



# 4 BELIEFS ABOUT CMMC 2.0 YOU MAY NOT BELIEVE.



**Maturing CUI cybersecurity practice is not theater.**

**Attempts at certification should not occur prior to maturing the practice.**



# You already practice protecting CUI, but you may have gaps.

No gaps allowed at this level for basic safeguarding Federal Contract Information (FCI), the fix must be in.

Level 1: Basic Safeguarding of FCI

<b>Access Control (AC)</b> Authorized Access Control Transaction & Function Control External Connection	<b>Identification and Authentication (IA)</b> Identification Authentication	<b>Media Protection (MP)</b> Media Disposal	<b>Physical Protection (PE)</b> Limit Physical Access Escort Visitors	<b>System and Communications Protections (SC)</b> Boundary Protection Public Access system Separation	<b>System and Information Integrity (SI)</b> Flaw Remediation Malicious Code Protection Update Malicious Code Protection
--	---	--	---	---	---

## 15 REQUIREMENTS FOR LEVEL 1

**Notes:**  
Annual self-assessment and annual affirmation of compliance with the 15 security requirements in FAR clause 52.204-21.

**Bottom Line: No POA&Ms Permitted.**



# Closing gaps is not a journey, nor a trend that will fade.

Limited gaps allowed at this level for broad protection of CUI, but the fix must be in.

### Level 2: Broad Protection of CUI

Access Control (AC)	Awareness and Training (AT)	Audit and Accountability (AU)	Configuration Management (CM)	Identification and Authentication (IA)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PP)	Risk Assessment (RA)	Security Assessment (SA)	System and Communications Protections (SC)	System and Information Integrity (SI)
Authorized Access Control (CUI Data) Transaction & Function Control Control CUI Flow Separation of Duties Least Privilege Privileged Functions Privacy & Security Notices Session Lock Session Termination Control Remote Access Remote Access Confidentiality Remote Access Routing Privileged Remote Access Wireless Access Authorization Wireless Access Protection Mobile Device Connection Encrypt CUI on Mobile External Connections (CUI Data) Portable Storage Use Control Public Information (CUI Data)	Role-Based Risk Awareness Role-Based Training Insider Threat Awareness Audit correlation Audit management	System Auditing User Accountability Event review Audit failure alerting Audit correlation Audit management	System Baselining Security Configuration Enhancements System Change Management Security Impact Analysis Access Restrictions for Change User-Installed Software	Identification (CUI Data) Authentication (CUI Data) Identifier authentication Replay Resistance Authentication Identifier Reuse Temporary Passwords Cryptographically-Protected Passwords Obscure Feedback	Perform Maintenance System Maintenance Control Equipment Sanitation Media Inspection Media Accountability Protect Backups	Media Protection Media Access Media Disposal (CUI Data) Media Markings Media Accountability Shared Media	Screen Individuals Personnel Actions	Limit Physical Access (CUI Data) Monitor Facility Escort Visitors (CUI Data) Physical Access Logs (CUI Data) Manage Physical Access (CUI Data)	Risk Assessments Vulnerability Scan Vulnerability Remediation	Security Control assessment Operational Plan of Action Security Control Monitoring System Security	Boundary Protection (CUI Data) Security Engineering Role Separation Shared Resources Control Public-access System Sensations (CUI Data) Data Transit Connection Termination Key Management CUI Encryption Collaboration Device Control Mobile Code Voice Over Internet Protocol Communication Authority Data at Rest	Flaw Remediation (CUI Data) Malicious Code Protection (CUI Data) Security Alerts & Adversaries Update Malicious Code Protection (CUI Data) System Scanning Control for Security Concerns for CUI Data Identify Unauthorized Use

**110 REQUIREMENTS FOR LEVEL 2**

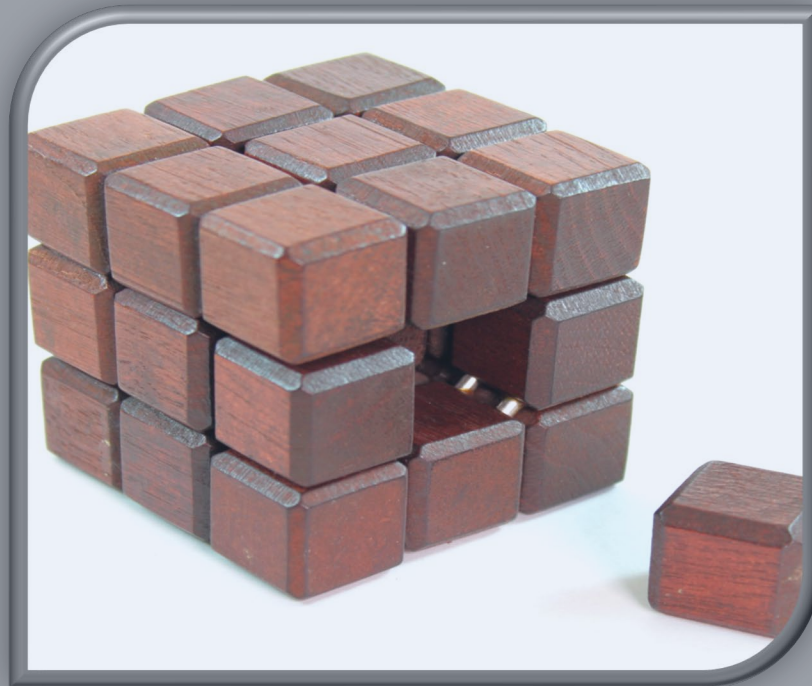
**Notes:**

1. Either a self-assessment or an independent assessment by an authorized CMMC Third-Party Assessment Organization (C3PAO) every three years, as specified in the solicitation.
2. Decided by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems.
3. Annual affirmation, verify compliance with the 110 security requirements in NIST SP 800-171 Revision 2.

**Bottom Line: POA&Ms Permitted with 180-day Limit.**



**Gaps closed today may need to be reclosed tomorrow.**



**Continuous monitoring (ConMon) is a key enabler to keeping CMMC 2.0.**

**Visit <https://rgb-ps.com> to begin planning for ConMon support of CMMC 2.0.**

CMMC 2.0 Phase 1 started November 10, 2025

Contracting officers will include CMMC Level 1 and 2 in new contracts

Suppliers must self-assess and submit scores in the Supplier Performance Risk System (SPRS) system

CMMC will eventually be mandatory after the 3-year phase-in.