CMMC Level 1 Quick Start Guide for Subcontractors

(Federal Contract Information – FCI Only)

What is CMMC Level 1?

The Cybersecurity Maturity Model Certification (CMMC) program ensures contractors protect sensitive government information.

- Level 1 applies to companies handling Federal Contract Information (FCI)
- Requires implementation of 17 basic cybersecurity practices
- Requires active accounts in various Government procurement systems
- It is achievable without complex infrastructure
- You can self-assess and maintain compliance internally

Why This Matters to You?

- Required for DoD contract eligibility
- Applies to prime contractors AND subcontractors (at every tier) handling FCI
- Failure to comply may result in:
  - Inability to bid or receive awards
  - Contract termination risk
  - Potential False Claims Act exposure

Step-by-Step: How to Start Your Level 1 Self-Assessment

1. Ensure access to the required government systems
   1.1. Active account in System for Award Management (SAM), sam.gov
   1.2. Active contract administrator account in the Procurement Integrated Enterprise Environment (PIEE), piee.eb.mil
   1.3. Perform an annual self-assessment + affirmation in the Suppliers Performance and Risk System (SPRS), sprs.csd.disa.mil
2. Define your internal business systems (devices, software programs, networks, even hard-copy file cabinets) that are used to process, transmit, and store FCI.
   2.1. Start with email, file storage, and user access controls
   2.2. Use Microsoft 365 / Google Workspace security features if available
   2.3. Limit FCI to controlled systems only (no personal devices unless secured)
   2.4. Document everything — if it's not written, it doesn't count

Review the 17 Security Requirements

1. Use the official assessment guide, see *CMMC Level 1 Self-Assessment Guide.pdf*
2. Key control areas include:
   2.1. Access control (limit who can access FCI)
   2.2. Identification & authentication (unique users, passwords)
   2.3. Media protection
   2.4. Physical security
   2.5. Basic cyber hygiene (antivirus, updates)

Conduct Your Self-Assessment

1. Evaluate each requirement as Met / Not Met using the Operational Plan of Action Memorandum (PoAM), see Excel file *Self-Assessment & POAM.xls*
2. Document evidence (policies, screenshots, configurations) in the System Security Plan (SSP), see the Word file *CMMC L1 SSP Template*
3. Identify gaps and create a remediation plan within the

Record & Affirm in SPRS

1. Access the SPRS system via the PIEE portal
2. Enter your score in Supplier Performance Risk System (SPRS)
3. Submit annual affirmation of compliance