RGBPSLLC-CONNECTION™

# 4 BELIEFS ABOUT CMMC 2.0 YOU MAY NOT BELIEVE.

## Maturing CUI cybrsecurity practice is not theather.

**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

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

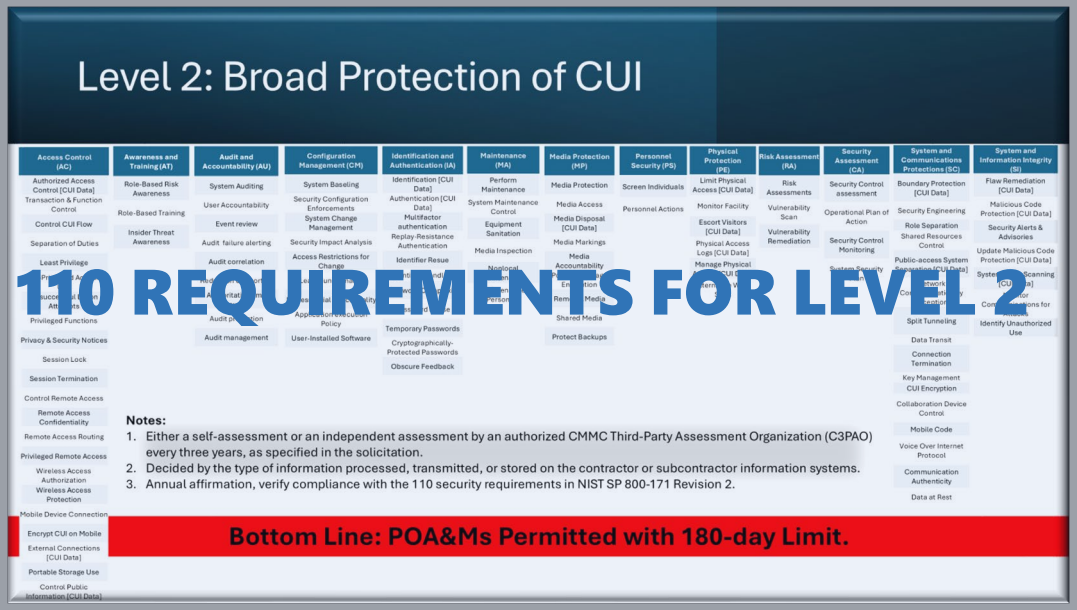
**15 REQUIREMENTS FOR LEVEL 1**

**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.




# 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.