EMRY NETWORKS
IT Solutions That Click

2026 DEFENSE INDUSTRIAL BASE GUIDE • CMMC 2.0 LEVEL 2 & NIST SP 800-171

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.

CMMC 2.0 LEVEL 2 • NIST 800-171 • DFARS 252.204-7012

110 / 110	**70% Less**	**72-Hour SLA**	**4 Minutes**
NIST SP 800-171 Controls Mapped	C3PAO Audit Scope via CUI Enclave	DFARS 7012 DoD Cyber Reporting	U.S.-Based 24/7 MDR Isolation

WHAT'S INSIDE

- How to use this checklist and assessment details — p. 2
- 1 The 10 controls: status, owner, target date and evidence — p. 3
- 2 Your results and open items — p. 5
- Rules cited, related resources and next step — p. 6

Book a 30-Minute Risk Assessment →

USING THE INTERACTIVE VERSION

- **Type in any shaded box.** Press Tab to move to the next one.
- **Blue-outlined boxes are drop-downs** for each control's status.
- **Grey boxes calculate themselves:** the counts, readiness % and open items on your Results page.
- **Best in Adobe Acrobat Reader (free)** or another desktop PDF app. Browser viewers and Apple Preview let you type, but may not run the calculations; you can type those values in yourself.
- **Use the links** in the contents list, the header (Contents, Results) and the bookmarks panel to jump around.
- **Save often.** Prints on US Letter, landscape; the on-screen buttons do not print.

Print checklist | Clear all entries

STATUS KEY

In place: Implemented today and you can show evidence. Earns all of the control's points.
Partial: Started, or covers only some users, systems or sites. Earns 40% of the control's points.
Gap: Not in place yet. Earns 0 points, the same as a control you have not marked.
N/A: No CUI in that scope. Offered only on controls 02 and 08, and counts as met, the way DoD scores N/A.

How to use this checklist

NIST SP 800-171 · DFARS 252.204-7012

1. Mark a status for each control. Use the drop-down next to each of the 10 controls: In place, Partial or Gap (N/A only where it is offered).

2. Assign the work. For anything Partial or a Gap, name an owner and a target date.

3. Note the evidence. Say where the proof lives (policy, screenshot, report, contract), so you can produce it on request.

4. Review your results. The Results page counts your answers, works out a weighted, self-rated readiness % and lists the open items.

5. Get a second opinion. Bring the results to a 30-minute risk assessment if you want an outside review.

Assessment details

Company / CAGE code(s)		**Date completed**	
Completed by (name, title)		**Next review date**	
Enclave / SSP name and version		**Reviewed with (RPO, C3PAO, counsel)**	

The controls at a glance

01 Controlled Unclassified Information (CUI) Enclave Boundary Segmentation
02 Microsoft 365 GCC High & Azure Government for CUI (DFARS 7012 FedRAMP Moderate)
03 FIPS 140-2 / 140-3 Validated Cryptography Across All CUI Paths (SC.L2-3.13.11)
04 Phishing-Resistant FIDO2 MFA for Privileged & Non-Privileged Enclave Access (IA.L2-3.5.3)
05 Live 110-Control System Security Plan (SSP) & POA&M Evidence Engine
06 Verified SPRS Score Calculation & False Claims Act Defensibility
07 24/7 U.S.-Citizen SOC Monitoring & 72-Hour DIBNet Incident Reporting
08 CAD / CAM / ERP Engineering Workload Hardening (SolidWorks, AutoCAD, JobBOSS)
09 Sub-24-Hour KEV Remediation & Continuous Vulnerability Scanning (RA.L2-3.11.2/3.11.3)
10 Immutable Air-Gapped CUI Backups (MP.L2-3.8.9) & Quarterly Restoration Testing

Disclaimer

This checklist is an educational self-check, not legal advice, a certification, or a formal assessment. Confirm requirements against the current regulation, your contracts, and your assessor or counsel. © 2026 Emry Networks.

1 The 10 controls

NIST SP 800-171 · DFARS 252.204-7012

For each control, pick a status, then add an owner, a target date and where the evidence lives. Your answers feed the Results page.

01. Controlled Unclassified Information (CUI) Enclave Boundary Segmentation

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.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

02. Microsoft 365 GCC High & Azure Government for CUI (DFARS 7012 FedRAMP Moderate)

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.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

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

Enforce FIPS-validated cryptographic modules for BitLocker/FileVault disk encryption, SASE/VPN tunnels, and TLS data in transit. NIST moved all FIPS 140-2 certificates to its Historical List in September 2026; they remain supported for existing systems, so specify FIPS 140-3 validated modules for new deployments.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

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

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

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

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

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.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

06. Verified SPRS Score Calculation & False Claims Act Defensibility

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

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

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

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

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

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

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

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

09. Sub-24-Hour KEV Remediation & Continuous Vulnerability Scanning (RA.L2-3.11.2/3.11.3)

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.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

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

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.

STATUS · 1 PT | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

2 Your results and open items

Calculated from the 10 controls

These totals fill in automatically from your answers in Adobe Acrobat Reader and most desktop PDF apps. If a box stays blank in your viewer, count from the controls pages and type or write the number in. Readiness is your own self-assessment, not a compliance determination.

In place	Partial	Gap	N/A	Assessed (controls marked)	Readiness (self-rated)	Gaps and partials with no owner

Points:

Readiness = points earned ÷ points available. Each control is worth 5, 3 or 1 points (shown next to its status). In place earns all of its points, Partial earns 40%, and a Gap or an unmarked control earns 0, so the score climbs from 0% as you mark controls. N/A counts as met, as in DoD's NIST SP 800-171 scoring. Control 05 is required for any score: DoD's methodology says an assessment cannot be completed without a System Security Plan (3.12.4).

Open items to close (calculated: Gaps first, then Partials, with owner and target date)

Sign-off

Reviewed by (name, title)	
Signature / date	
Date of next review	

Rules and documents cited in this checklist

Official sources for the rules, standards and documents named in the controls above. Check them for updates before relying on any requirement.

NIST SP 800-171 Rev. 2: https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
NIST SP 800-171A (assessment procedures and objectives): https://csrc.nist.gov/pubs/sp/800/171/a/final
DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting:
https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
DoD CIO memo: FedRAMP Moderate Equivalency for Cloud Service Offerings (Dec. 21, 2023): https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf
DoD CIO: Cybersecurity Maturity Model Certification (CMMC): https://dodcio.defense.gov/cmmc/
NIST Cryptographic Module Validation Program (FIPS 140-2 / 140-3): https://csrc.nist.gov/projects/cryptographic-module-validation-program
DoD DIBNet (cyber incident reporting): https://dibnet.dod.mil/
CISA Known Exploited Vulnerabilities (KEV) Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Sources for the figures on the cover

110 / 110: NIST SP 800-171 Rev. 2 contains 110 security requirements (the set CMMC Level 2 assesses, 32 CFR 170.14). https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
320 objectives: NIST SP 800-171A defines 320 assessment objectives for those 110 requirements. https://csrc.nist.gov/pubs/sp/800/171/a/final
180-day POA&M closeout: 32 CFR 170.21: POA&M closeout within 180 days of the Conditional CMMC Status Date.
https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.21
72-hour SLA: DFARS 252.204-7012(c)(1)(ii): rapidly report cyber incidents to DoD within 72 hours of discovery.
https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
FIPS 140-2 historical: NIST CMVP FIPS 140-3 transition: all FIPS 140-2 certificates moved to the Historical List in September 2026; still supported for existing systems.
https://csrc.nist.gov/projects/fips-140-3-transition-effort

Related Emry Networks resources

CMMC Level 2 & CUI Enclave Readiness Checklist (web page): https://www.emrynetworks.com/cmmc-level-2-readiness-checklist
SPRS Score Worksheet for NIST SP 800-171 (Excel + PDF): https://www.emrynetworks.com/post/sprs-score-worksheet-nist-800-171
CMMC compliance for defense contractors: https://www.emrynetworks.com/services/regulated-industries/defense-contractors-cmmc
All resources: https://www.emrynetworks.com/resources

Want a second set of eyes before your C3PAO assessment?

Emry Networks helps small defense suppliers scope a CUI enclave and build NIST SP 800-171 evidence that holds up. Call (603) 202-3200 or Book a 30-Minute Risk Assessment.

EMRY NETWORKS • DEFENSIBLE IT, 24/7 MDR & LIVE COMPLIANCE ENGINEERING
Jacksonville, FL & Manchester, NH Operations Hubs • Serving Regulated SMBs Across All 50 States • (603) 202-3200 • www.emrynetworks.com/contact-us

Book a 30-Minute Risk Assessment →

Print checklist
Clear all entries