BLACK BOX

TRUST CENTER | SECURITY & COMPLIANCE

CMMC Level 2 Compliance:

Self-Attestation, Its Relationship to NIST SP 800-171, and the Business Value of Our Security Posture

What Is CMMC Level 2?

The Cybersecurity Maturity Model Certification (CMMC) 2.0 framework, established by the U.S. Department of Defense (DoD), defines three tiers of cybersecurity requirements for contractors and suppliers that handle federal information. CMMC Level 2 — the middle tier — is specifically designed for organizations that process, store, or transmit Controlled Unclassified Information (CUI) and aligns precisely with the 110 security practices defined in NIST Special Publication 800-171. It represents a mature, comprehensive security posture applicable across both defense and commercial sectors.

The Foundation: NIST SP 800-171

CMMC Level 2 and NIST SP 800-171 are structurally inseparable. NIST SP 800-171 provides the underlying 110 security requirements — spanning fourteen control families including Access Control, Incident Response, Configuration Management, and Risk Assessment — that CMMC Level 2 directly adopts, one-for-one, as its required practices. In practical terms:

- Achieving NIST SP 800-171 compliance is the substantive work of CMMC Level 2.
- A mature System Security Plan (SSP) and Plan of Action & Milestones (POA&M) — required under NIST 800-171 — are also the primary artifacts evaluated under CMMC Level 2.
- Our SPRS (Supplier Performance Risk System) score, submitted to the DoD, is a direct numerical representation of our NIST 800-171 implementation completeness.

Why CMMC Level 2 Does Not Require a Formal Certification

A critical and often misunderstood aspect of CMMC 2.0 is that Level 2 compliance is achieved through annual self-attestation for a significant subset of contractors — not mandatory third-party assessment. This is intentional policy design, not a gap in the framework:

- Tiered Assessment Model: CMMC 2.0 reserves mandatory third-party C3PAO (CMMC Third-Party Assessment Organization) assessments for a narrower category of high-priority programs handling the most sensitive CUI. For the broader Level 2 population, DoD determined that rigorous self-attestation with senior official accountability achieves the appropriate risk balance.
- Legal Accountability Without a Certificate: Self-attestation under CMMC 2.0 carries legal weight. Senior company officials submit compliance affirmations subject to the False Claims Act, creating enforceable accountability that mirrors — and in some ways exceeds — the liability implications of a certificate alone.
- Continuous vs. Point-in-Time: Unlike a certification that reflects a snapshot audit, our self-attestation posture is maintained continuously. Security controls are monitored, evaluated, and updated on an ongoing basis, with POA&M items actively tracked to closure.

Why Our Compliance Posture Is a Competitive Advantage for Partners

Compliance without a certificate is still a powerful, verifiable trust signal. Here is what our CMMC Level 2 posture delivers for organizations that partner with us:

✔ **Immediate DoD Supply Chain Eligibility**
Our SPRS score and self-attestation make us contractually eligible to handle CUI on DoD programs today — a prerequisite that disqualifies many competitors. Partners working in the defense industrial base can onboard us with confidence and without remediation delays.

✔ **CMMC C3PAO-Ready: Minimal Partner Risk When Mandates Expand**
As CMMC mandates expand across DoD contracts through 2026 and beyond, partners who select us now benefit from a supplier already operating at Level 2 standards — positioned to transition smoothly to third-party assessment if required, without disrupting program timelines.

✔ **Reduced Vendor Risk Burden for Your Compliance Program**
Our documented SSP, POA&M, and control evidence directly support your third-party risk management obligations. We can complete vendor security questionnaires, provide control mapping documentation, and participate in your supplier risk review processes — reducing your compliance burden, not adding to it.

✔ **Cross-Framework Coverage Supporting Your Own Obligations**
CMMC Level 2's 110 practices map closely to NIST SP 800-53 (FedRAMP), ISO 27001, SOC 2, and HIPAA Security Rule controls. Engaging us as a partner supports your own regulatory posture across federal, commercial, and international compliance frameworks simultaneously.

Documentation Available to Partners

Upon execution of an appropriate non-disclosure or data handling agreement, we can provide:

- SSP summary covering all 14 NIST SP 800-171 / CMMC Level 2 control families
- Current SPRS score and DoD self-attestation confirmation
- POA&M status summary with remediation timelines
- Completion of standard Vendor Security Questionnaires (VSQs) and third-party risk intake forms

---

Security Security & compliance inquiries:
For questions about our security posture or to request compliance documentation - Contact Us