

Defense Contractor CMMC 2.0 Level 2 & CUI Enclave Readiness Checklist

10 High-Assurance Engineering Controls to Satisfy All 110 NIST SP 800-171 Requirements, Maximize SPRS Scores, and Pass C3PAO Assessments.

110 / 110

NIST SP 800-171 Controls Mapped

70% Less

C3PAO Audit Scope via CUI Enclave

72-Hour SLA

DFARS 7012 DoD Cyber Reporting

4 Minutes

U.S.-Based 24/7 MDR Isolation

**01. Controlled Unclassified Information (CUI) Enclave Boundary Segmentation**

[] PASS [] GAP / REMEDIATE

Isolate CUI/ITAR CAD, ERP, and contract files inside a dedicated enclave so 70% of non-CUI commercial endpoints are removed from C3PAO assessment scope.

**02. Microsoft 365 GCC High & Azure Government Sovereign Hosting (DFARS 7012)**

[] PASS [] GAP / REMEDIATE

Ensure all CUI email, SharePoint, Teams, and cloud workloads reside in FedRAMP High sovereign environments staffed exclusively by U.S. persons.

**03. FIPS 140-2 / 140-3 Validated Cryptography Across All CUI Paths (SC.L2-3.13.11)**

[] PASS [] GAP / REMEDIATE

Enforce FIPS-validated cryptographic modules for BitLocker/FileVault disk encryption, SASE/VPN tunnels, and TLS data in transit.

**04. Phishing-Resistant FIDO2 MFA for Privileged & Non-Privileged Enclave Access (IA.L2-3.5.3)**

[] PASS [] GAP / REMEDIATE

Deploy hardware-bound FIDO2 security keys or Windows Hello for Business across all local, network, and cloud access to CUI repositories.

**05. Live 110-Control System Security Plan (SSP) & POA&M Evidence Engine**

[] PASS [] GAP / REMEDIATE

Maintain a live SSP mapped to all 320 NIST SP 800-171A assessment objectives with automated screenshot/log artifacts and strict 180-day POA&M closeout tracking.

**06. Verified SPRS Score Calculation & False Claims Act Defensibility**

[] PASS [] GAP / REMEDIATE

Ensure your Supplier Performance Risk System (SPRS) score is backed by live technical telemetry rather than aspirational self-attestation.

**07. 24/7 U.S.-Citizen SOC Monitoring & 72-Hour DIBNet Incident Reporting**

[] PASS [] GAP / REMEDIATE

Monitor enclave endpoints and identity logs 24/7 with <4-minute host isolation and forensic packet preservation required for 72-hour DoD DIBNet reporting.

**08. CAD / CAM / ERP Engineering Workload Hardening (SolidWorks, AutoCAD, JobBOSS)**

[] PASS [] GAP / REMEDIATE

Enforce application allowlisting, USB/removable media cryptographic blocks, and high-IOPS segmented VLANs for CNC shop-floor and PDM servers.

**09. Sub-24-Hour CISA KEV Remediation & Continuous Vulnerability Scanning (RA.L2-3.11.2)**

[] PASS [] GAP / REMEDIATE

Patch critical vulnerabilities within 24 hours and export monthly authenticated vulnerability scan reports directly into your C3PAO evidence binder.

**10. Immutable Air-Gapped CUI Backups & Quarterly Restoration Testing (CP.L2-3.8.9)**

[] PASS [] GAP / REMEDIATE

Protect CUI backups with FIPS-validated encryption and immutable Object-Lock, verified every 90 days via documented test restorations.