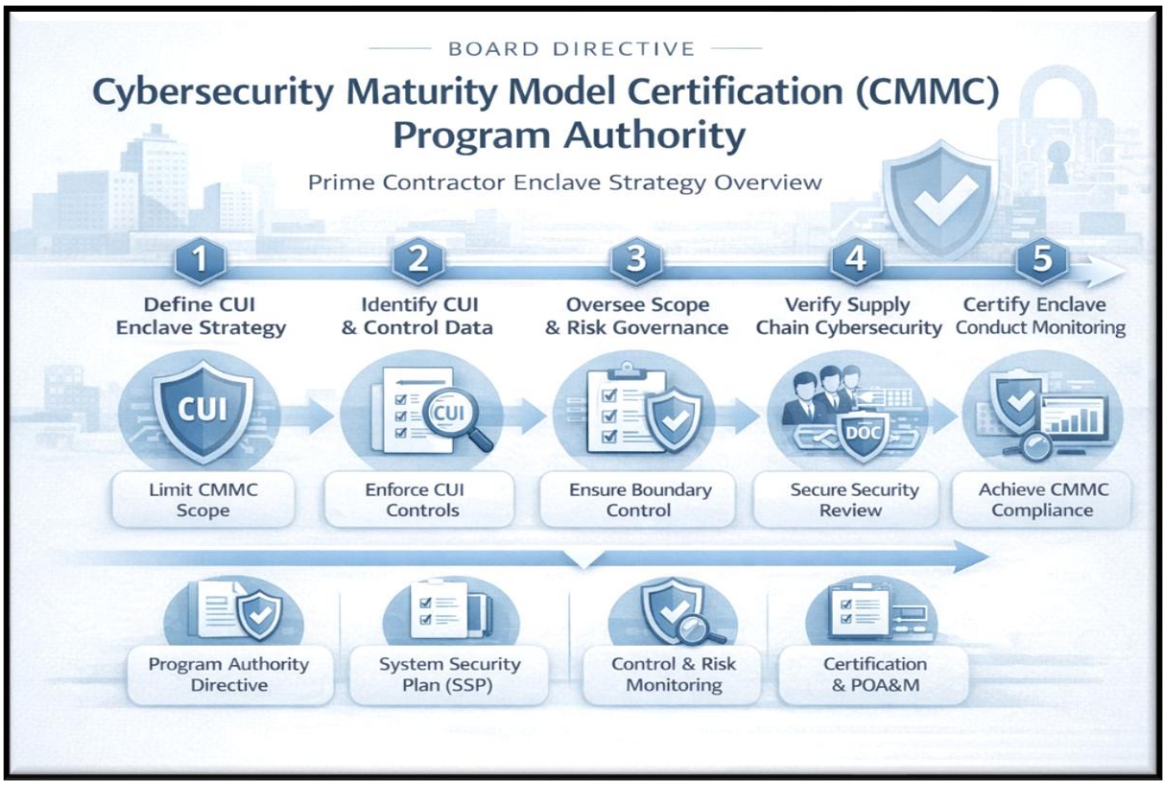
BOARD DIRECTIVE

Cybersecurity Maturity Model Certification (CMMC) Program Authority

Prime Contractor – Enclave Strategy Model



Created by:

Thomas Bronack, President

Data Center Assistance Group, LLC

bronackt@dcag.com | bronackt@gmail.com | www.dcag.com | (917) 673-6992

1. Executive Authority and Governance Mandate

1.1 Purpose

This directive formally establishes executive authority, governance structure, and strategic intent for the Company's Cybersecurity Maturity Model Certification (CMMC) Program.

The Company, as a Prime Contractor supporting the United States Department of Defense, is obligated to protect Controlled Unclassified Information (CUI) and to demonstrate compliance with applicable federal security requirements.

This directive authorizes the structured implementation of a CMMC Level 2 security program, architected for scalability toward Level 3 maturity.

Governance Area	Must Be Defined Before Phase 1
Program Authority	Yes
Budget	Yes
Enclave Scope	Yes
ODP Values	Yes
Risk Tolerance	Yes
Subcontractor Policy	Yes
Incident Authority	Yes
Monitoring Strategy	Yes
Certification Signatory	Yes

1.2 Program Authority

The Chief Executive Officer designates the Chief Information Security Officer (CISO) as the **CMMC Program Authority and Designated Official** responsible for:

- Establishing Organization-Defined Parameters (ODPs)
- Approving and maintaining the System Security Plan (SSP)
- Overseeing implementation of enclave architecture
- Approving residual risk acceptance decisions
- Authorizing certification affirmation submissions
- Serving as executive liaison for C3PAO and DIBCAC engagements

The CMMC Program Authority shall report quarterly to executive leadership and the Board on compliance status, risk posture, and remediation progress.

1.3 Strategic Objective

The CMMC Program shall:

1. Protect CUI from unauthorized disclosure or modification.
2. Achieve CMMC Level 2 certification within the approved timeline.

3. Architect a scalable enclave model to support enterprise replication.
4. Establish continuous monitoring mechanisms to sustain certification.
5. Position the organization for Level 3 readiness without architectural redesign.

2. Enclave Strategy

2.1 Strategic Decision

In alignment with the scoping principles of NIST SP 800-171 Rev. 3, which limit applicability of requirements to systems processing, storing, transmitting, or protecting CUI, the Company adopts a **CUI Security Enclave Strategy**.

The enclave model isolates CUI systems into a defined and segmented security domain to:

- Limit certification scope.
- Control compliance costs.
- Improve monitoring and traceability.
- Reduce enterprise-wide operational disruption.

2.2 Enclave Definition

A CUI Security Enclave is defined as:

A logically and technically segmented security domain engineered to contain and protect CUI and enforce CMMC control requirements within a defined boundary.

The enclave shall include:

- Segmented network architecture
- Strong identity and access control enforcement
- Centralized logging and monitoring
- Encrypted data transmission
- Controlled administrative access.
- Defined system inventory and configuration baseline

CUI shall not reside outside the enclave boundary without explicit executive authorization.

3. CUI Identification Standard

3.1 Policy Statement

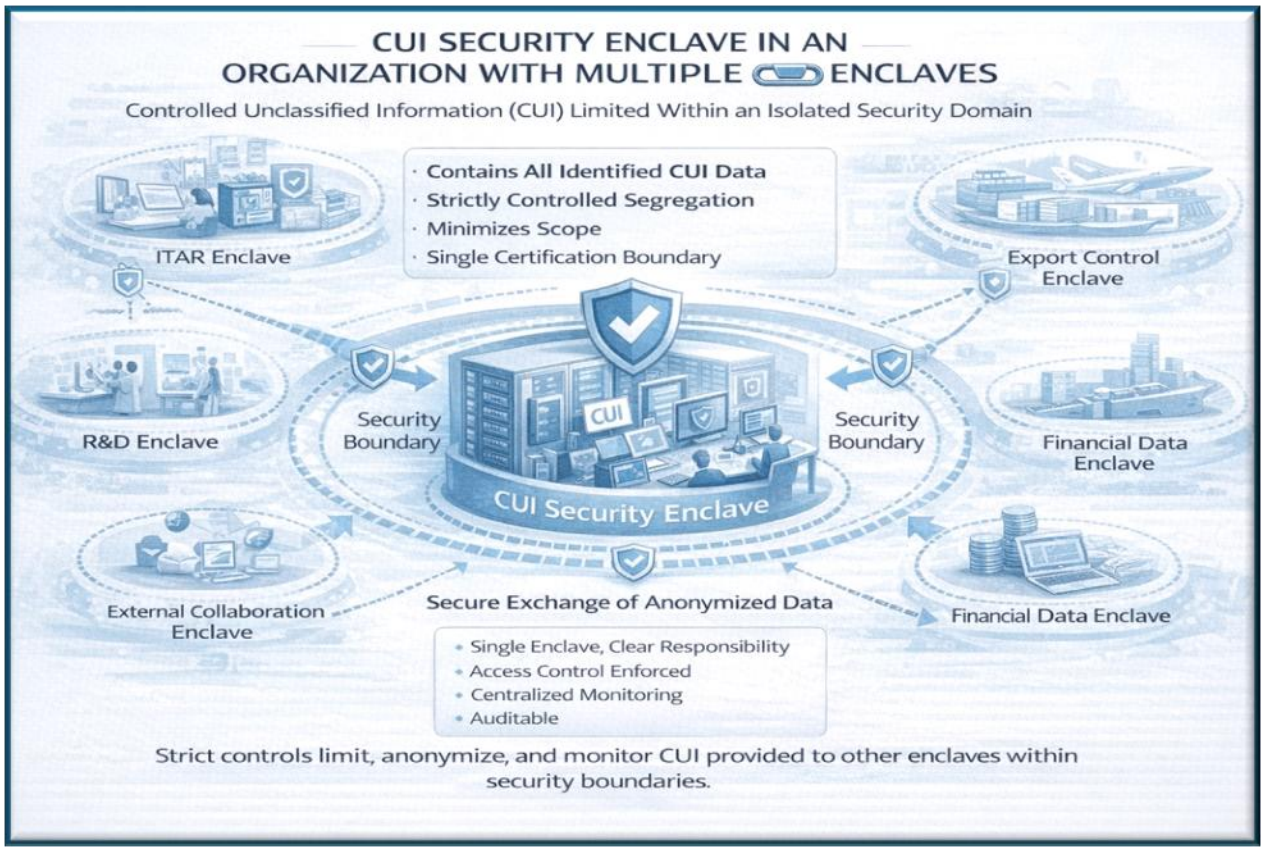
All business units must identify and classify CUI in accordance with:

- Contractual obligations
- Applicable federal registry definitions
- Program-specific security requirements.

CUI shall:

- Be labeled or logically tagged.
- Be stored exclusively within enclave-designated systems.
- Be transmitted only through approved secure channels.
- Be prohibited from storage on unauthorized enterprise platforms.

Failure to properly identify CUI constitutes a governance failure and expands compliance exposure.



4. Scope Control Rule

4.1 Boundary Enforcement

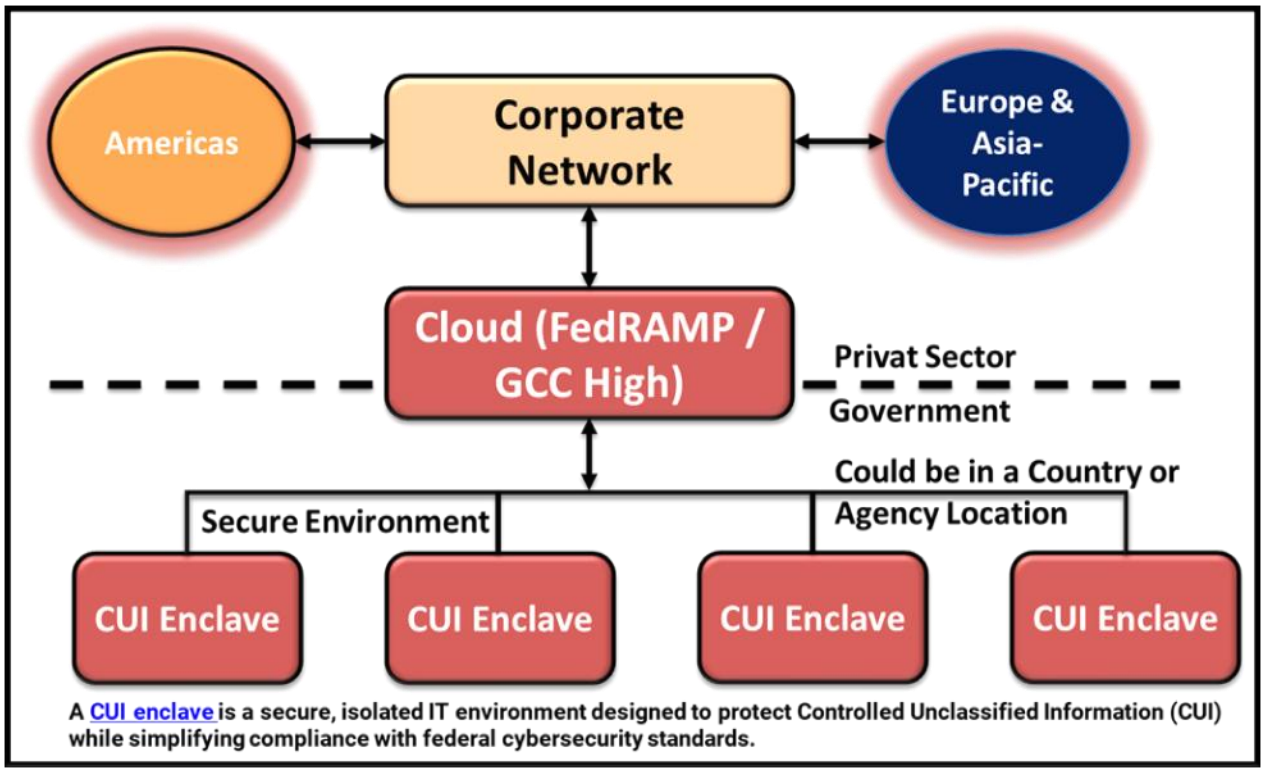
Only systems explicitly identified in the approved Enclave Boundary Diagram are subject to CMMC compliance controls.

The following are prohibited:

- Processing CUI on general enterprise systems
- Storing CUI on non-segmented infrastructure
- Administrative overlap without documented separation of duties

Any architectural change affecting the enclave boundary requires:

- Security impact analysis
- Executive review
- Formal approval by the CMMC Program Authority



5. Risk Governance and Residual Risk Acceptance

The Board acknowledges that:

- Compliance is determined through evidence-based assessment procedures.
- Findings are classified as “Satisfied” or “Other Than Satisfied.”
- Only the designated executive authority may accept residual risk.
- Plans of Action and Milestones (POA&Ms) must be formally tracked and governed.

The organization shall not submit certification affirmation unless executive management determines the security posture is defensible under independent assessment.

6. Supply Chain Accountability

As a Prime Contractor, the Company shall:

- Flow down security requirements to subcontractors.
- Verify subcontractor compliance where required.
- Restrict CUI sharing to approved and authorized entities.
- Enforce contractual cybersecurity clauses.

7. Continuous Monitoring Commitment

The CMMC Program shall evolve beyond static compliance to an operational model that includes:

- System Security Plan (SSP)
- Continuous control monitoring
- Configuration drift detection
- Log integrity validation.
- Periodic internal mock assessments
- Executive risk dashboards

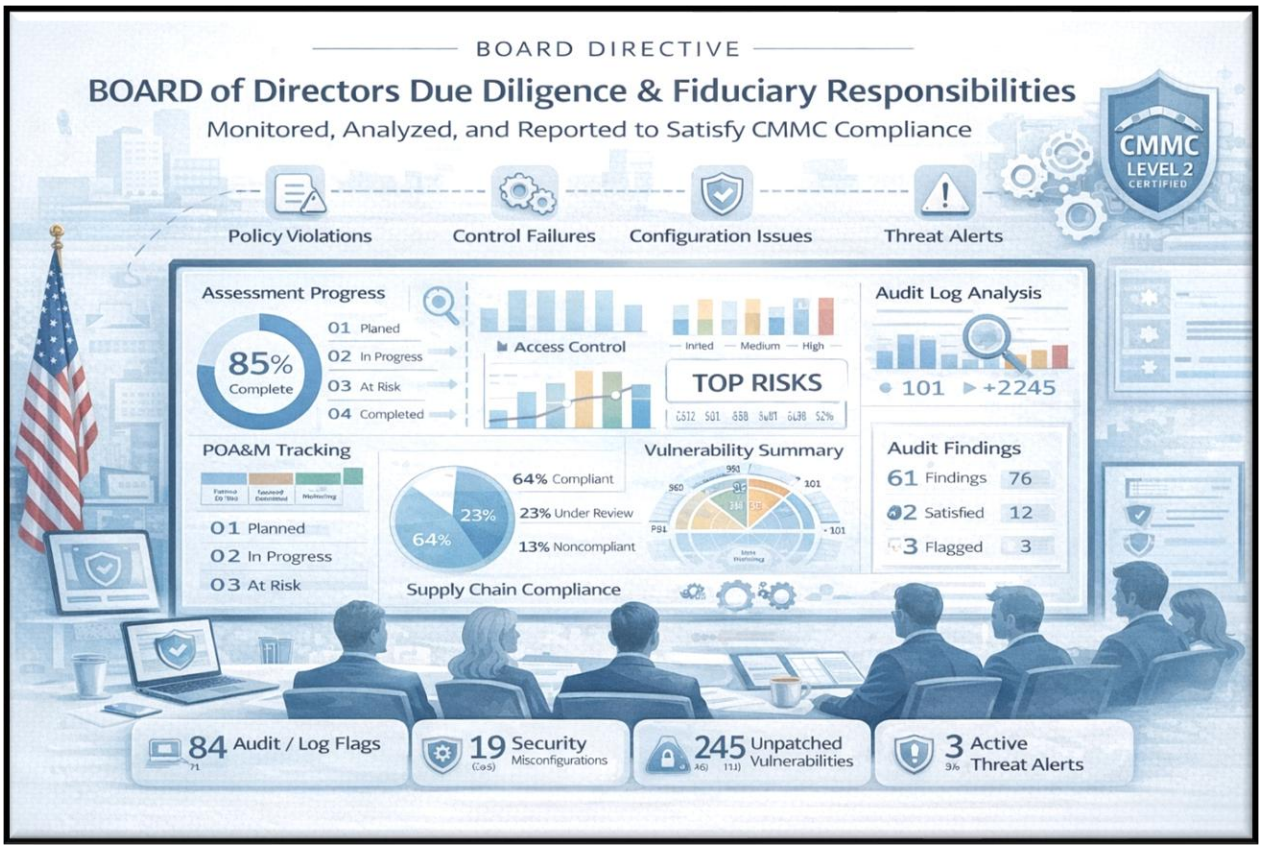
8. Executive Commitment

The Board and Executive Management affirm that:

- CMMC compliance is mandatory.
- Budget and staffing will be allocated to achieve certification.
- Enclave restrictions are enforceable corporate policy.
- Security governance is a fiduciary responsibility.

This directive is effective immediately.

Executive Dashboard for CMMC Compliance



Executive management can obtain an overview of Information Technology operation and adherence to CMMC Level 2 processes via a single pane of glass display with drill-down options to locate problem areas and make sure actions are being taken to remediate any noted flaws.

This is the end goal of the CMMC Level 2 process, with Level 3 requirements embedded within the process to quickly allow for the next phase of CMMC compliance without having to start the process all over again.

Call to Action

Contact:

Thomas Bronack, President
Data Center Assistance Group, LLC
bronackt@dcag.com |
bronackt@gmail.com
https://www.dcag.com
(917) 673-6992

- Executive and Board Level due diligence and fiduciary management support.
- Application Factory with adjustable quality control gates and automation to achieve Authorization to Operate (ATO).
- Continuous Threat Exploitation Management (CTEM) to achieve continuous ATO (cATO).
- Vulnerability Management with Patch and Release Management.
- Vendor and Third-Party Risk Management.
- Supply Chain Management, with Contracts and SLAs.
- Risk and Security Management, with CMMC.
- Quantum Readiness and Pos-Quantum Cryptography (PQC)
- Program/Project and Team Management.
- Documentation, Awareness, and Training services.
- Technical and Managerial services.

If you believe the information provided in this document provides an excellent overview of the CMMC Level 2 certification process and would like help achieving certification within your organization, please reach out to schedule a discussion of how DCAG can help you achieve your goals. We would love to collaborate with your firm to assist implementing CMMC compliance and obtaining certification.

