

CMMC 2.0 Compliance: A Practical Roadmap for DIB Contractors

Author: Genesis Group Holdings Compliance Advisory Team | Published: August 2026 | Distribution: Public Guidance

1. EXECUTIVE SUMMARY & FRAMEWORK CONTEXT

The Cybersecurity Maturity Model Certification [CMMC] 2.0 program is the Department of Defense [DoD] standard ensuring defense suppliers safeguard Federal Contract Information [FCI] and Controlled Unclassified Information [CUI]. As CMMC acquisition clauses appear in prime and subcontractor solicitations, contractors must achieve demonstrable, audit-ready compliance to remain eligible for contract awards.

2. CORE COMPLIANCE TIERS & REQUIREMENTS

- Level 1 [Foundational]: Enforces 17 basic safeguarding requirements derived from FAR 52.204-21. Requires annual executive self-attestation submitted directly into the Supplier Performance Risk System [SPRS].
- Level 2 [Advanced]: Enforces all 110 security controls from NIST SP 800-171 across 14 security domains. Requires third-party validation by accredited C3PAOs for contractors handling critical CUI priorities.
- System Security Plan [SSP]: The authoritative blueprint detailing technical architecture, policies, and safeguards.

3. STRATEGIC PREPARATION & AUDIT SURVIVAL

- Scoping & Data Segregation: Isolate CUI into compliant enclaves to minimize organizational audit surface area.
- Plan of Action & Milestones [POA&M]: Document temporary remediation paths with firm 180-day closeout timelines.
- Continuous Monitoring: Implement centralized SIEM logging, endpoint detection, and periodic access recertification.

Ready to Accelerate Your Compliance & Audit Readiness?

Genesis Group Holdings provides hands-on advisory, gap assessments, and audit defense.
Contact our specialists: info@genesishgh.net | 571.788.7081 | www.genesishgh.net