

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 for CUI (DFARS 7012 FedRAMP Moderate)

[] PASS [] GAP / REMEDIATE

DFARS 252.204-7012 requires cloud services that hold CUI to meet the FedRAMP Moderate baseline or its equivalent (DoD memo, Dec. 21, 2023). GCC High and Azure Government are FedRAMP High authorized, exceeding that bar, and add screened U.S.-person support for ITAR data.



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 KEV Remediation & Continuous Vulnerability Scanning (RA.L2-3.11.2/3.11.3)

[] PASS [] GAP / REMEDIATE

Emry recommends patching KEV-listed vulnerabilities within 24 hours (CISA's KEV deadlines bind federal civilian agencies only) and exporting monthly authenticated vulnerability scan reports directly into your C3PAO evidence binder.



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

[] PASS [] GAP / REMEDIATE

Protect the confidentiality of backup CUI (MP.L2-3.8.9) with FIPS-validated encryption and immutable Object-Lock, verified every 90 days via documented test restorations.