CMMC Scoping Guide

Level 2

Version 2.11 - DRAFT | November 2023

DoD-CIO-00006 (ZRIN 0790-ZA22)

NOTICES

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing CMMC requirements under the law or departmental policies.

[DISTRIBUTION STATEMENT A] Approved for public release.

Introduction

This document provides scoping guidance for Level 2 of the Cybersecurity Maturity Model Certification (CMMC) as set forth in section 170.19 of title 32, Code of Federal Regulations (CFR). Guidance for scoping a CMMC Level 1 assessment can be found in the *CMMC Scoping Guide – Level 1* document. Guidance for scoping a CMMC Level 3 assessment can be found in the *CMMC Scoping Guide – Level 3* document. More details on the CMMC Model can be found in the *CMMC Model Overview* document.

Purpose and Audience

This guide is intended for Organizations Seeking Assessment (OSAs) that will be conducting a CMMC Level 2 Self-Assessment in accordance with 32 CFR § 170.16, Organizations Seeking Certification (OSCs) that will be obtaining a CMMC Level 2 Certification Assessment in accordance with 32 CFR § 170.17, and the professionals or companies that will support them in those efforts. OSCs are a subset of OSAs as all organization will participate in an assessment, but self-assessment cannot result in a certification.

Identifying the CMMC Assessment Scope

An *Assessment*, as defined in 32 CFR § 170.4, means the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

This document should help the reader understand the categorization of assets that, in turn, inform the specification of the boundary for a CMMC assessment. The scope of the CMMC Program does not include classified assets, even if they contain applicable Controlled Unclassified Information (CUI).

Prior to conducting a CMMC assessment, the OSA must specify the CMMC Assessment Scope as defined in 32 CFR § 170.19. The CMMC Assessment Scope defines which assets within the OSA's environment will be assessed and the details of the assessment.

Because the scoping of a CMMC Level 2 assessment is not the same as the scoping of a Level 3 assessment, before determining the CMMC Assessment Scope it is important to first consider whether the goal is a CMMC Level 2 Final Certification or CMMC Level 3 Final Certification. If the intent is not to obtain a CMMC Level 3 Final Assessment Certification, as defined in 32 CFR § 170.18(a)(1), refer to the scoping guidance provided in this document which provides guidance on 32 CFR § 170.19(c). If the intent is to obtain a CMMC Level 3 Final Certification, refer to the guidance provided in the CMMC Scoping Guide – Level 3 document, which provides guidance on 32 CFR § 170.19(d). The OSC must achieve a CMMC Level 2 Final Certification and complete and implement all Level 3 security requirements specified in § 170.14(c)(4) prior to initiating a CMMC Level 3 Certification Assessment. Both documents are available on the official CMMC documentation site at https://dodcio.defense.gov/CMMC/Documentation/.

CMMC Asset Categories

For a Level 2 assessment, assets are mapped into one of five categories defined in 32 CFR § 170.19(c)(1) Table 3. This table describes each asset category and its corresponding OSA requirements and CMMC assessment requirements. Additional information about each asset category is provided in the ensuing sections.

Table 1. CMMC Asset Categories and Associated Requirements Overview

Asset Category	Asset Description	OSA Requirements	CMMC Assessment Requirements
Assets that are in the Level 2 CMMC Assessment Scope[1]			
Controlled Unclassified Information (CUI) Assets	o Assets that process, store, or transmit CUI	o Document in the asset inventory o Document in the System Security Plan (SSP) o Document in the network diagram of the CMMC Assessment Scope o Prepare to be assessed against CMMC security requirements	o Assess against CMMC security requirements
Security Protection Assets	o Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI	o Document in the asset inventory o Document in SSP o Document in the network diagram of the CMMC Assessment Scope o Prepare to be assessed against CMMC security requirements	o Assess against CMMC security requirements
Contractor Risk Managed Assets	o Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place o Assets are not required to be physically or logically separated from CUI assets	o Document in the asset inventory o Document in the SSP o Document in the network diagram of the CMMC Assessment Scope o Prepare to be assessed against CMMC security requirements	o Review the SSP: i. If sufficiently documented, do not assess against other CMMC security requirements, except as noted below ii. If OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies iii. The limited check(s) shall not materially increase the assessment duration nor the assessment cost iv. The limited check(s) will be assessed against CMMC security requirements
Specialized Assets	o Assets that can process, store, or transmit CUI but are unable to be fully secured, including Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment	o Document in the asset inventory o Document in the SSP o Show these assets are managed using the contractor's risk-based security policies, procedures, and practices o Document in the network diagram of the CMMC Assessment Scope	o Review the SSP o Do not assess against other CMMC security requirements

[1] Inclusive of requirements for FCI

Assets that are not in the Level 2 CMMC Assessment Scope			
Out-of-Scope Assets	o Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets o Assets that are physically or logically separated from CUI assets o Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset	o Prepare to justify the inability of an Out-of-Scope Asset to store, process, or transmit CUI	o None

Additional Guidance on Level 2 Scoping

The OSA is required to document all asset categories that are part of the CMMC Level 2 Certification Assessment or Self-Assessment in an asset inventory and provide a network diagram of the CMMC Assessment Scope to facilitate scoping discussions during pre-assessment activities.

CUI Assets

CUI Assets process, store, or transmit CUI as follows:

- **Process** – CUI can be used by an asset (e.g., accessed, entered, edited, generated, manipulated, or printed).
- **Store** – CUI is inactive or at rest on an asset (e.g., located on electronic media, in system component memory, or in physical format such as paper documents).
- **Transmit** – CUI is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods).

CUI Assets are part of the CMMC Assessment Scope and are assessed against all CMMC requirements.

In addition, the OSA is required to:

- document these assets in an asset inventory;
- document these assets in the SSP; and
- provide a network diagram of the CMMC Assessment Scope (to include these assets) to facilitate scoping discussions during the pre-assessment.

Security Protection Assets

Security Protection Assets provide security functions or capabilities within the OSA's CMMC Assessment Scope.

Security Protection Assets are part of the CMMC Assessment Scope and are assessed against all CMMC requirements. For example, an External Service Provider (ESP, defined in 32 CFR §170.4) that provides a security information and event management (SIEM) service may be separated logically and may process no CUI, but the SIEM does contribute to meeting the CMMC requirements within the OSA's CMMC Assessment Scope. Table 2 provides examples of Security Protection Assets.

Table 2. Security Protection Asset Examples

Asset Type	Security Protection Asset Examples
People	• Consultants who provide cybersecurity service • Managed service provider personnel who implement system maintenance • Enterprise network administrators
Technology	• Cloud-based security solutions • Hosted Virtual Private Network (VPN) services • SIEM solutions
Facilities	• Co-located data centers • Security Operations Centers (SOCs) • OSA office buildings

In addition, the OSA is required to:

- document these assets in an asset inventory;
- document these assets in the SSP; and
- provide a network diagram of the CMMC Assessment Scope (to include these assets) to facilitate scoping discussions during the pre-assessment.

Contractor Risk Managed Assets

Contractor Risk Managed Assets are not intended to, but are capable of processing, storing, or transmitting CUI because of the security policy, procedures, and practices in place. Contractor Risk Managed Assets are not required to be physically or logically separated from CUI Assets.

Contractor Risk Managed Assets are part of the Level 2 CMMC Assessment Scope. These assets are managed using the OSA's risk-based information security policy, procedures, and practices. Furthermore, the assets must be assessed against CMMC requirements if insufficiently documented in the SSP or if the OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets. In these cases, the assessor can conduct a limited check to identify deficiencies.

In addition, the OSA is required to:

- document these assets in an asset inventory;
- document these assets in the SSP; and
- provide a network diagram of the CMMC Assessment Scope (to include these assets) to facilitate scoping discussions during the pre-assessment.

Assessment requirements for Contractor Risk Managed Asset are detailed in Table 1.

Specialized Assets

The following are considered specialized assets for a CMMC Level 2 assessment when documented in accordance with Table 1 (reprinted from 32 CFR § 170.19(c)(1) Table 3).

- **Government Furnished Equipment (GFE)** is all equipment owned or leased by the government and includes OSA/OSC-acquired equipment that is based on government required specifications and/or configurations. Government Furnished Equipment does not include intellectual property or software [Reference: Federal Acquisition Regulation (FAR) 52.245-1].
- **Internet of Things (IoT) or Industrial Internet of Things (IIoT)** means the network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information, as. defined in NIST SP 800-172A. They are interconnected devices having physical or virtual representation in the digital world, sensing/actuation capability, and programmability features. They are uniquely identifiable and may include smart electric grids, lighting, heating, air conditioning, and fire and smoke detectors.
- **Operational Technology (OT)**[2] means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. [Source: as defined in NIST SP 800-160v2 Rev 1 (incorporated by reference, see 32 CFR § 170.2.)]. NOTE: Operational Technology (OT) specifically includes Supervisory Control and Data Acquisition (SCADA); this is a rapidly evolving field. [Source: DRAFT, NIST SP 800-82r3 is used in manufacturing systems, industrial control systems (ICS), or supervisory control and data acquisition (SCADA) systems.
- **Restricted Information Systems** means systems (and associated IT components comprising the system) that are configured based on government requirements (i.e., connected to something that was required to support a functional requirement) and are used to support a contract (e.g., fielded systems, obsolete systems, and product deliverable replicas). They can include systems [and associated Information Technology (IT) components comprising the system] that are configured based on government security requirements (i.e., connected to something that was required to support a functional requirement) and are used to support a contract (e.g., fielded systems, obsolete systems, and product deliverable replicas).

[2] OT includes hardware and software that use direct monitoring and control of industrial equipment to detect or cause a change.

- **Test Equipment** means hardware and/or associated IT components used in the testing of products, system components, and contract deliverables. It can include hardware and/or associated IT components used in the testing of products, system components, and contract deliverables (e.g., oscilloscopes, spectrum analyzers, power meters, and special test equipment).

Specialized Assets are part of the CMMC Assessment Scope. In accordance with 32 CFR § 170.19(c)(1) Table 3, the OSA shall document these assets in the SSP and detail how they are managed using the OSA's risk-based information security policy, procedures, and practices.

In addition, the OSA is required to:

- document these assets in asset inventory;
- document these assets in the SSP to show they are managed using the OSA/OSC's risk-based security policies, procedures, and practices; and
- provide a network diagram of the CMMC Assessment Scope (to include these assets) to facilitate scoping discussions during the pre-assessment.

An assessor will review the SSP to verify that specialized assets are managed using the OSA's risk-based information security policy, procedures, and practices, and accounted for within the OSA's CMMC Assessment Scope.

Out-of-Scope Assets

Out-of-Scope Assets cannot process, store, or transmit CUI, and do not provide security protections for CUI Assets. Assets that are physically or logically separated from CUI Assets and do not provide security protections for CUI Assets are also Out-of-Scope Assets. An asset that falls into any in-scope asset category cannot be considered an Out-of-Scope Asset.

In accordance with 32 CFR § 170.19(c)(1), Out-of-Scope Assets are not part of a CMMC Level 2 assessment. There are no documentation requirements for Out-of-Scope Assets.

Defining the CMMC Assessment Scope

After categorizing its assets, the OSA then specifies the CMMC Assessment Scope.

The CMMC Assessment Scope includes all assets in the OSA's environment that will be assessed in accordance with Table 1. OSAs will be required to provide documentation that specifies the CMMC Assessment Scope to the assessor. Details about required documentation for each asset category can be found in the CMMC Asset Categories section above.

The following asset categories are part of the Level 2 CMMC Assessment Scope:

- CUI Assets
- Security Protection Assets

- Contractor Risk Managed Assets
- Specialized Assets

Separation Techniques

Separation is a system architecture design concept that can provide physical/logical isolation of assets that process, transmit, or store CUI from assets not involved with CUI. Effective separation involves logically or physically separating assets and is required only for Out-of-Scope Assets. By separating assets, the CMMC Assessment Scope can be limited. Effective separation for CMMC follows the guidance in NIST SP 800-171 Rev 2, which states:

> *If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.*

Logical separation occurs when data transfer between physically connected assets (wired or wireless) is prevented by non-physical means such as software or network assets (e.g., firewall, routers, VPNs, VLANs).

Physical separation occurs when assets have no connection (wired or wireless). Data can only be transferred manually (e.g., USB drive).

Use Cases

CMMC Level 1 security requirements are closely aligned with corresponding CMMC Level 2 security requirements, but they are not identical. Assessment and attestation requirements for the two levels also differ. If an OSA processes, stores, or transmits FCI and CUI within its systems, two separate assessments should be performed. The OSA identifies those assets that process, store, or transmit FCI and those assets which process, store, or transmit CUI and defines the assessment scopes separately.

A CMMC Level 2 Self-Assessment or CMMC Level 2 Certification Assessment, regardless of result, does not satisfy the need to assess the FCI environment. If FCI is processed, stored, or transmitted within the same scope as CUI in the CMMC Level 2 scope, then the methods to implement the CMMC Level 2 security requirements could apply towards meeting the CMMC Level 1 assessment objectives. The OSA may choose to conduct the assessments concurrently but two distinct assessments are required. The OSA is still responsible for ensuring that only authorized users and processes have access to data regardless of its designation.

If FCI and CUI do not share an environment, the two assessments would be performed independently and methods to implement security requirements in one scope would not apply to the other scope.

Satisfaction of CMMC security requirements may be accomplished by people, process, or technologies which apply to the entire OSA enterprise. This does not mean all assets across the entire OSA enterprise are automatically part of a CMMC Assessment Scope. For example, a centralized IT group may acquire, configure, deploy, and maintain a standard anti-malware tool. Systems within a defined assessment scope use that centrally deployed tool. The anti-malware tool and the people in the IT group who maintain it, the processes and policies to deploy and update it, and the supporting systems (i.e., management server, etc.) could be in the CMMC Assessment Scope but other functions performed by the enterprise IT and other enterprise assets would not be automatically part of the CMMC Assessment Scope.

External Service Provider Considerations

An External Service Provider (ESP) can be within the scope CMMC requirements if it meets CUI Asset and/or Security Protection Asset criteria. **To be considered an ESP, data (specifically CUI or Security Protection Data, e.g., log data, configuration data) must reside on the ESP assets** as set forth in 32 CFR § 170.19(c)(2)**.** Special considerations in for an OSA using an ESP include the following:

- Evaluate the ESP's shared responsibility matrix where the provider identifies security control objectives that are the provider's responsibility and security control objectives that are the OSA's responsibility.
- Consider the agreements in place with the ESP, such as service-level agreements, memoranda of understanding, and contracts that support the OSA's information security objectives.
- As set forth 32 CFR § 170.16(c)(2) and 32 CFR § 170.17(c)(5) respectively, an OSA may use a Federal Risk and Authorization Management Program (FedRAMP) Moderate (or higher) cloud environment to process, store, or transmit CUI in execution of a contract or subcontract, if the OSA ensures the Cloud Service Provider's offering either:
    - is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace, **OR**
    - is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline in accordance with DFARS 252.204-7012. This condition is met if the evidence includes a System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the

Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 requirements.

- OSAs shall also be assessed at Level 2, as applicable, against their on-premise infrastructure connecting to the CSP. As part of the CMMC Assessment Scope, the security requirements from the CRM must be documented or referred to in the OSA's SSP, which will also be assessed.
- If the OSA utilizes an ESP other than a CSP, the ESP must have a CMMC Level 2 Certification as set forth in 32 CFR § 170.19(c)(2). If the ESP is **internal** to the OSA, the CMMC requirements being assessed should be listed in the OSA's SSP to show connection to its in-scope environment.


DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
CYBERSECURITY MATURITY MODEL
CERTIFICATION