CMMC Scoping Guide

Level 3

Version 2.13 | September 2024

DoD-CIO-00007 (ZRIN 0790-ZA23)

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. Distribution is unlimited.

Introduction

This document provides scoping guidance for Level 3 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 2 self-assessment or certification assessment can be found in the *CMMC Scoping Guide – Level 2* 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 Certification (OSCs) that will be obtaining a Level 3 certification assessment and the professionals or companies that will support them in those efforts.

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 Level 3 certification assessment, the CMMC Assessment Scope must be defined as addressed in 32 CFR § 170.19(d). The CMMC Assessment Scope informs which assets within the OSC's environment will be assessed and the details of the assessment.

When seeking a Level 3 certification assessment, the OSC must have a Final Level 2 (C3PAO) CMMC Status for the same CMMC Assessment Scope as the Level 3 assessment. Any Level 2 Plan of Action and Milestones (POA&M) items, as defined in 32 CFR §170.4, must be closed prior to the initiation of the Level 3 assessment. The Level 3 CMMC Assessment Scope may be a subset of the Level 2 CMMC Assessment Scope (e.g., a Level 3 data enclave with greater restrictions and protections within the Level 2 data enclave).

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 Level 3 certification assessment and will be assessed against all CMMC Level 3 security requirements.

CMMC Asset Categories

For a Level 3 assessment, assets are mapped into one of four categories defined in 32 CFR § 170.19(d)(1) Table 4. This table describes each asset category and its corresponding OSC requirements and CMMC assessment requirements. Additional information about each asset category is provided in the ensuing sections.

Table 1. Level 3 Asset Categories and Associated Requirements Overview

Asset Category	Asset Description	OSC Requirements	CMMC Assessment Requirements
Assets that are in the Level 3 CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	○ Assets that process, store, or transmit CUI ○ Assets that can, but are not intended to, process, store, or transmit CUI (defined as Contractor Risk Managed Assets in Table 1 to 32 CFR § 170.19(c)(1))	○ 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 and Level 3 security requirements	○ Limited check against Level 2 and assess against all Level 3 CMMC security requirements
Security Protection Assets	○ Assets that provide security functions or capabilities to the OSC's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI	○ 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 and Level 3 security requirements	○ Limited check against Level 2 and assess against all Level 3 CMMC security requirements that are relevant to the capabilities provided
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, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment	○ 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 and Level 3 security requirements	○ Limited check against Level 2 and assess against all Level 3 CMMC security requirements ○ Intermediary devices are permitted to provide the capability for the specialized asset to meet one or more CMMC security requirements
Assets that are not in the Level 3 CMMC Assessment Scope			

Asset Category	Asset Description	OSC Requirements	CMMC Assessment Requirements
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 3 Scoping

The OSC is required to document all assets that are part of the Level 3 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 can process, store, or transmit CUI as follows:

- **Process** – CUI is 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 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 OSC 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;
- 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 OSC's CMMC Assessment Scope.

Security Protection Assets are part of the CMMC Assessment Scope and are assessed against all Level 2 and Level 3 security requirements that are relevant to the capabilities provided. For example, an External Service Provider (ESP) that provides a security information and event management (SIEM) service may be separated logically and may process no CUI, but the SIEM contributes to meeting the CMMC requirements within the OSC'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 services • 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) • OSC office buildings

In addition, the OSC 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.

Specialized Assets

The following are considered Specialized Assets for a Level 3 certification assessment:

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

[1] NIST SP800-172A March 2022

- **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 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).

Specialized Assets are part of the Level 3 CMMC Assessment Scope per 32 CFR § 170. 19(d)(1) Table 3. Note that Specialized Assets may be eligible for an Enduring Exception. The OSC should prepare for these assets to be assessed against all CMMC requirements unless they are physically or logically isolated into purpose-specific networks (with no connection to the Internet or other networks). Specialized Assets may have limitations on the application of certain security requirements. To accommodate such issues intermediary devices are permitted to provide the capability for the specialized asset to meet one or more CMMC requirements. An example of an intermediary device used in conjunction with a specialized asset is a boundary device or a proxy.

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. Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset.

In accordance with 32 CFR § 170.19(d)(1), Out-of-Scope Assets are not part of a Level 3 certification assessment. There are no documentation requirements for Out-of-Scope Assets.

Defining the CMMC Assessment Scope

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

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

The CMMC Assessment Scope includes all assets in the OSC's environment that will be assessed in accordance with Table 1. OSCs 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 3 CMMC Assessment Scope:

- CUI Assets
- Security Protection Assets
- Specialized Assets

Self-assessments and certification assessments are 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 are covered by the 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 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(d)(2). Special considerations in for an OSC 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 control objectives that are the provider's responsibility and security control objectives that are the OSC's responsibility.
- Consider the agreements in place with the ESP, such as service-level agreements, memoranda of understanding, and contracts that support the OSC'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.
        - Use of a CSP does not relieve an OSC of its obligation to implement the 24 Level 3 security requirements. These 24 requirements apply to every environment where the CUI data is processed, stored, or transmitted, when Level 3 (DIBCAC) is the designated CMMC Status. If any of these 24 requirements are inherited from a CSP, the OSC must demonstrate that

protection during a Level 3 certification assessment via a Customer Implementation Summary/Customer Responsibility Matrix (CIS/CRM) and associated Body of Evidence (BOE). The BOE must clearly indicate whether the OSC or the CSP is responsible for meeting each requirement and which requirements are implemented versus inherited.

  - 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 DIBCAC assessment, and the DIBCAC may conduct such an assessment, if the ESP makes that business decision.
- OSAs shall also be assessed at Level 2 or Level 3, as applicable, against their on-premise infrastructure connecting to the ESP. 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

An ESP may voluntarily request its own Level 3 assessment by contacting the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). Contact information can be found at https://www.dcma.mil/DIBCAC/.

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.

This page intentionally left blank.


DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
CYBERSECURITY MATURITY MODEL
CERTIFICATION