Secure Roots
info@secureroots.io · 310-421-8132 · www.secureroots.io

The 12-Point CMMC Level 2 Readiness Checklist

What AS9100 and ITAR registration do NOT cover, and what your shop is on the hook for

CMMC Level 2 is a separate cybersecurity requirement from AS9100 and ITAR registration. Primes are starting to flow the clause down into subcontracts, and it maps to NIST SP 800-171, a different control set than the quality and export-control frameworks you already run. Score yourself: for each item, can you show a document that proves it?

Administrative

1. You know your current SPRS (Supplier Performance Risk System) score, and it's been updated in the last 12 months.
2. A System Security Plan (SSP) exists and describes how CUI is handled in your environment.
3. A Plan of Action and Milestones (POA&M) exists for any gaps not yet closed.
4. One person is clearly designated as responsible for CMMC/NIST 800-171 compliance.
5. Staff who handle CUI have received security awareness training, and you can show they completed it.

Technical

1. Multi-factor authentication is enforced for email, remote access, and any system that touches CUI.
2. CUI is encrypted at rest and in transit, not just "the network is behind a firewall."
3. Each user has a unique login, and access is reviewed when someone leaves or changes roles.
4. You have endpoint protection on every device that touches CUI, and someone actually monitors the alerts.
5. Network boundaries are documented, and CUI is segmented from general business systems.

Physical and Response

1. Physical access to areas where CUI is stored or discussed is controlled and logged.
2. A written incident response plan exists, and you know your 72-hour DoD reporting obligation if CUI is compromised.

> **How did you score?** Most small and mid-size shops with AS9100 and ITAR registration can prove four or five of these. AS9100 covers quality. ITAR covers export control. Neither one covers NIST 800-171, which is what CMMC Level 2 actually assesses.

A note on timing: DFARS 252.204-7021 phases CMMC requirements into new contracts over several years. If you haven't seen the clause yet, that doesn't mean you won't. Primes are starting to ask for it ahead of the formal requirement so they aren't caught flat-footed.

This checklist is a general educational resource, not a substitute for a formal CMMC assessment by a C3PAO.