PRESCIENT SECURITY

a Better CMMC Experience

CMMC can feel confusing and high-stakes. Requirements change, guidance is dense, and it's not always clear what "good enough" looks like in practice. Many organizations are left stitching together advice from tools, consultants, and auditors but often with unclear lines between readiness support and formal assessments. We combine an assessment-first mindset and C3PAO credentials so you can move from uncertainty to a audit-ready position without undermining your future certification.

Whether you are early in your NIST SP 800-171 journey or preparing for a formal C3PAO assessment we help you understand what is needed. You'll learn how it applies to your environment, and what it will take to reach and maintain compliance.

What sets our approach apart

COI-safe readiness and certification

Prescient Security is an Authorized C3PAO, and we treat conflict-of-interest boundaries seriously. For any given certification cycle, we either provide light, COI-safe readiness guidance and then defer the formal assessment to another C3PAO, or we serve as your independent assessor and route deeper consulting and implementation work to trusted partners. We do not blur adviser and assessor roles for the same customer in the same cycle.

Practical, evidence-driven guidance

Instead of asking you to rebuild your program from scratch, we look first at what you already have . Things like GRC platforms, tickets, logs, policies, procedures, technical controls. We then map those to NIST SP 800-171 and CMMC expectations. We highlight those gaps, and help you prioritize remediation. These will lead to a more efficient path to readiness and evidence set that is reusable across frameworks.

End-to-end solution map and partner coordination

Many clients need a complete CMMC path that includes a CUI enclave, a readiness consultant, a GRC/evidence platform, and an authorized C3PAO assessor. Prescient Security can help you connect with the right parties without creating conflict-of-interest risk. This will ensure that the work stays coordinated and your certification path remains audit-ready.

How Prescient Security supports CMMC 2.0

Prescient Security supports you across the whole CMMC journey, with clear lanes for readiness and assessment.

1 Readiness and gap analysis

- We help you understand where you stand against NIST SP 800-171 and Level 2 requirements
- Scoped view of in-scope systems and environments
- Structured review of existing policies, procedures, and technical controls
- Identification of gaps, partial implementations, and documentation needs

2 Formal Level 2 assessments (Authorized C3PAO)

- Control-by-control evaluation aligned to NIST SP 800-171 and CMMC 2.0
- Evidence-based testing with an emphasis on how controls work in practice
- Transparent findings with clear pass/fail decisions and rationale
- Reporting suitable for leadership, primes, and DoD stakeholders

3 Ongoing support and alignment

- Guidance on integrating CMMC practices into existing security and IT processes
- Input on using existing tools for ongoing monitoring and evidence collection
- Coordination with COI-safe partners for continuous support and deeper remediation

Key capabilities

1. **NIST SP 800-171** and **CMMC 2.0 expertise** informed by federal assessment experience
2. **Authorized C3PAO status** for formal Level 2 certifications
3. **COI-aware engagement models** that keep advisory and assessment roles clearly separated
4. **Evidence-driven methodology** that leverages existing tools and workflows
5. **Practical recommendations** that security, IT, and compliance teams can execute

3-year CMMC continuity program

CMMC is not a one-time event. For predictable coverage and lower disruption over time, Prescient offers a 3-year contract structure that supports certification and ongoing DoD reporting:

- **Year 1:** Mock + Official Assessment and Reporting to DoD
- **Year 2:** Self Affirmation Assessment and Reporting to DoD
- **Year 3:** Self Affirmation Assessment and Reporting to DoD

Why organizations choose Prescient Security

Independent, Authorized C3PAO with federal lineage

Prescient Security's CMMC work is led by assessors with deep experience in federal and public-sector frameworks. That background shapes how we see readiness, interpret requirements, and conduct assessments.

Clear boundaries, no mixed incentives

We treat conflict of interest as a design principle, not a footnote. When we advise, we stay within limits and coordinate independent partners for deeper implementation. When we assess, we remain independent and do not act as your hands-on consultant in the same certification cycle.

Built for how real DIB organizations work

Prescient Security can support your organization's effort toward CMMC Level 2, though certification outcomes depend on your environment, remediation efforts and the formal assessment process.

Comparison of CMMC Levels

Levels	Requirements	Purpose	Assessment
Level 3 Expert	**134+ Practices** Based on NIST 800-171 and 800-172A	FCI, stricter CUI protection + implementation plan	Annual Affirmation
Level 2 Advanced	**110 Practices** Aligned with NIST SP800-171r2	FCI + CUI protection	Annual Affirmation
Level 1 Foundational	**15 Practices** Aligned with FAR 52-204-21	FCI protection	Annual Affirmation