DEPARTMENT OF ECONOMIC
DEVELOPMENT
AND COMMERCE
GOVERNMENT OF PUERTO RICO

2025

CMMC Level 1 Requirements, Procedures & Examples

FeCC
FEDERAL CONTRACTING CENTER
AN APEX ACCELERATOR

APEX ACCELERATORS

CMMC Level 1 Requirements, Procedures & Examples
Last updated: March 14, 2025

This APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense.

Table of Contents

I. Disclaimer

This guide focuses on **Cybersecurity Maturity Model Certification (CMMC) Level 1 requirements**. It's important to understand that CMMC has three levels of certification, each with increasing cybersecurity requirements. While this guide provides a foundation for basic cybersecurity practices, organizations should consider their long-term business goals and potential future contract opportunities. If your organization anticipates bidding on contracts requiring CMMC Level 2 or higher, it is **strongly recommended** to consider implementing infrastructure and security controls that align with those higher levels from the outset.

- **Information Provided As-Is:** The contents of this guide are offered solely for informational purposes and should not be considered professional advice. **The Puerto Rico Federal Contracting Center (FeCC),** an APEX Accelerator, makes no guarantees, expressed or implied, regarding the accuracy, completeness, or effectiveness of the information contained herein.
- **No Warranty or Endorsement:** The FeCC does not warrant that the information, methods, or processes described in this guide will not infringe on intellectual property rights or prevent damage resulting from their use. Mention of specific products or trade names does not constitute endorsement by the FeCC.
- **Official Resources Remain Primary:** You are responsible for consulting the official DoD CMMC website, FAR clause 52.204-21, and the latest CMMC Assessment Guide for current CMMC Level 1 requirements. While this guide reflects current DoD guidance, CMMC requirements are subject to change. Therefore, regularly check the official DoD CMMC website and the latest CMMC Assessment Guide for updates to maintain compliance.
- **Limited Scope and Development:** This guide was produced by FeCC with the assistance of artificial intelligence and has not been reviewed by cybersecurity experts.
- **Flow-down Requirements:** Federal Acquisition Regulation (FAR) and Department of Defense Federal Acquisition Regulation Supplement (DFARS) clauses, including FAR 52.204-21, DFARS 252.204-7012, and DFARS 252.204-7021, generally require prime contractors to "flow down" cybersecurity requirements to their subcontractors. This means that, in most cases, subcontractors must also comply with the applicable cybersecurity standards.

II. Introduction

Businesses working with the federal government (or intend to), particularly the **Department of Defense (DoD)**, must adhere to specific **cybersecurity standards**. This guide simplifies the foundational level of the CMMC Level 1, by breaking it down into easy-to-understand steps. It covers the essential cybersecurity practices required at this level, which focuses on protecting Federal Contract Information (FCI). A complete description of the requirements for level 1 can be found in the CMMC Assessment Guide Level 1 (Version – 2.13 | September 2024).

Although this guide covers level 1, it is important to know that the CMMC program includes three levels. These levels are:

Level 1: Self-Assessment (Federal Contract Information – FCI)

This is a self-assessment required to secure Federal Contract Information (FCI) that is processed, stored, or transmitted while fulfilling the contract.

- The contractor must comply with the 15 security requirements set by FAR clause 52.204-21.
- All 15 requirements must be met in full—no exceptions are allowed.

Level 2: Self-Assessment (Controlled Unclassified Information – CUI)

This is a self-assessment required to secure Controlled Unclassified Information (CUI) that is processed, stored, or transmitted while fulfilling the contract.

- The contractor must comply with the 110 Level 2 security requirements derived from NIST SP 800-171 R2.

Level 2: C3PAO Assessment (Third Party Verified Compliance)

This level differs from Level 2 (Self) in the method of compliance verification.

- Companies must hire a CMMC Third Party Assessment Organization (C3PAO) to conduct an assessment.

Level 3 DIBCAC Assessment (Advanced Requirements)

This is a government-conducted assessment with 24 additional requirements, derived from NIST SP 800-172.

III. What is Federal Contract Information (FCI)?

Understanding FCI is crucial for ensuring its proper protection. FCI includes a wide range of data generated or exchanged during a federal government contract. Essentially, it is **any information not available to the public** that is created by or provided to a contractor in support of a federal contract. To qualify as FCI, the information must:

- Be generated for or provided to the contractor **specifically for a contract**.
- **Not publicly available**.
- Directly **supports the contract's fulfillment**.

Examples of FCI include:

Contractual Documents:

- Contract terms and conditions
- Performance work statements
- Contract award notices

Technical Data:

- Engineering drawings and schematics
- Software source code
- Research and development reports

Financial Data:

- Cost proposals and reports
- Financial performance data

Personnel Information:

- Roles and responsibilities related to the contract
- Security clearances and authorizations

IV. Why CMMC Matters

The increasing sophistication of cyberattacks poses significant risks to *national security* and the integrity of DoD programs. CMMC is crucial for ensuring that contractors handling sensitive information have the necessary cybersecurity safeguards in place.

Every business with an active federal contract should verify if **FAR clause 52.204-21** is included in the contract. If it is, be aware that you are certifying that you meet all requirements. *Not being in compliance with the FAR clause may constitute a* ***breach of contract*** *and could* *lead to **liability under the False Claim Act**.* Failure to comply with **CMMC requirements** can result in **contract denial, suspension, or termination**, potentially impacting a company's revenue and reputation.

It is strongly recommended that companies with a federal contract or those pursuing federal business opportunities take appropriate actions to meet all the requirements of this clause.

V. Identifying the CMMC Assessment Scope – First Step

The **first step** in meeting **CMMC Level 1** requirements is "scoping". Think of scoping as drawing a map of the systems you need to protect. This step helps you identify which of your **computer systems**, including those managed by External Service Providers (ESPs) that handle Federal Contract Information (FCI).

Scoping determines which systems, and equipment must meet the CMMC Level 1 security requirements. In short, any system that handles FCI in any way is considered "in scope" for your Level 1 self-assessment.

When a System is "In Scope"

A system is "In scope" if it:

- **Processes FCI:** The asset uses FCI (e.g., accesses, enters, edits, generates, manipulates, or prints it). Examples include: a computer used to create invoices containing contract numbers, a printer used to print contract documents, or a software application used to manage contract data.
- **Stores FCI:** FCI is inactive or at rest on the asset (e.g., located on electronic media, a hard disk, or in physical format like paper documents). Examples include: a server storing contract files, a laptop containing downloaded contract specifications, a filing cabinet holding printed contract agreements, or a USB drive used to back up contract data.
- **Transmits FCI:** FCI is being transferred from one asset to another (e.g., data in transit using physical or digital transport methods). Examples include emailing contract files, uploading contract documents to a government portal, transferring contract data via a network, or physically shipping FCI on a hard drive.

Key Questions to Ask During Scoping:

- Does this system process, store, or transmit FCI?
- Does this system connect to other systems that handle FCI?
- Do external service providers (ESPs) manage any systems that handle FCI on your behalf?

When a System is Out of Scope

Assets that do **not** process, store, or transmit FCI are considered **out of scope**. It's still important to identify all assets, even those outside the scope of the assessment. In addition to these general out-of-scope assets, **some specialized assets are automatically excluded** from Level 1 assessments—even if they could technically handle FCI—because they cannot be fully secured under **CMMC Level 1** requirements. These specialized assets include:

- Internet of Things (IoT) devices
- Industrial Internet of Things (IIoT) devices
- Operational Technology (OT)
- Government Furnished Equipment (GFE)
- Restricted Information Systems
- Test Equipment

How to Determine if an Asset is In or Out of Scope:
Consider these questions when deciding which category an asset falls into:

- **Ownership**: Who owns the asset (company or personal)?
- **Usage**: Is the asset used only for business, personal use, or both?
- **Connection**: Does the asset connect to systems containing FCI?
- **FCI Handling**: Does the asset store, process, or transmit FCI?

Mixed-Use Environments *(Personal and Work Devices):*

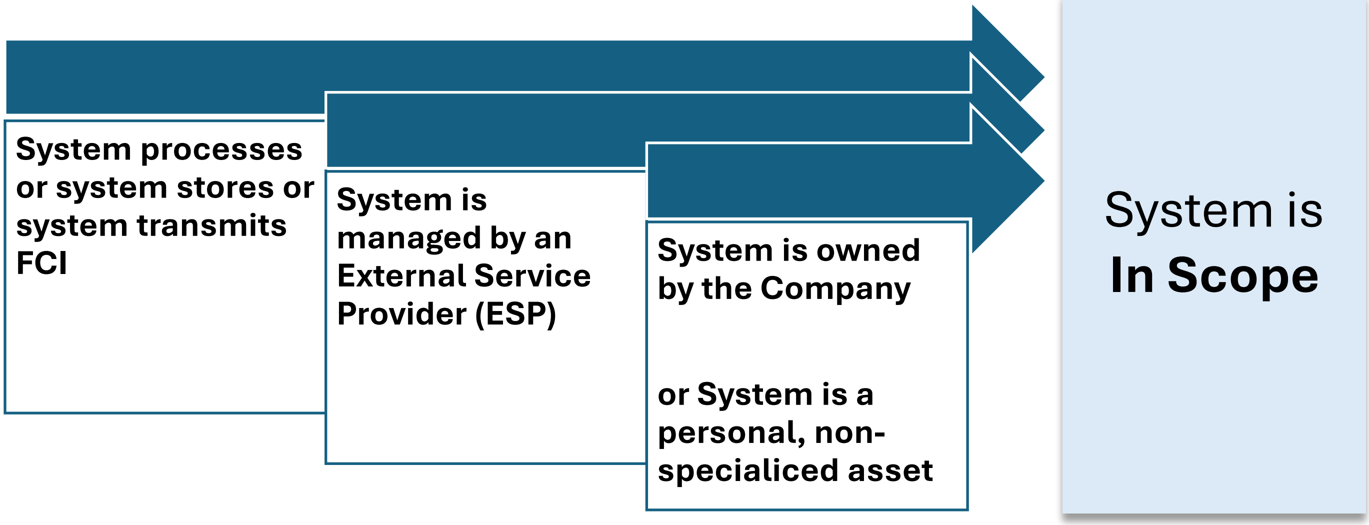
In these situations, the *primary* use of the asset usually determines its scope.

- **Out of Scope Example**: A personal laptop mainly used for personal tasks but occasionally used to check work email (if properly separated from FCI and covered by usage policies).
- **In Scope Example**: A personal device regularly used to handle FCI, such as drafting or reviewing contract documents.

Key Takeaway: Keep a detailed inventory of *all* assets. Clearly mark each asset as "in scope" or "out of scope" and explain why. This documentation is crucial for audits and demonstrates your understanding of your CMMC boundary.

CMMC Level 1 Scoping Decision Flowchart

The following flowchart provides a visual representation of how to determine whether a system is in scope for CMMC Level 1.


System processes or system stores or system transmits FCI
System is managed by an External Service Provider (ESP)
System is owned by the Company
or System is a personal, non-specialiced asset
System is In Scope

Example Scenarios – Assessing Systems in/out of Scope

Scenario 1: Regular Business (Small Manufacturing Company)

- **Business Description:** A small manufacturing company that produces parts for a federal agency or a larger contractor. They receive blueprints, specifications, and contract information electronically.
- **Systems and Assets:**
  - **In Scope:**
    - Desktop computers used by engineers to access and modify blueprints.
    - File server storing blueprints and contract data.
    - Email server used to receive and send emails containing FCI.

        - Network routers and firewalls that protect these systems.
        - Cloud storage service used to back up blueprints.
    - **Out of Scope:**
        - Computers used for accounting and human resources (unless they directly interact with systems handling FCI).
        - Company website (unless it stores or transmits FCI).
        - Printers used only for internal administrative documents.

Scenario 2: Home-Based Business (Independent Consultant)

- **Business Description:** An independent consultant who provides technical writing services to a government agency. They receive and deliver documents containing FCI electronically.
- **Systems and Assets:**
    - **In Scope:**
        - Personal laptop used to create, edit, and store documents containing FCI.
        - Home Wi-Fi router and modem.
        - Personal email account used to exchange FCI with the agency.
        - Cloud storage service used to back up FCI-related documents.
    - **Out of Scope:**
        - Personal smartphone used for calls and personal messaging (unless used to access or store FCI).

Why the Difference Matters:

As you can see, the scope of **CMMC Level 1** can vary significantly depending on the nature of your business. The manufacturing company has a more complex IT infrastructure and more systems that handle FCI, resulting in a larger scope. The independent consultant, working from home, has a much simpler setup, resulting in a smaller scope.

Important Considerations:

- **Data Flow:** Trace the flow of FCI through your business. This will help you identify all systems that process, store, or transmit FCI.
- **External Service Providers (ESPs):** If you use ESPs (e.g., cloud storage, managed IT services), you must consider their systems and security practices as part of your scope.

- **Documentation:** Document your scoping decisions. This will be important for your self-assessment and any future audits.

The CMMC Scoping Guide Level 1 provides a comprehensive overview of the scoping requirements and processes.

VI. Current Requirements for Contractors and Subcontractors – Second Step

After identifying which systems handle FCI, you'll need to put basic security measures in place to protect that information and meet CMMC Level 1. These measures are called "security controls," and there are 15 of them for Level 1. They're detailed in 48 CFR 52.204-21(b)(1)(i) through (xv). This publication explains the basics of what you need to do to safeguard your systems. Because government rules can change, it's important to **always check the most recent version of FAR clause 52.204-21.**

CMMC Level 1 Security Controls: 15 Required Safeguards

I. **Limit information system access** to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

II. **Limit information system access** to the types of transactions and functions that authorized users are permitted to execute.

III. **Verify and control/limit connections** to and use of external information systems.

IV. **Control information posted or processed** on publicly accessible information systems.

V. **Identify information system users**, processes acting on behalf of users, or devices.

VI. **Authenticate (or verify)** the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

VII. **Sanitize or destroy information system media** containing Federal Contract Information before disposal or release for reuse.

VIII. **Limit physical access** to organizational information systems, equipment, and the respective operating environments to authorized individuals.

IX. **Escort visitors and monitor visitor activity**; maintain audit logs of physical access; and control and manage physical access devices.

X. **Monitor, control, and protect organizational communications** (*i.e.,* information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

XI. **Implement subnetworks** for publicly accessible system components that are physically or logically separated from internal networks.

XII. **Identify, report, and correct information and information system flaws** in a timely manner.

XIII. **Provide protection from malicious code** at appropriate locations within organizational information systems.

XIV. **Update malicious code protection mechanisms** when new releases are available.

XV. **Perform periodic scans** of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

The 52.204-21 clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information.

Prime Contractor’s Responsibility

It's crucial to understand that prime contractors are responsible for flowing down the requirements of this clause to subcontractors working under a covered contract. This applies even to subcontracts for commercial products or commercial services (excluding commercially available off-the-shelf items) if the subcontractor's information system may store or transmit Federal Contract Information.

VII. Checking CMMC Level 1 Compliance – Third Step

Now it's time to see how well your systems stack up against the CMMC Level 1 security rules for protecting FCI. This is done through a "self-assessment", where you check your own systems. Don't worry, there are resources to help! Project Spectrum (PS) is a great example. It's a free learning platform packed with resources, tools, training, and videos to guide you through the CMMC process. They even have a Cyber Readiness Assessment tool to help you pinpoint any areas you might need to improve.

For CMMC Level 1, you need to meet **all 15 required controls** and have *all* of them fully implemented at the time of your self-certification. This means you can't have a plan to fix things later, everything must be operational and effective. However, if a particular requirement doesn't apply to your business (and you can show why), it's considered met.

VIII. Supplier Performance Risk System (SPRS) – Fourth Step

Once all requirements are met, you must submit assessment results in the Supplier Performance Risk System (SPRS). To maintain compliance with the requirements, you must conduct a Level 1 self -assessment on an *annual basis* and submit the results in SPRS.

IX. Example of the process - CMMC Level 1 Compliance Documentation

We've talked about the important steps for achieving **CMMC Level 1**, and now it's time to see how they work in practice! This section provides a **practical example** of how to scope your systems, identify the relevant **security requirements**, and perform a self-assessment. To help visualize this, we've created a table that walks through a sample self-assessment for all 15 requirements.

This table offers explanations of how compliance can be achieved in two common scenarios: a **home-based business** and a **standard business**. *We've included both to show how the same security goals can be accomplished with different approaches and resources.* Think of this as a helpful illustration, it's not a one-size-fits-all solution. You'll need to adapt these steps to your own business, considering the specific types of systems and information you handle.

This example will help you understand the process, but *remember to tailor it to your own unique setup*.

1. Example of Identifying Systems for CMMC Compliance

Scoping:

The following assets have been identified as in scope for this CMMC Level 1 self-assessment:

Process:

1. Computer 01 used to create invoices containing contract numbers
2. Computer 02 used to manage the contract
3. Printer 02 used to print and scan contract documents
4. Mobile Devices: Phone-01

Store:

1. Server 01 storing contract files
2. Laptop 01 containing downloaded contract specifications
3. Filing cabinet 01 holding printed contract agreements
4. USB drive 01 is used to back up contract data
5. External hard drives 01 and 02

Transmit:

1. Email platform (Outlook, Gmail...)
2. Government portal PIEE
3. Network (describe)
4. Physically mailing contract information

Justification for Inclusion/Exclusion:

Computer 01 is used by the contracts manager to create and edit contracts. Therefore, it is "in scope". Printer 02 is only used for internal documents and never handles FCI. Therefore, it is out of scope.

2. Example Table of the 15 Required Security Controls

The following table lists the 15 safeguarding requirements from FAR clause 52.204-21 and shows how two types of businesses—**a standard business** with employees and a formal IT infrastructure, and a **home-based business** operated by a single individual—can meet them.

The table includes:

- Each requirement and a brief description.
- Compliance status.
- Implementation examples for both business types.

This comparison shows how **business size and complexity** shape compliance methods. For example, while a standard business might use **key card access and visitor logs**, a home-based business relies on **residential security** and **direct supervision**. Similarly, network segmentation and advanced security appliances are essential for larger networks, while a single computer relies on its built-in firewall and antivirus software.

Key Takeaway: Even home-based businesses can meet the requirements of **FAR 52.204-21** by implementing security controls appropriate to their specific circumstances.

Requirement	Description	Compliance Status	Explanation of Compliance (Standard Business Implementation)	Explanation of Compliance (Home-Based Business Implementation)
(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Restrict access to information systems to authorized users, processes, and devices	Met	Access to in-scope systems is controlled through unique user accounts with strong passwords. Access is granted based on the principle of least privilege. Regular reviews of user accounts are conducted to ensure only authorized personnel have access.	Access is limited to the single user (owner) via a password-protected user account on the computer. No other users, processes, or devices access the system directly.
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Limit access to authorized transactions and functions.	Met	User permissions are configured based on roles and responsibilities. Users only have access to the specific applications and data required for their work. Regular reviews of user roles and permissions are performed.	The single user (owner) has full administrative access to the computer and all software. This is inherently limited by the software installed and the user's operational needs. Standard user account controls are utilized.
(iii) Verify and control/limit connections to and use of external information systems.	Control connections to external systems.	Met	Connections to external information systems are controlled through a firewall and access control lists. Access is granted only to authorized external systems. Regular reviews of external connections are performed.	Outbound connections are managed through the computer's firewall and internet browser settings. Access to external services is initiated by the user (owner).
(iv) Control information posted or processed on publicly accessible information systems.	Control information on public systems.	Met / Not Applicable	No FCI is posted or processed on publicly accessible information systems. Individuals authorized to post or process information on publicly accessible systems are identified. A policy is in place prohibiting the storage or processing of FCI on such systems.	If the business does not operate any publicly accessible information systems, this is "Not Applicable". If public facing services are required, they are hosted by a third-party provider. The owner is responsible for ensuring data posted to public sites comply with applicable requirements.

(v) Identify information system users, processes acting on behalf of users, or devices.	Identify users, processes, or devices.	Met	Unique user accounts with strong passwords are required for all users. Multi-factor authentication is implemented where feasible. Device authentication is used for network access.	The single user is identified by their user account. Processes are identified by the operating system. The single computer is the only device.
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Authenticate users, processes, or devices before granting access.	Met	Established strong password policies for user accounts. Implemented digital signatures and code signing for software. Deployed device certificates and Network Access Control. Documented all policies, configurations, and maintain audit logs. Regularly assess security controls.	User authentication is performed via password login to the computer.
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Sanitize/destroy media before disposal/reuse.	Met	Hard drives and other storage media are securely wiped using approved methods before disposal or reuse. A documented procedure is in place for media sanitization.	Data is securely deleted using software tools or physical destruction of the media (e.g., hard drive shredding) before disposal or reuse.
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Limit physical access to systems, equipment, and environments.	Met	Physical access to server rooms and other sensitive areas is controlled through locked doors and access control systems. Visitor access is logged and monitored.	Physical access to the computer is controlled by standard residential security measures within the private residence.
(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	Escort visitors, monitor activity, maintain physical access logs, and control/manage physical access devices.	Met / Not Applicable	All visitors are required to sign in and out and are escorted while on company premises. Sign-in logs are retained for one year in accordance with company policy. We utilize key card access to control and manage physical access to our facilities and restricted areas.	As a home-based business, residential security measures control access. Formal visitor logs are not maintained. Business-related visitors are escorted and supervised. Computer access is controlled via passwords.

(x) Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems.	Monitor, control, and protect communications at external and key internal boundaries.	Met / Not Applicable	Deployed firewalls, IDS/IPS, and content filtering at network boundaries. Secured device configurations. Monitored traffic logs and conducted regular vulnerability scans and penetration testing.	As a single computer setup, there are no internal network boundaries. External boundary protection is achieved through the computer's built-in firewall and antivirus software. All communications are considered external.
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Implement subnetworks (e.g., DMZ) to separate public systems from internal networks.	Met / Not Applicable	Created a Demilitarized Zone (DMZ) to host publicly accessible servers and services. Implemented firewall rules to restrict traffic between the DMZ and internal networks. Regularly review firewall rules and network segmentation.	As a single computer setup, there are no separate systems requiring a DMZ or subnetworks. If public facing services are required, they are hosted by a third-party provider.
(xii) Identify, report, and correct information and information system flaws in a timely manner.	Identify, report, and correct system flaws.	Met	A vulnerability scanning process is in place. Identified vulnerabilities are reported and remediated in a timely manner based on risk level.	The user (owner) is responsible for keeping the operating system and software updated with security patches. Automatic updates are enabled where possible.
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.	Protect against malicious code.	Met	Anti-malware software is installed and actively running on all in-scope systems. Regular scans are performed, and updates are automatically installed.	Anti-virus/anti-malware software is installed and kept up to date.
(xiv) Update malicious code protection mechanisms when new releases are available.	Update malware protection.	Met	Anti-malware software is configured to automatically receive and install updates. Regular checks are performed to ensure updates are occurring.	Anti-virus/anti-malware software is configured for automatic updates.
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Perform periodic and real-time scans.	Met	Regular full system scans are performed on all in-scope systems. Real-time scanning is enabled for all file downloads, openings, and executions.	Anti-virus/anti-malware software performs real-time scanning of files and periodic full system scans.

3. Self-Assessment Statement:

A self-assessment was conducted on [Date] using [Method used e.g. NIST Handbook 162, Project Spectrum's Cyber Readiness Assessment Tool] to verify compliance with the 15 safeguarding requirements. The results of the assessment confirmed that all requirements were met. Refer to the above table for the self-assessment findings.

4. Submission to SPRS:

The results of this CMMC Level 1 self-assessment have been submitted to the Supplier Performance Risk System (SPRS) on [Date of Submission]. Use this link for a complete set of instructions to upload the self-assessment into SPRS.

5. Summary of CMMC Level 1 Compliance Implementation

[Company Name] has successfully implemented the necessary safeguards to protect Federal Contract Information and has achieved CMMC Level 1 (Self) compliance. This documentation serves as evidence of our commitment to cybersecurity and compliance with federal regulations.

X. Sample Policies and Procedures

Now, let's review examples of policies and procedures that **support CMMC Level 1 compliance**. Policies are important for any business, big or small, office or home based. They set clear expectations for how to handle sensitive data and help prevent security mistakes.

This section includes examples, including one tailored for a home-based business, to give you a better understanding of what policies might look like. These examples were **created using AI** and are for illustrative purposes only. *They aren't meant to be copied directly.*

Because every business is unique, you'll need to tailor your policies to your specific situation. Working with a **cybersecurity expert** is the best way to ensure your policies are effective and fully **CMMC-compliant**.

1. Access Control Policy
2. Identification and Authentication Policy
3. Media Protection Policy

1. Access Control Policy (use as example)

Purpose:

This Access Control Policy outlines the procedures and controls for limiting access to [Organization Name]'s information systems and data, including Federal Contract Information (FCI), to authorized users, processes, and devices. This policy aligns with the Cybersecurity Maturity Model Certification (CMMC) Level 1 requirements.

Scope:

This policy applies to all employees, contractors, and third-party users who have access to [Organization Name]'s information systems and data.

Policy Statement:

[Organization Name] is committed to protecting the confidentiality, integrity, and availability of its information systems and data. Access to these resources will be granted only to authorized individuals based on their job responsibilities and the principle of least privilege. Access enforcement mechanisms can be employed at the application and service level to provide increased information security.

Access Control Measures:

1. **Identification and Authentication:**
    - **Unique Usernames and Passwords:** All users must have unique usernames and strong, complex passwords.
    - **Multi-Factor Authentication (MFA):** Implement MFA for all user accounts, including administrative accounts.
    - **Regular Password Changes:** Enforce regular password changes for all users.
2. **Access Control Lists (ACLs):**
    - Implement ACLs on all network devices and systems to restrict access to authorized users and devices.
    - Regularly review and update ACLs to reflect changes in user roles and responsibilities.
3. **Least Privilege:**
    - Grant users only the minimum level of access necessary to perform their job duties.

    - Regularly review user access rights and remove unnecessary privileges and / or software.

4. **Account Management:**
    - Disable or delete inactive user accounts promptly.
    - Implement procedures for managing privileged accounts, including regular reviews and rotation of passwords.
5. **Physical Access Control:**
    - Limit physical access to data centers, server rooms, and other areas containing sensitive information.
    - Implement physical security measures, such as locks, security cameras, and access badges.
6. **Data Classification:**
    - Classify data based on its sensitivity and value.
    - Implement appropriate access controls based on the data classification level.
7. **System and Information Integrity:**
    - Implement security controls to protect the integrity of information systems and data.
    - Regularly monitor systems for unauthorized access and malicious activity.
8. **Control information posted or processed on publicly accessible information systems:**
    - **Data Sanitization:** Ensure that any FCI or other sensitive data posted or processed on publicly accessible systems is properly sanitized or anonymized to remove any sensitive information.
    - **User Guidance:** Provide clear guidance to employees on what information can and cannot be posted or processed on publicly accessible systems.
    - **Monitoring:** Regularly monitor publicly accessible systems for any unauthorized disclosure of sensitive information.
    - **Posting:** Ensure that individuals authorized to post onto publicly accessible systems are designated and that the content of information is reviewed prior to posting to safeguard that non-public information is not included.
9. **Verify and control/limit connections to and use of external information systems:**
    - **Authorized Connections:** Only authorized connections to external information systems will be permitted. These connections must be documented and approved by [Designated Authority/Role].

- **Connection Methods:** Control the methods used to connect to external systems. This may include using Virtual Private Networks (VPNs), secure file transfer protocols (SFTP), or other secure communication channels.
- **Data Transfer Restrictions:** Implement controls to limit the type and amount of data that can be transferred to external systems. Prohibit the transfer of FCI without explicit authorization.
- **Regular Review:** Regularly review and audit connections to external systems to ensure compliance with this policy.
- **Prohibition of Unauthorized Devices:** Prohibit the connection of unauthorized personal devices to the organization's network without explicit authorization from [Designated Authority/Role].

Enforcement:

- Violations of this policy will be subject to disciplinary action, up to and including termination of employment.
- Regular audits and assessments will be conducted to ensure compliance with this policy.

Training and Awareness:

- All employees and contractors will receive training on this policy and their responsibilities for protecting information systems and data.
- Regular security awareness training will be provided to all users.

Review and Updates:

- This policy will be reviewed and updated at least annually or as needed to address changes in technology, threats, or regulatory requirements.

Contact Information:

For questions or concerns regarding this policy, please contact [Contact Person] at [Contact Information].

Note: This is a sample Access Control Policy and will need to be adapted to meet the specific needs and requirements of your organization. It is recommended to consult with a qualified cybersecurity professional to ensure compliance with CMMC Level 1 and other applicable regulations.

2. Identification and Authentication Policy (use as example)

Purpose:

This policy establishes the requirements for identifying and authenticating users, processes acting on behalf of users, and devices seeking access to [Organization Name]'s information systems. This policy is designed to meet the requirements of Cybersecurity Maturity Model Certification (CMMC) Level 1.

Scope:

This policy applies to all employees, contractors, third-party users, and devices that access [Organization Name]'s information systems, including those containing Federal Contract Information (FCI).

Policy Statement:

[Organization Name] is committed to ensuring that only authorized users, processes, and devices are granted access to its information systems. This is achieved through robust identification and authentication mechanisms.

Identification and Authentication Requirements:

1. **Unique User Identification:**
    - Every user accessing organizational information systems will be assigned a unique identifier (username or account name).
    - Generic or shared accounts are prohibited except for specific, documented, and approved purposes (e.g., guest Wi-Fi access with limited privileges).
    - User identifiers will be managed through a formal account management process, including creation, modification, suspension, and deletion.
2. **Authentication Mechanisms:**
    - **Passwords:** Passwords must adhere to the following minimum requirements:
        - Minimum length of 12 characters.
        - Combination of uppercase and lowercase letters, numbers, and symbols.
        - Not be based on personal information (e.g., names, birthdays).
        - Not be reused.
    - **Multi-Factor Authentication (MFA):** MFA is required for all user accounts, especially privileged accounts (administrators). Acceptable MFA methods include:
        - Time-based One-Time Passwords (TOTP) (e.g., Google Authenticator, Authy).
        - Hardware tokens.

   - **Device Authentication:** Devices connecting to the organizational network will be identified and authenticated through mechanisms such as:
      - MAC address filtering.
      - Network Access Control (NAC).
      - Device certificates.

3. **Authentication Management:**
   - **Password Changes:** Users will be required to change their passwords at least every 90 days or as directed by the [Designated Authority/Role].
   - **Account Lockout:** Account lockout mechanisms will be implemented to prevent brute-force password attacks. After a defined number of incorrect login attempts (e.g., 5), the account will be locked for a specified period (e.g., 30 minutes) or require an administrator intervention to unlock.
   - **Session Management:** Inactive user sessions will be automatically terminated after a defined period of inactivity (e.g., 15 minutes).
4. **Processes Acting on Behalf of Users:**
   - Automated processes requiring access to information systems will be assigned unique service accounts with appropriate privileges.
   - These service accounts will be subject to the same authentication and access control policies as user accounts.
5. **Guest Access:**
   - Guest access to organizational resources will be limited and controlled.
   - Guest accounts will be temporary and granted only for specific purposes.
   - Guest access will be provided on a separate network segment, if possible, to isolate it from internal resources.
6. **Identification and Authentication for Wireless Access:**
   - All wireless network access will require authentication using strong encryption protocols (e.g., WPA2/3-Enterprise) and unique credentials.

Enforcement:

- Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.[1]

Training and Awareness:

- All users will receive training on this policy and their responsibilities for maintaining strong passwords and protecting their credentials.

Review and Updates:

- This policy will be reviewed and updated at least annually or as needed to address changes in technology, threats, or regulatory requirements.

Contact Information:

For questions or concerns regarding this policy, please contact [Contact Person] at [Contact Information].

Note: This is a sample Identification and Authentication Policy and will need to be adapted to meet the specific needs and requirements of your organization. It is recommended to consult with a qualified cybersecurity professional to ensure compliance with CMMC Level 1 and other applicable regulations.

3. Media Protection Policy (use as example)

Purpose:
This policy establishes requirements for the protection, handling, and disposal of information system media containing Federal Contract Information (FCI) within [Organization Name]. This policy is designed to meet the requirements of Cybersecurity Maturity Model Certification (CMMC) Level 1.

Scope:
This policy applies to all employees, contractors, and third-party users who handle, store, or dispose of information system media, whether digital or non-digital, that contains FCI. This includes, but is not limited to:

- Computer hard drives
- Solid-state drives (SSDs)
- USB flash drives
- Optical discs (CDs, DVDs, Blu-rays)
- Magnetic tapes
- Paper documents
- Printers and multi-function devices with storage capabilities

Policy Statement:
[Organization Name] is committed to protecting FCI throughout its lifecycle, including proper disposal and reuse of media. All media containing FCI must be sanitized or destroyed before disposal or release for reuse to prevent unauthorized disclosure.

Media Handling and Storage:

1. **Storage:** Media containing FCI must be stored in secure locations with appropriate physical access controls (e.g., locked cabinets, secure rooms).
2. **Labeling:** Media containing FCI must be clearly labeled to indicate its sensitivity.
3. **Transportation:** When transporting media containing FCI, appropriate security measures must be taken to prevent loss or theft (e.g., using secure couriers, encryption).

Media Sanitization and Destruction:

1. **Sanitization:** Sanitization refers to the process of removing data from media in such a way that it cannot be recovered using standard forensic techniques. Acceptable sanitization methods include:
    - **Clearing:** Overwriting data with patterns (e.g., zeros, ones, random characters). This is suitable for some magnetic media but may not be effective for SSDs.

   - **Purging:** Using specialized software or hardware to overwrite data multiple times with complex patterns, effectively rendering the data unrecoverable. This method is suitable for most magnetic media and some SSDs.
   - **Degaussing:** Using a strong magnetic field to erase data from magnetic media. This method renders the media unusable for future storage.
   - **Cryptographic Erase:** Using the drive's built-in encryption capabilities to erase the encryption key, effectively rendering the data inaccessible. This is a fast and effective method for self-encrypting drives (SEDs).
2. **Destruction:** Destruction refers to physically destroying the media to render it unusable. Acceptable destruction methods include:
   - **Shredding:** Using a cross-cut shredder to destroy paper documents.
   - **Pulverizing:** Grinding media into small particles.
   - **Incineration:** Burning media to ashes.
   - **Drilling/Crushing:** Physically damaging the media to make it unusable.
3. **Sanitization/Destruction Procedures:**
   - All sanitization and destruction activities must be documented, including the date, method used, individual performing the action, and media serial number (if applicable).
   - A designated individual will be responsible for overseeing the media sanitization and destruction process.
   - For media that cannot be sanitized or destroyed in-house, a certified third-party vendor specializing in data destruction must be used. A Certificate of Destruction must be obtained for all media destroyed by third-party vendors.
4. **Sanitization Techniques for Specific Media Types:**
   - **Paper Documents:** Shredding using a cross-cut shredder is the preferred method. Burning or pulping are also acceptable.
   - **Hard Drives (HDDs):** Purging using specialized software or degaussing are preferred methods. Physical destruction (crushing, drilling, pulverizing) is also acceptable.
   - **Solid State Drives (SSDs):** Cryptographic erase (if supported), purging using specialized software designed for SSDs, or physical destruction are preferred methods. Overwriting is generally not reliable for SSDs.
   - **Optical Media (CDs, DVDs, Blu-rays):** Physical destruction (shredding, pulverizing) is the most reliable method.
   - **USB Flash Drives:** Purging using specialized software or physical destruction.

Release for Reuse:

Media that has been properly sanitized using approved methods may be released for reuse within the organization or for donation/resale. Media that has been physically destroyed cannot be reused.

Enforcement:

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract. [1]

Training and Awareness:

All users who handle media containing FCI will receive training on this policy and proper media handling, sanitization, and destruction procedures.

Review and Updates:

This policy will be reviewed and updated at least annually or as needed to address changes in technology, threats, or regulatory requirements.

Contact Information:

For questions or concerns regarding this policy, please contact [Contact Person] at [Contact Information].

Note: This is a sample Media Protection Policy and will need to be adapted to meet the specific needs and requirements of your organization. It is recommended to consult with a qualified cybersecurity professional to ensure compliance with CMMC Level 1 and other applicable regulations.

4. Physical Protection Policy (use as example)

Purpose:

This policy establishes requirements for the physical protection of [Organization Name]'s information systems, equipment, and operating environments containing Federal Contract Information (FCI). This policy is designed to meet the requirements of Cybersecurity Maturity Model Certification (CMMC) Level 1.

Scope:

This policy applies to all physical locations housing [Organization Name]'s information systems, equipment, and related operating environments, including but not limited to:

- Data centers
- Server rooms
- Office spaces
- Storage areas

Policy Statement:

[Organization Name] is committed to protecting its information systems and FCI by implementing appropriate physical security measures to prevent unauthorized access, damage, and disruption.

Physical Protection Requirements:

1. **Limit Physical Access to Authorized Individuals:**
    - Access to areas housing information systems and equipment will be restricted to authorized personnel only.
    - Access will be granted based on job responsibilities and the principle of least privilege.
    - Access control mechanisms will be implemented, such as:
        - Keycard access systems
        - Combination locks
        - Traditional locks and keys
    - All access points (doors, windows, etc.) will be secured.
2. **Escort Visitors and Monitor Visitor Activity:**
    - All visitors must sign in upon arrival and sign out upon departure, providing their name, organization, purpose of visit, and the name of the employee they are visiting.
    - Visitors will be issued visitor badges that must be visibly displayed at all times.
    - Visitors will be escorted by authorized personnel at all times while in areas housing information systems and equipment.

   - Visitor logs will be maintained and retained for a defined period [Specify time, e.g., one year].

3. **Maintain Audit Logs of Physical Access:**
   - Audit logs of physical access will be maintained for areas protected by electronic access control systems (e.g., keycard systems).
   - These logs will record the date, time, and individual accessing the area.
   - Audit logs will be regularly reviewed and retained for a defined period [Specify time, e.g., one year].
   - For areas not protected by electronic access control systems (e.g., areas secured with traditional locks and keys), manual logs will be maintained when feasible and necessary for high security areas.
4. **Control and Manage Physical Access Devices:**
   - **Keys and Access Cards:**
     - A designated individual will be responsible for managing keys and access cards.
     - A log of issued keys and access cards will be maintained.
     - Lost or stolen keys and access cards will be reported immediately and deactivated.
   - **Locks and Access Control Systems:**
     - Locks and access control systems will be regularly inspected and maintained.
     - Changes to access codes or card access permissions will be documented and authorized.
   - **Physical Inventories:** Periodic physical inventories of sensitive equipment will be conducted and documented.
5. **Environmental Controls:**
   - Appropriate environmental controls will be maintained in areas housing information systems and equipment to prevent damage from temperature, humidity, and other environmental factors.
6. **Protection from Natural Disasters and Other Threats:**
   - Reasonable measures will be taken to protect information systems and equipment from natural disasters (e.g., fire, flood, earthquake) and other threats (e.g., power outages, vandalism).

Enforcement:

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract. [1]

Training and Awareness:

All employees will receive training on this policy and their responsibilities for maintaining physical security.

Review and Updates:

This policy will be reviewed and updated at least annually or as needed to address changes in technology, threats, or regulatory requirements.

Contact Information:

For questions or concerns regarding this policy, please contact [Contact Person] at [Contact Information].

Note: This is a sample Physical Protection Policy and may need to be adapted to meet the specific needs and requirements of your organization. It is recommended to consult with a qualified security professional to ensure compliance with CMMC Level 1 and other applicable regulations.

5. System and Communication Protection Policy (use as example)

Purpose:

This policy establishes requirements for protecting [Organization Name]'s information systems and communications, including Federal Contract Information (FCI), at both external and internal boundaries. This policy is designed to meet the requirements of Cybersecurity Maturity Model Certification (CMMC) Level 1.

Scope:

This policy applies to all information systems owned, managed, or used by [Organization Name], including network devices, servers, workstations, mobile devices, and related communication channels.

Policy Statement:

[Organization Name] is committed to protecting its information systems and communications from unauthorized access, use, disclosure, disruption, modification, or destruction.

System and Communication Protection Requirements:

1. **Monitor, Control, and Protect Organizational Communications:**
    - Network traffic will be monitored at external and key internal boundaries using firewalls, intrusion detection/prevention systems (IDS/IPS), and other appropriate security tools.
    - Firewall rules will be implemented to control inbound and outbound network traffic based on approved ports, protocols, and IP addresses.
    - Access Control Lists (ACLs) will be used to restrict network access between different segments of the internal network.
    - Network traffic logs will be maintained and regularly reviewed.
2. **Implement Subnetworks for Publicly Accessible System Components:**
    - Publicly accessible system components (e.g., web servers, email servers) will be placed in a Demilitarized Zone (DMZ), a subnetwork physically or logically separated from the internal network.
    - Communication between the DMZ and the internal network will be strictly controlled through firewall rules.
    - Direct connections from the internet to the internal network will be prohibited.
3. **Identify, Report, and Correct Information and Information System Flaws:**
    - A vulnerability management process will be implemented to identify, report, and correct information system flaws (vulnerabilities) in a timely manner.
    - Regular vulnerability scans will be conducted on all information systems.

    - Security patches and updates will be applied promptly following vendor releases.
    - A process for reporting and tracking security incidents will be established.

4. **Provide Protection from Malicious Code:**
    - Antivirus and anti-malware software will be installed on all endpoints (workstations, servers, mobile devices).
    - Email filtering and web filtering will be implemented to block malicious emails and websites.
    - File integrity monitoring software will be used to detect unauthorized changes to critical system files.
5. **Update Malicious Code Protection Mechanisms:**
    - Antivirus and anti-malware software definitions and engines will be automatically updated regularly (e.g., daily).
    - Operating systems and application software will be patched promptly to address known vulnerabilities.
6. **Perform Periodic and Real-Time Scans:**
    - Regular full system scans will be conducted on all endpoints and servers [Specify frequency, e.g., weekly].
    - Real-time scanning of files from external sources (e.g., downloads, email attachments, USB drives) will be enabled to detect malicious code as files are accessed.
7. **Wireless Network Protection:**
    - Wireless networks will utilize strong encryption protocols (WPA2/3-Enterprise) and strong authentication methods.
    - Guest wireless networks will be isolated from internal networks.

Enforcement:

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract. [1]

Training and Awareness:

All users will receive training on this policy and their responsibilities for protecting information systems and communications. This includes training on identifying and reporting phishing emails, malicious websites, and other security threats.

Review and Updates:

This policy will be reviewed and updated at least annually or as needed to address changes in technology, threats, or regulatory requirements.

Contact Information:

For questions or concerns regarding this policy, please contact [Contact Person] at [Contact Information].

Note: This is a sample System and Communication Protection Policy and will need to be adapted to meet the specific needs and requirements of your organization. It is recommended to consult with a qualified cybersecurity professional to ensure compliance with CMMC Level 1 and other applicable regulations.

6. Home-Based Business Information Security Policy (use as example)

Policy Statement: This policy outlines the security requirements for protecting Federal Contract Information (FCI) within my home-based business. It addresses access control, identification and authentication, media protection, physical protection, and system and communication protection, aligning with CMMC Level 1 requirements.

1. Access Control Policy

- **Principle of Least Privilege:** Access to systems and data containing FCI will be granted only to authorized individuals and only to the extent necessary to perform their job duties.
- **User Accounts:** Each authorized user will have a unique user account with a strong, complex password. Generic or shared accounts are prohibited.
- **Access Reviews:** Access privileges will be reviewed periodically (at least annually) or upon termination of a contract/project to ensure that access is still appropriate.
- **Remote Access:** Remote access to systems containing FCI will be secured using strong authentication methods (e.g., multi-factor authentication where possible, strong passwords).

2. Identification and Authentication Policy

- **User Identification:** Each authorized user will be uniquely identified by a username or other unique identifier.
- **Password Requirements:** Passwords must:
  - Be at least 12 characters long.
  - Contain a mix of uppercase and lowercase letters, numbers, and symbols.
  - Not be based on personal information (e.g., name, birthdate).
  - Be changed at least every 90 days.
- **Password Management:** Passwords will not be written down or stored in plain text. (A password manager is recommended.)
- **Multi-Factor Authentication (MFA):** Where available and feasible (e.g., for email, cloud storage), MFA will be enabled to provide an additional layer of security.

3. Media Protection Policy

- **Media Handling:** Media containing FCI (e.g., USB drives, external hard drives, printed documents) will be physically protected and stored securely when not in use.
- **Media Storage:** Physical media will be stored in a locked drawer or cabinet when not in use.

- **Media Disposal:** When media is no longer needed, it will be securely destroyed. Digital media will be securely erased using appropriate software or physically destroyed. Printed documents will be shredded.
- **Electronic Media:** All electronic media used to store FCI will be encrypted at rest.

4. Physical Protection Policy

- **Work Area Security:** The home office/work area where FCI is processed and stored will be secured to prevent unauthorized access. This includes locking doors when the area is unattended.
- **Visitor Access:** Visitors to the home will be supervised to prevent unauthorized access to FCI or systems that handle FCI.
- **Device Security:** Laptops and other devices containing FCI will be physically secured when not in use to prevent theft.

5. System and Communication Protection Policy

- **Antivirus/Anti-malware:** Up-to-date antivirus and anti-malware software will be installed and actively running on all systems that handle FCI. Regular scans will be conducted.
- **Firewall Protection:** A firewall will be enabled on the home network and on individual devices to prevent unauthorized network access.
- **Software Updates:** Operating systems and software applications will be kept up to date with the latest security patches. Automatic updates will be enabled where possible.
- **Email Security:** Caution will be exercised when opening email attachments or clicking on links from unknown senders.
- **Wireless Security:** The home Wi-Fi network will be secured with a strong password (WPA2 or WPA3 encryption). The default router password will be changed.
- **Data Backup:** Regular backups of data containing FCI will be performed and stored securely, preferably using an encrypted cloud backup service or on a physically separate, secure storage device. Backup media will be protected in accordance with the media protection policy.

Policy Enforcement: This policy applies to all individuals who access or handle FCI within my home-based business. Failure to comply with this policy may result in appropriate action.

Policy Review: This policy will be reviewed and updated at least annually or as needed to reflect changes in business operations, technology, or applicable regulations.

This policy provides a starting point for a home-based business. It's important to review and adapt it to your specific circumstances and to stay updated on the latest CMMC guidance. Remember, this is a simplified example, and consulting with a cybersecurity professional is always recommended for a comprehensive security plan.

Note: This is a sample generic policy for a home-based business and will need to be adapted to meet the specific needs and requirements of your organization. It is recommended to consult with a qualified cybersecurity professional to ensure compliance with CMMC Level 1 and other applicable regulations.

XI. Key References

CMMC Assessment Guide Level 1(v2)

CMMC Scoping Guide Level 1(v2)

DFARS Clause 252.204-7012

DFARS Clause 252.204-7021

FAR Clause 52.204-21 b.1.xv

Official DoD CMMC Website

Project Spectrum

Supplier Performance Risk System (SPRS)

XII. Appendix A – Acronyms and Abbreviations

C3PAO	Certified Third-Party Assessor Organization
CMMC	Cybersecurity Maturity Model Certification
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DMZ	Demilitarized Zone
DoD	Department of Defense
ESP	External Service Provider
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
FeCC	The Puerto Rico Federal Contracting Center
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
PIEE	Procurement Integrated Enterprise Environment
SPRS	Supplier Performance Risk System
WPA	Wi-Fi Protected Address

This APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense.