CMMC Scoping Guide

Level 2

Version 2.13 | September 2024

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 Level 1 self-assessment can be found in the *CMMC Scoping Guide – Level 1* document. Guidance for scoping a Level 3 certification 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 Level 2 self-assessment in accordance with 32 CFR § 170.16, Organizations Seeking Certification (OSCs) that will be obtaining a Level 2 certification assessment in accordance with 32 CFR § 170.17, and the professionals or companies that will support them in those efforts. The security requirements for a Level 2 self-assessment and a Level 2 certification assessment are the same, the only difference in these assessments is whether it is conducted by the OSA or by an independent C3PAO.

OSCs are a subset of OSAs as all organizations 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(c). 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 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 if the organization will seek a CMMC Status of Final Level 3 (DIBCAC). If the intent is to obtain a CMMC Status of Final Level 3 (DIBCAC), the OSC should also consider the guidance provided in the *CMMC Scoping Guide – Level 3* document. The OSC must closeout any Level 2 Plan of Action and Milestones (POA&M) and achieve a CMMC Status of Final Level 2 (C3PAO) prior to initiating a Level 3 certification assessment.

Assets designated as Contractor Risk Managed Assets (CRMAs) in the Level 2 CMMC Assessment Scope are treated as CUI assets if they fall within the Level 3 CMMC Assessment Scope. OSCs may choose to designate them as CUI Assets for the Level 2 certification assessment and have them assessed by a C3PAO.

Since the assessment requirements for Specialized Assets differ between Level 2 and Level 3, the OSC may choose to have them assessed by a C3PAO during the Level 2 certification assessment. During a Level 3 certification assessment, DCMA DIBCAC may check any Level 2 security requirement of any in-scope asset.

CRMAs and Specialized Assets not assessed to the Level 3 scoping requirements by a C3PAO during the Level 2 certification assessment will undergo limited checks for compliance with Level 2 security requirements during the DCMA DIBCAC certification assessment.

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			
Controlled Unclassified Information (CUI) Assets	○ Assets that process, store, or transmit CUI	○ Document in the asset inventory ○ Document asset treatment in the System Security Plan (SSP) ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC Level 2 security requirements	○ Assess against all Level 2 security requirements
Security Protection Assets	○ Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope	○ Document in the asset inventory ○ Document asset treatment in SSP ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC Level 2 security requirements	○ Assess against Level 2 security requirements that are relevant to the capabilities provided
Contractor Risk Managed Assets	○ Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place ○ Assets are not required to be physically or logically separated from CUI assets	○ Document in the asset inventory ○ Document asset treatment in the SSP ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC Level 2 security requirements	○ Review the SSP: i. If sufficiently documented, do not assess against other CMMC security requirements, except as noted 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	○ 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,	○ Document in the asset inventory ○ Document asset treatment in the SSP ○ Show these assets are managed using the	○ Review the SSP ○ Do not assess against other CMMC security requirements

	Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment	contractor's risk-based security policies, procedures, and practices ○ Document in the network diagram of the CMMC Assessment Scope	
Assets that are not in the Level 2 CMMC Assessment Scope			
Out-of-Scope Assets	○ Assets that 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 ○ Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset ○ An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset	○ Prepare to justify the inability of an Out-of-Scope Asset to store, process, or transmit CUI	○ None

Additional Guidance on Level 2 Scoping

The OSA is required to document all asset categories that are part of the Level 2 self-assessment or certification 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 each asset in an asset inventory; there is no requirement to embed each asset in the System Security Plan (SSP);
- document the treatment of these assets in the SSP;
- 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 Data

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 Level 2 security requirements that are relevant to the capabilities provided. 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 not process 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.

Security Protection Data means data stored or processed by Security Protection Assets that are used to protect an OSA's assessed environment.

Security Protection Data is security-relevant information which, if disclosed, could aid an attacker in the compromise of the system. It includes, but is not limited to:

- configuration data required to operate a security protection asset,

- log files generated by or ingested by a security protection asset,
- data related to the configuration or vulnerability status of in-scope assets, and
- passwords that grant access to the in-scope environment.

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 each asset in an asset inventory; there is no requirement to embed each asset in the SSP;
- document the treatment of 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 each asset in an asset inventory; there is no requirement to embed each asset in the SSP;
- document the treatment of 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 Level 2 assessment when documented in accordance with Table 1 (reprinted from 32 CFR § 170.19(c)(1) Table 3). Note that a Specialized Asset may be eligible for an Enduring Exception.

- **Government Furnished Equipment (GFE)** is all equipment owned or leased by the government and includes OSA-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)**[1] 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 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).
- **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).

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

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 each asset in asset inventory; there is no requirement to embed every asset in the SSP;
- document these assets in the SSP to show they are managed using the OSA'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. The assessor will not retain a copy of the SSP.

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 Level 2 self-assessment or certification 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).

Self-assessments and certification assessments may be valid for a defined CMMC Assessment Scope as outlined in 32 CFR § 170.19 CMMC Scoping. A new assessment is required if there are significant architectural or boundary changes to the previous CMMC Assessment Scope. Examples include, but are not limited to, expansions of networks or mergers and acquisitions. Operational changes within a CMMC Assessment Scope, such as adding or subtracting resources within the existing assessment boundary that follow the existing SSP, do not require a new assessment, but rather may be covered by annual affirmations to the continuing compliance with requirements.

External Service Provider Considerations

An External Service Provider (ESP) can be within the OSA's scope of 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 for an OSA using an ESP include the following:

- The use of an ESP, its relationship to the OSA, and the services provided need to be documented in the OSA's SSP and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSA and ESP with respect to the services provided.
- Evaluate the ESP's CRM where the provider identifies security requirement objectives that are the provider's responsibility and security requirement 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.
- ESPs that are CSPs,
  - and store, process, or transmit CUI, must meet the FedRAMP requirements in DFARS clause 252.204-7012.
  - and do NOT store, process, or transmit CUI, are not required to meet FedRAMP requirements in DFARS clause 252.204-7012. Services provided by an ESP are in the OSA's assessment scope.
- ESPs that are not a CSP,
  - and store, process, or transmit CUI, require assessment. The ESP services used to meet OSA requirements are within the scope of the OSA's CMMC assessment.
  - and do NOT store, process, or transmit CUI, do not require their own CMMC assessment. Services provided by an ESP are in the OSA's assessment scope.
  - may voluntarily request a C3PAO assessment, and a C3PAO may conduct such an assessment, if the ESP makes that business decision.
- 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.
- ESPs can be part of the same corporate/organizational structure but still be external to the OSA such as a centralized SOC or NOC which supports multiple business units. The same requirements apply and are based on whether or not the ESP provides cloud services and whether or not the ESP processes, stores, or transmits CUI on their systems.
- An ESP that is used as staff augmentation and the OSA provides all processes, technology, and facilities does not need CMMC assessment.
- When ESPs are assessed as part of an OSAs assessment, the type of the assessment is dictated by the OSA's DoD solicitation and contract requirement.

Cloud Service Provider (CSP) means an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. An ESP would be considered a CSP when it provides its own cloud services based on a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction.

An ESP (not a CSP) that provides technical support services to its clients would be considered a Managed Service Provider. It does not host its own cloud platform offering. An ESP may utilize cloud offerings to deliver services to clients without being a CSP.

An ESP that manages a third-party cloud service on behalf of an OSA would not be considered a CSP.

Not all companies that provide services to an OSA should be considered an ESP. Cloud based services such as human resource and accounting SaaS applications typically do not contribute to the security of the OSA's environment; process or store SPD; or process, store, or transmit CUI. The OSA must determine if the company providing the service should be considered an ESP based on the services provided and if CUI is processed, stored, or transmitted.

Use Cases

FCI and CUI in the Same Assessment Scope

A Level 2 self-assessment or Level 2 certification assessment satisfies the Level 1 self-assessment requirements for the same CMMC Assessment Scope. If FCI is processed, stored, or transmitted within the same scope as CUI in the Level 2 scope, then the methods to implement the Level 2 security requirements apply towards meeting the Level 1 assessment objectives. The OSA is responsible for ensuring that only authorized users and processes have access to data regardless of its designation.

FCI and CUI in Different Assessment Scopes

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

Use of Enclaves

Satisfaction of CMMC security requirements may be accomplished by people, processes, 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 (e.g., management server) 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.

Within the enclave, the OSA determines which requirements are implemented and which requirements are inherited; all requirements must be MET. If a process, policy, tool, or technology within the enclave would invalidate an implementation at the Enterprise level, that requirement cannot be inherited and the OSA must demonstrate that it is MET by implementation in some other way.

There is no established metric for inherited implementations from an enterprise to any defined enclaves. The OSA determines the architecture that best meets its business needs and complies with CMMC requirements.

Security Protection Data

Security Protection Data (SPD) can be created by or used by a Security Protection Asset (SPA). Aggregated logs in a SIEM are one example of SPD and the SIEM is considered the SPA. The SIEM is part of the assessment scope. Because of the wide range of SIEM tools available, (on-premise hardware appliance; on-premise virtual appliance; or cloud based), methods of

assessing the SIEM will also vary. If the SIEM and/or associated log data is hosted or maintained by an ESP, then the portion of the ESP that is used to provide the SIEM service or log storage is part of the OSA's assessment scope. SIEM logs are typically available in hot storage for some period of time as part of the SIEM deployment. In this case, the SPD is collocated with the SPA. Cold storage of logs for a longer period of time is typically done offline or in cloud storage. The method used and the location of the cold storage are also in the OSA's assessment scope.

This page intentionally left blank.


DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
CYBERSECURITY MATURITY MODEL
CERTIFICATION