

Cybersecurity

# CMMC Readiness Assessment



## THE CHALLENGE

The Office of the Undersecretary of Defense for Acquisition and Sustainment (“OUSD(A&S)”) issued the Cybersecurity Maturity Model Certification (CMMC) standards in January 2020, and established guidance for all Department of Defense procurement contracts moving forward to require any contractor or sub-contractor to be CMMC-certified. CMMC expands on and enhances protections previously established for Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). Most contractors who store, process, or transmit CUI will need CMMC Level 3 certification.

## THE SOLUTION

Presidio has deep experience in supporting and assessing client environments for regulatory compliance. Presidio Cybersecurity is a CMMC Registered Provider Organization (RPO) providing consulting and advisory services to customers with CMMC compliance requirements.

The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. The Presidio CMMC Readiness Assessment leverages our deep experience with NIST 800-171 which in turn aligns extremely closely to CMMC compliance requirements.

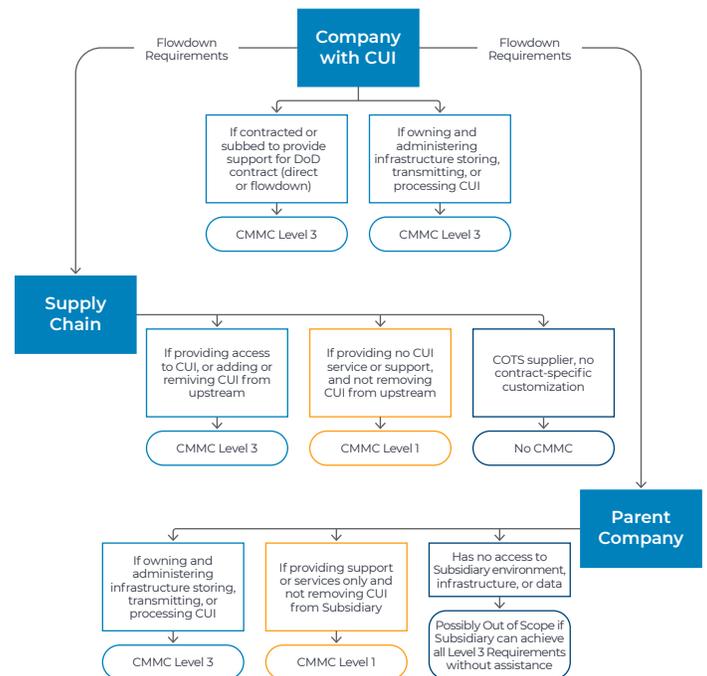
The Presidio CMMC Readiness Assessment will assess a client’s current environment and map out requirements that need to be addressed prior to attempting the CMMC certification. Presidio will work with the client to determine the appropriate level of certification needed for their specific business.

Presidio’s CMMC Readiness Assessment will support the goals of a Level 3 certification:

- ◆ Identify and review all systems and access controls for systems that handle CUI

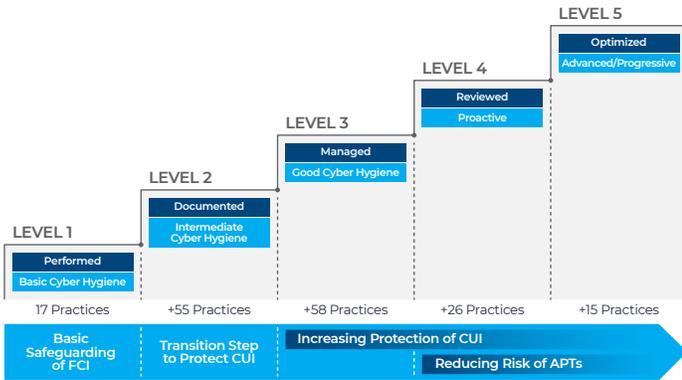
- ◆ Perform a gap analysis of the current state environment, including policy, process, and controls against compliance requirements
- ◆ Create a prioritized set of remediation recommendations to attain a compliant state
- ◆ Create a formal documentation plan describing the environment
- ◆ Rationale for any deviations from the documented plan
- ◆ Create a Plan of Action and Milestones (POAM)

The Presidio CMMC Assessment will take into consideration the relationships of the contractor and any flowdown requirements for the CUI data.



The result of this engagement will provide clients with a concrete understanding of their current level of compliance with CMMC requirements, and a sound roadmap noting deficiencies and appropriate remediation actions required to achieve compliance.

# CMMC Readiness Assessment



While the specifications support up to Level 5 (which would include Advanced Persistent Threats (APTs)), certifications are only available up to Level 3. The CMMC Readiness Assessment for a Level 3 Certification typically takes 4-weeks depending on the size and complexity of the client’s organization, providing comprehensive and immediately actionable recommendations.

## KEY BENEFITS

Presidio helps our clients to be positioned to work effectively with the Federal Government. The Level 3 regulations are designed to protect Controlled Unclassified Information (CUI) and applies to those who store, process, or transmit Controlled Unclassified Information (CUI). It is anticipated to be required by approximately 30% of federal contractors.

Clients will have the confidence and a Plan of Action and Milestones (POAM) to prepare for their Level 3 CMMC certification.

Presidio’s CMMC Readiness Assessments are designed to help clients prepare for certification. The CMMC-AB (Accreditation Body) is the only entity that can certify C3PAOs (Certified Third-Party Assessor Organization) and assessors.

## WHAT MAKES US DIFFERENT

Presidio is a trusted partner to our clients, securing their infrastructure, employees, clients and assets from ever-growing cyber threats. Our clients trust Presidio:

- ◆ **Deep Cyber Experience** – Presidio’s highly-credentialed cybersecurity consultants collectively have decades of combined practical experience spanning cyber security governance, architecture, and operations
- ◆ **Proven Cyber Leadership** – Presidio has 15+ years of providing cybersecurity leadership and securing our nations’ most sensitive networks with specialization across many of the largest industry verticals

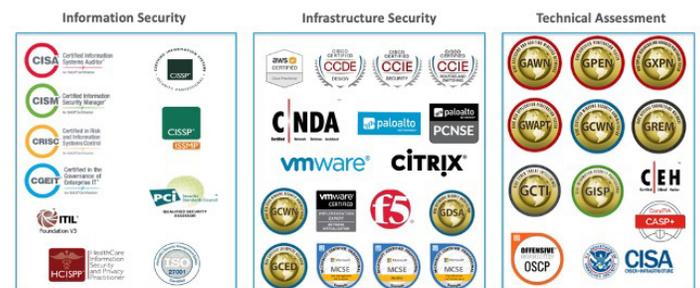
- ◆ **Business Enablers** – We understand cybersecurity policies and practices should reduce risk in order to enable the success of your business, not serve as a roadblock to your success

## WHY PRESIDIO

Presidio is a leading digital systems integrator, with deep experience in networking, cloud computing and broad hybrid infrastructures. Presidio recognizes that cybersecurity is foundational to the success of any business and has a highly specialized expert team at the ready. Our clients benefit from:

- ◆ Services methodology built on recognized industry standards including NIST, CIS, and ISO
- ◆ Compliance depth & breadth including PCI, HIPAA, NERC CIP, GDPR, CCPA, SOC 2, ISO 27001, DFARS 800-171, CMMC
- ◆ Multi-discipline experts provide for a broad view of client’s potential vulnerabilities
- ◆ Deep security services bench and broad security services solutions provide domain expertise and consistent deliverables

**Presidio Cybersecurity Practice covers a broad security services portfolio. Our highly skilled and tenured cybersecurity practitioners maintain leading industry certifications, provide thought leadership and practical industry experience. We have conducted thousands of engagements across all major industry segments. Getting started with Presidio is easy. Let’s explore how we can secure your business.**



Experience, Education, and Expertise

Visit us online today or call us at 800.235.6259