENETRATION TESTING

CMMC's pentest requirements differ significantly by level. At Level 2 - where most contractors operate - the requirement is indirect but practically expected by C3PAOs. Here is how it breaks down:

| Level | Control Count | Pentest Requirement | Assessment Type | Enforcement |
|---|---|---|---|---|
| **Level 1 Foundational** | 17 controls (FAR 52.204-21) | No pentest required | Annual self-assessment + SPRS entry | Annual self-attestation only |

| | | | | |
|---|---|---|---|---|
| **Level 2 Advanced** | 110 controls (NIST SP 800-171 Rev 2) | Not explicitly mandated - but strongly expected. C3PAOs evaluate CA.L2-3.12.1 (security assessments) and RA.L2-3.11.2 (vulnerability scanning) | C3PAO certification every 3 years + annual affirmation | Mandatory C3PAO from Nov 10, 2026 |
| **Level 3 Expert** | 110 + 24 controls (NIST SP 800-172) | Penetration testing explicitly required under CA.L3-3.12.1e. Must be threat-informed, APT-simulating, annually recurring, with full evidence chain | DIBCAC government assessment every 3 years | Introduced Nov 10, 2027 |

## 04 Level 2 Deep Dive

WHY PENTEST MATTERS EVEN WITHOUT AN EXPLICIT MANDATE

CMMC Level 2 does not use the word 'penetration test' in its control list - but two controls together create a strong practical expectation that your clients will have one:

### CA.L2-3.12.1 - Security Assessments

Requires periodic assessment of security controls to determine effectiveness. C3PAOs interpret this as requiring technical validation that controls actually work - not just documented policies. A pentest is the most defensible form of evidence for a significant subset of controls, particularly those governing access control, network boundaries, authentication, and incident detection.

### RA.L2-3.11.2 - Vulnerability Scanning

Requires regular vulnerability scans of organizational systems. While scanning is distinct from pentesting, C3PAOs assess these together. Clients who only run scans and have never tested whether findings can be exploited are exposed - assessors ask what was done with scan results, and a pentest cycle that validates remediation is the cleanest answer.

**THE REAL RISK AT LEVEL 2**

A C3PAO can mark a control as NOT MET if they cannot find sufficient evidence that it functions as intended. Policies alone rarely satisfy a technical assessor. Penetration testing produces the kind of hands-on evidence - proof-of-exploitation, attack path documentation, and remediation verification - that most clearly demonstrates controls hold under real-world conditions.

### What C3PAOs Are Looking For in Practice

Based on how the 110 controls map to real assessments, clients going into a C3PAO assessment should expect technical scrutiny around:

- Access controls - can privilege escalation be achieved? Are separation boundaries enforced?

- Network segmentation - is CUI genuinely isolated from non-CUI assets?
- Multi-factor authentication - is it bypassable via common techniques?
- Audit logging and detection - would an attack be detected and recorded?
- Incident response - is there evidence the IR plan has been tested?
- Patch and vulnerability management - has remediation been verified, not just tracked?

## 05 Level 3 Requirements

PENETRATION TESTING IS EXPLICITLY REQUIRED

Level 3 applies to contractors handling CUI associated with critical programs or high-value assets. It builds on all 110 Level 2 controls and adds 24 enhanced requirements from NIST SP 800-172, assessed by the Defense Contract Management Agency's DIBCAC - not a commercial C3PAO.

### CA.L3-3.12.1e - The Explicit Pentest Control

NIST SP 800-172 places this control within its penetration-resistant architecture strategy. It requires:

- Annual penetration testing, at minimum
- Testing must be threat-informed - simulating the specific tactics, techniques, and procedures (TTPs) of Advanced Persistent Threat (APT) actors
- Generic scanning tools and standard vulnerability assessments do not satisfy this control
- Testers must have demonstrated APT expertise, including working knowledge of MITRE ATT&CK; behaviors relevant to defense contractor environments
- A complete evidence chain: test report, remediation records, and documentation that testing recurs on schedule

**LEVEL 3 PENTEST IS NOT A COMMERCIAL ENGAGEMENT**

Standard commercial penetration testing does not satisfy CA.L3-3.12.1e. If your client handles CUI on a critical program, they need testers with real threat-intel-driven methodology, APT simulation capability, and the ability to produce a report that a DIBCAC assessor can trace back to specific TTPs and attack scenarios.

### The Three Pillars of NIST SP 800-172 Your Pentest Must Address

| Pillar | What It Means | Testing Focus |
|---|---|---|
| Penetration-Resistant Architecture (PRA) | Can one compromised component hand an attacker the rest of the environment? | Isolation validation, dual-authorization for high-impact actions, boundary controls between security domains |
| Damage-Limiting Operations (DLO) | How quickly can the defender detect and contain a breach? | Detection capability, lateral movement constraints, data exfiltration barriers |

| | | |
|---|---|---|
| Designing for Cyber Resiliency | Can the environment recover and maintain mission capability during an attack? | Backup integrity, failover controls, resilience mechanisms under active attack simulation |

## 06 Assessment Scoping

HOW TO SCOPE A CMMC PENTEST

Scoping is the most consequential decision in a CMMC assessment. Only systems that store, process, or transmit CUI - and systems that protect them - need to be in scope. Getting scope right reduces cost and assessment complexity. Getting it wrong means failed controls or scope creep that derails certification.

The CMMC Level 2 Scoping Guide (DoD) defines five asset categories. Your pentest scope should mirror the CMMC assessment boundary:

| Asset Category | Description | Pentest Implication |
|---|---|---|
| CUI Assets | Any system, endpoint, or application that stores, processes, or transmits Controlled Unclassified Information | Always in scope - the core of the assessment boundary |
| Security Protection Assets | Systems that protect the CUI environment: firewalls, IAM, SIEM, EDR, MFA infrastructure, SSO platforms | In scope - controls must be tested and validated |
| Contractor Risk Managed Assets | Assets that could impact the CUI environment if compromised but do not directly touch CUI | In scope at L2 assessment - risk must be documented and assessed |
| Cloud Service Provider (CSP) Platforms | Any cloud platform storing or processing CUI (M365, AWS GovCloud, Azure, etc.) | Must meet FedRAMP Moderate equivalency; CSP's boundary is part of the CMMC scope |
| External Service Providers (ESPs / MSPs) | MSPs managing IT infrastructure, security tools, or endpoints within the CUI environment | In scope if they handle CUI or Security Protection Data; must be included in SSP and Shared Responsibility Matrix |
| Out-of-Scope Assets | Systems fully isolated from CUI with no logical or physical connection | Must demonstrate documented, verifiable segmentation - segmentation itself should be validated in the pentest |

**SEGMENTATION IS NOT FREE**

Many clients assume that systems outside the CUI enclave are automatically out of scope for the pentest. That is only true if segmentation is verifiably enforced. Testing whether an out-of-scope system can actually reach CUI assets is a legitimate and often expected part of the engagement - especially for C3PAO readiness.

## 07 The CMMC-Ready Pentest Package

WHAT A CMMC PENTEST SHOULD INCLUDE

### Core Testing Components

- External network pentest - public-facing assets, internet-exposed services, email infrastructure
- Internal network pentest - lateral movement, privilege escalation, segmentation validation
- Web application / API pentest - any application that handles FCI/CUI or authenticates into the CUI environment
- Cloud configuration review - M365 GCC/GCC High, Azure, AWS GovCloud configurations, conditional access policies, sharing permissions
- Boundary and segmentation validation - confirm CUI enclave isolation holds under active testing
- Credentialed testing - validates authentication controls and internal privilege boundaries
- Remediation retest - documented verification that identified findings were resolved

### CMMC Controls Your Pentest Report Should Address

| Control | What the Pentest Demonstrates |
|---|---|
| CA.L2-3.12.1 | Evidence that security controls were technically assessed and validated |
| RA.L2-3.11.2 | Confirmation that vulnerability findings were identified, remediated, and verified |
| AC.L2 controls | Proof that access control boundaries hold under active exploitation attempts |
| SC.L2-3.13.1 / SC.L2-3.13.3 | Network segmentation and boundary protection validated |
| SI.L2-3.14.6 / SI.L2-3.14.7 | Security monitoring and malicious code detection tested |

### What the Report Must Contain for C3PAO Review

- Clearly scoped authorization boundary matching the client's System Security Plan (SSP)
- Methodology and tools used - assessors want to know how testing was performed
- Exploitable attack paths with proof-of-exploitation artifacts
- Risk-rated findings with business impact assessment
- Remediation guidance mapped to CMMC/NIST controls
- Retest confirmation with dated evidence of fixes validated

## 08 MSP and ESP Obligations

WHAT MSPS NEED TO KNOW ABOUT THEIR OWN CMMC POSITION

The CMMC final rule (32 CFR Part 170) removed the term 'MSP' and replaced it with the broader category of External Service Provider (ESP). Where your firm lands in the CMMC picture depends entirely on what you handle on behalf of your clients.

### The Key Question: Do You Touch CUI?

- If your MSP stores, processes, or transmits CUI on your own systems - you are an ESP and need your own CMMC Level 2 assessment
- If your MSP manages IT/security infrastructure inside the client's CUI environment but does not handle CUI on your own systems - you are in scope for the client's assessment
- If you provide services with no contact with CUI or Security Protection Data (SPD) - you are generally out of scope, but your services must be documented in the client's SSP

Pentesters, IR firms, and assessors who access a client's environment only temporarily are explicitly carved out - they are not considered ESPs and do not need CMMC certification.

**SHARED RESPONSIBILITY MATRIX (SRM) - NON-OPTIONAL**

Every MSP relationship that touches the CMMC assessment boundary must be documented in a Shared Responsibility Matrix. The SRM maps which party (client or MSP) is responsible for each of the 320 NIST 800-171A assessment objectives. C3PAOs will ask for it. Very few MSPs have one ready today - preparing it proactively is one of the highest-value things an MSP can do to help clients prepare for assessment.

## 09 Readiness Timeline

WORKING BACKWARDS FROM NOVEMBER 10, 2026

As of July 2026, approximately 80,000 contractors need Level 2 C3PAO certification. Fewer than 500 have completed it. There are fewer than 100 authorized C3PAOs, with booking windows stretching 3-8 months. The math is stark.

| Timeframe | What Should Be Done |
|---|---|
| 12+ months out | Gap assessment against NIST 800-171 Rev 2. Score in SPRS. Define CUI enclave. Begin remediation of high-priority gaps. Identify C3PAO and get on their calendar. |
| 9-12 months out | Complete SSP. Build Shared Responsibility Matrix with MSP. Identify and remediate critical control gaps. Commission internal readiness pentest against CMMC scope. |
| 6-9 months out | Remediate pentest findings. Conduct retest. Finalize all CMMC documentation (POA&M;, CUI flow diagrams, asset inventory). Confirm C3PAO booking. |
| 3-6 months out | Final review of SSP vs. implemented controls. Conduct mock assessment. Provide pentest report and remediation evidence to C3PAO pre-assessment. |
| 0-3 months out | C3PAO assessment window. Ensure evidence is organized, current, and traceable. Have pentest retest confirmation documentation available for assessor review. |
| Post-certification | Annual affirmation of compliance. Annual vulnerability scanning. Pentest on any significant architecture changes. 3-year reassessment cycle begins. |

## 10 CMMC vs. FedRAMP: Framework Comparison

KEY DIFFERENCES FOR MSPS SUPPORTING BOTH PROGRAMS

MSPs often support clients across both CMMC and FedRAMP Moderate environments. Understanding how the two frameworks handle pentesting helps you scope correctly and avoid under- or over-delivering.

| | CMMC Level 2 | NIST 800-53 Moderate (FedRAMP) |
|---|---|---|
| **Underlying standard** | NIST SP 800-171 Rev 2 (110 controls) | NIST SP 800-53 Rev 5 (325 controls at Moderate) |
| **Pentest explicitly required?** | No - but strongly expected by C3PAOs | Yes - CA-8 is a required control |
| **Who conducts the assessment?** | C3PAO (accredited commercial 3PAO) | 3PAO accredited by A2LA / FedRAMP PMO |
| **Assessment cadence** | Every 3 years + annual affirmation | Annual assessment + continuous monitoring |
| **Pentest cadence** | Recommended annually; triggered by significant changes | At least annually; triggered by significant changes |
| **Tester citizenship requirement** | No federal requirement; agency-specific rules may apply | No federal requirement; agency-specific rules may apply |
| **Cloud service requirement** | FedRAMP Moderate equivalency for CSPs handling CUI | FedRAMP authorization (or agency ATO) |
| **Key pentest controls** | CA.L2-3.12.1, RA.L2-3.11.2 | CA-8, RA-5, CA-2, SI-2, SI-4, SC-7 |

## 11 Resources

CMMC COMPLIANCE AND PENTESTING REFERENCES

**DoD CMMC Program Page** dodcio.defense.gov/CMMC

The official DoD source for CMMC requirements, phased implementation timeline, and links to scoping guides and assessment guides for Levels 1-3. Primary source for all CMMC compliance decisions.

**Secureframe: CMMC Hub and FedRAMP 20x Roadmap** secureframe.com

GRC automation platform with strong neutral explainers on CMMC Level 2 requirements, C3PAO process, and FedRAMP overlap. Useful for client conversations and tracking readiness progress.

**Software Secured: NIST SP 800-115 and Pentesting** softwaresecured.com

Explains the testing methodology standard (800-115) that underlies compliant pentesting for NIST-based frameworks including CMMC. Covers what independent testing actually means in practice beyond what a scan delivers.

**DoD CMMC Scoping Guide Level 2** dodcio.defense.gov

Official DoD scoping guidance defining the five asset categories and how to determine what belongs inside vs. outside the CMMC assessment boundary. Essential for defining the CUI enclave.

**DoD CMMC FAQ: MSPs and External Service Providers (Q33-Q37)** dodcio.defense.gov/CMMC

Official DoD FAQ covering how the final rule (32 CFR Part 170) classifies MSPs as External Service Providers and when they need their own CMMC assessment. The primary source for every MSP asking: do I need my own certification?

**NIST SP 800-171 Rev 2: Protecting CUI in Nonfederal Systems** csrc.nist.gov

The underlying 110-control standard that CMMC Level 2 maps to directly. Essential reading for understanding what each control requires and how to build evidence that satisfies a C3PAO assessor.

**NIST SP 800-172: Enhanced Security for CUI** csrc.nist.gov

The 24 enhanced controls that CMMC Level 3 adds on top of Level 2. Covers CA.L3-3.12.1e (the explicit penetration testing requirement), penetration-resistant architecture, and damage-limiting operations. Required reading for any Level 3 engagement.

### About Software Secured

Software Secured is a Canadian penetration testing company specializing in manual security testing for high-growth SaaS companies and regulated environments. We help technical teams find real vulnerabilities - not just run scans. Our engagements are scoped and reported to satisfy NIST, CMMC, SOC 2, and FedRAMP evidence requirements.

softwaresecured.com