CMMC Level 2 Compliance Guide

CoreReconOS | Texas Defense Contractors | NIST SP 800-171 Rev 2/3

CMMC Level 2 Enforcement: November 10, 2026 | SDVOSB Certified

Texas Defense Corridor

The Fort Worth–Dallas corridor anchors a $40B+ annual DoD supply chain. Lockheed Martin Fort Worth builds the F-35 and F-16 Fighting Falcon — every tier-1, -2, and -3 supplier in that chain is CMMC-gated. BAE Systems, L3Harris, and Bell Textron add to the regional defense supplier base. Hundreds of small and mid-sized Texas contractors — wiring, avionics, logistics, maintenance — are in active CMMC Level 2 scope.

CMMC Level 2 enforcement begins November 10, 2026. Contract-gating starts before that: prime contractors (Lockheed, BAE, L3Harris) are embedding CMMC Level 2 requirements into subcontract agreements now. Defense subs without a credible compliance path face contract non-renewal — not at enforcement date, but at the next option period.

SPRS (Supplier Performance Risk System) scores are visible to contracting officers today. A self-attestation score of 110 is maximum; most defense subs are below 70. Low SPRS scores already affect contract decisions. C3PAO third-party assessment is required for programs handling CUI at Level 2.

SDVOSB — We've Been Through the Process

CoreReconOS is SDVOSB-certified (Service-Disabled Veteran-Owned Small Business). We understand DoD contracting, DIBCAC assessment processes, and the DFARS 252.204-7012 clause — because we are a veteran-owned shop that has navigated these requirements ourselves. That context is in every assessment, every remediation plan, every conversation.

14 CMMC Level 2 Control Domains

1. Access Control (AC — 22 practices)

Assessors look for: Limit system access to authorized users, processes, and devices; enforce least privilege; control remote access flows
Common gaps: Shared credentials, no MFA for remote access, overly broad user permissions without role assignments
Sentinel: RBAC enforcement, least-privilege audit, credential hygiene monitoring
Fortress adds: Privileged access management, session recording, just-in-time access provisioning
Command delivers: Continuous access analytics, SOC-validated access reviews, anomalous login alerting with 30-min response SLA

2. Awareness & Training (AT — 3 practices)

Assessors look for: All personnel with CUI access complete role-based security training; records documented and retained
Common gaps: Training completed but undocumented, contractors excluded, no annual refresh cadence
Sentinel: Training program management, documentation automation, annual refresh reminders
Fortress adds: Role-specific CUI training modules, contractor onboarding workflows
Command delivers: Continuous threat-awareness briefings, SDVOSB-sourced DoD-context training content

3. Audit & Accountability (AU — 9 practices)

Assessors look for: Audit logs capturing user actions, failed logins, and CUI access; 90-day minimum retention; regular review
Common gaps: Insufficient log retention, no user-level audit trails, logs not reviewed, no SIEM correlation
Sentinel: Automated log collection and 90-day retention, user activity tracking, monthly compliance reports
Fortress adds: SIEM log correlation, alerting on anomalous access patterns, 1-year retention
Command delivers: SOC-monitored audit streams, real-time anomaly detection, DoD-audit-ready evidence packages

4. Configuration Management (CM — 9 practices)

Assessors look for: Documented baseline configurations for all systems handling CUI; formal change management process; no

unauthorized software
Common gaps: No formal baseline, ad-hoc changes without approval, unknown software inventory, no CMDB
Sentinel: Software inventory tracking, policy enforcement for configuration standards
Fortress adds: CMDB implementation, change approval workflow, baseline deviation alerts, unauthorized software blocking
Command delivers: Continuous configuration drift detection, SOC-validated change management, DoD STIG alignment

5. Identification & Authentication (IA — 11 practices)

Assessors look for: Unique user IDs for all personnel; multi-factor authentication for remote and privileged access; password standards enforced
Common gaps: Shared accounts on CUI systems, no MFA for remote sessions, weak or default passwords
Sentinel: Unique ID enforcement, password policy automation, MFA deployment support
Fortress adds: MFA enforcement across all remote access vectors, identity governance workflows
Command delivers: Continuous identity anomaly monitoring, real-time MFA failure alerting, 30-min response SLA

6. Incident Response (IR — 3 practices)

Assessors look for: Documented IR plan, defined response roles, 24/7 capability, incident reporting to DoD/DCSA within required windows
Common gaps: No formal IR plan, response times undefined, no DCSA reporting mechanism, untested procedures
Sentinel: IR plan templates, incident logging, response role documentation
Fortress adds: Tabletop exercise support, escalation workflows, DCSA reporting procedures
Command delivers: 24/7 SOC, 30-min detection-to-response SLA, DoD DIBCAC-aligned incident reporting, veteran analyst team

7. Maintenance (MA — 6 practices)

Assessors look for: Controlled and logged maintenance of CUI systems; remote maintenance sessions authenticated and monitored
Common gaps: Undocumented maintenance by third-party vendors, unmonitored remote sessions, no approval workflow
Sentinel: Maintenance logging, third-party vendor access tracking
Fortress adds: Remote maintenance session monitoring, approval workflows, vendor access controls
Command delivers: SOC-supervised maintenance windows, real-time session recording, vendor security assessments

8. Media Protection (MP — 9 practices)

Assessors look for: CUI stored on encrypted media; physical media destruction certified; media accountability logs maintained
Common gaps: Unencrypted USB/portable drives, no destruction certificates, media not inventoried or tracked
Sentinel: Media encryption enforcement, chain-of-custody logging, certified destruction procedures
Fortress adds: Media sanitization workflows, encrypted portable storage provisioning
Command delivers: Continuous media audit, SOC-validated data destruction, DoD-compliant sanitization documentation

9. Personnel Security (PS — 2 practices)

Assessors look for: Background screening before CUI access; access revoked within 24 hours of termination; personnel security agreements on file
Common gaps: No formal clearance verification process, access not revoked on separation, personnel agreements missing
Sentinel: Background check tracking, termination checklists, access revocation workflow
Fortress adds: Automated access revocation on HR trigger, personnel security agreement management
Command delivers: Veteran-led insider threat awareness program, continuous personnel anomaly monitoring

10. Physical Protection (PE — 6 practices)

Assessors look for: CUI systems in controlled facility areas; visitor logging; badge access systems; escort procedures for uncleared personnel
Common gaps: No badge access controls, visitor logs incomplete, CUI workstations in open areas, no escort policy
Sentinel: Physical security assessment, workstation placement standards, badge access guidance
Fortress adds: Facility security design review, visitor management system integration
Command delivers: On-site physical security assessment, SDVOSB-sourced DoD-facility compliance review

11. Risk Assessment (RA — 5 practices)

Assessors look for: Documented risk assessment against NIST SP 800-171 Rev 2/3; periodic reassessment; risks tracked to remediation
Common gaps: No formal risk assessment, one-time assessment not refreshed annually, findings not tracked to closure
Sentinel: Risk assessment framework, finding tracking, remediation prioritization
Fortress adds: Annual risk assessment execution, POAM (Plan of Action & Milestones) management
Command delivers: Continuous risk posture monitoring, SPRS score management, DIBCAC pre-assessment simulation

12. Security Assessment (CA — 4 practices)

Assessors look for: System Security Plan (SSP) documenting all CMMC practices; POAM for gaps; periodic security control testing
Common gaps: No SSP, POAM not maintained, security controls not tested, no evidence packages for assessors
Sentinel: SSP template and baseline documentation, POAM tracking

Fortress adds: Full SSP authoring, evidence collection automation, control testing procedures
Command delivers: DIBCAC C3PAO assessment readiness package, SOC-supported evidence generation, $2,500 assessment credit toward C3PAO prep

13. System & Communications Protection (SC — 16 practices)

Assessors look for: Network segmentation for CUI systems; encrypted communications; firewall rules documented; VPN for remote CUI access
Common gaps: No CUI network segmentation, unencrypted internal communications, firewall rules undocumented, remote access without VPN
Sentinel: Firewall baseline documentation, VPN enforcement, encryption standards
Fortress adds: CUI network segmentation design, firewall management, IDS/IPS deployment
Command delivers: Continuous perimeter monitoring, SOC-managed network security, real-time threat blocking with 30-min SLA

14. System & Information Integrity (SI — 7 practices)

Assessors look for: Anti-malware deployed and updated; security alerts monitored; patches applied in a defined timeframe; spam protection
Common gaps: Anti-malware not centrally managed, patches delayed beyond 30 days, no centralized security alerting
Sentinel: Anti-malware management, patch tracking, security alert consolidation
Fortress adds: Automated patch enforcement, vulnerability scanning, centralized alert management
Command delivers: 24/7 SOC threat monitoring, zero-day detection, sub-30-min response to integrity alerts

Self-Assessment Checklist

Run through these 8 questions before booking your C3PAO or CoreReconOS assessment:

1. System Security Plan (SSP)
Have you documented all 110 NIST SP 800-171 Rev 2 practices in a written SSP?
Risk if No: Without an SSP, C3PAO assessment cannot begin — and contracting officers can request it at any time.

2. CUI Identification
Have you formally identified all locations (systems, shared drives, email, physical) where Controlled Unclassified Information is stored or transmitted?
Risk if No: Unidentified CUI flows are the #1 source of CMMC gaps found during assessments.

3. MFA on Remote Access
Is multi-factor authentication enforced on every remote access path into systems that handle CUI?
Risk if No: Missing MFA on a single VPN or remote desktop session is a Level 2 finding.

4. SPRS Self-Assessment
Have you submitted a current NIST SP 800-171 self-assessment score to SPRS within the last 12 months?
Risk if No: A stale or missing SPRS entry is visible to DoD contracting officers and can block contract awards.

5. Incident Reporting
Do you have a documented plan for reporting CUI incidents to DoD/DCSA within the 72-hour window?
Risk if No: 72-hour breach reporting is a DFARS 252.204-7012 contractual obligation, not just a CMMC requirement.

6. Patch Management
Are all systems handling CUI patched within your defined SLA (typically 30 days for critical)?
Risk if No: Unpatched systems processing CUI are a direct path to Level 2 non-compliance and contract risk.

7. Network Segmentation
Is your CUI environment isolated on a segmented network, separate from guest or general business traffic?
Risk if No: Flat networks where CUI mingles with general business traffic fail multiple SC domain controls.

8. POAM
Do you maintain an active Plan of Action & Milestones tracking all known gaps to remediation?
Risk if No: A POAM is required evidence for C3PAO assessment. Missing one signals no governance program.

John Martinez
CEO & Founder, CoreReconOS
SDVOSB Certified | AT&T Vendor for State of Texas Incident Response
corerecon@polsia.app | corerecon.polsia.app