CMMC Assessment Scope

Level 3

Version 2.1 - DRAFT | July 2023

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 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 CMMC Level 1 assessment can be found in CMMC Scoping Guide – Level 1. Guidance for Scoping a CMMC Level 2 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 CMMC Level 3 assessment and the professionals or companies that will support them in those efforts.

Identifying the CMMC Assessment Scope

This document provides scoping guidance as set forth in 32 CFR § 170.19(d) for conducting CMMC assessments for Level 3.

A CMMC 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.

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

Prior to conducting a CMMC assessment, the Level 3 CMMC Assessment Scope must be defined as addressed in 32 CFR. § 170.19(d) and the CMMC Assessment Scope – Level 3 document. 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, the OSC must have a CMMC Level 2 Final Certification for the same scope as the Level 3 assessment. Any Level 2 Plan of Action and Milestones (POA&M as defined in 32 CFR §170.4) items must be closed prior to the initiation of the CMMC Level 3 assessment. The CMMC 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).

CMMC Asset Categories

The *CMMC Assessment Guide – Level* 3 maps the assets of OSCs into one of four categories. Per 32 CFR. § 170.19(d)(1). Table 1 describes each asset category, OSC requirements, and CMMC assessment requirements. Additional information about each asset category is provided in the ensuing sections.

Table 1. CMMC 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	o Assets that process, store, or transmit CUI o Assets that can, but are not intended to, process, store, or transmit CUI (defined as Contractor Risk Managed Assets in 32 CFR. § 170.19 Table 1)	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 all CMMC security requirements
Security Protection Assets	o 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	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 all 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 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 all CMMC security requirements o 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			
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

The following sections provide more information about the CMMC Asset Categories and the documentation required during an assessment.

The OSC is required to document all assets that are part of the CMMC Assessment Scope 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 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 OSC'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) 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.

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 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.

Specialized Assets

The following are considered Specialized Assets for a CMMC Level 3 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. 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

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

evolving field. [Source: DRAFT, NIST SP 800-82r3is 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).
- **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 4. 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.

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 § 170.35, Out-of-Scope Assets are not part of a CMMC Level 3 assessment. There are no documentation requirements for Out-of-Scope Assets.

Defining the CMMC Assessment Scope

Prior to conducting a CMMC assessment, the Level 3 CMMC Assessment Scope must be defined as addressed in 32 CFR § 170.19(d) and the CMMC Assessment Scope – Level 3 document. The CMMC Assessment Scope informs which assets within the OSC's environment will be assessed and the details of the assessment. 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 to the Certified Assessor that specifies the CMMC Assessment Scope. 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 CMMC Assessment Scope:

- CUI Assets
- Security Protection Assets
- Specialized Assets

Relationship between Level 2 and Level 3 CMMC Assessment Scope

When seeking a Level 3 Certification, the OSA must have a CMMC Level 2 Final Certification for the same scope as the Level 3 assessment. Any Level 2 POA&M items must be closed prior to the initiation of the CMMC Level 3 assessment. The CMMC 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).

External Service Provider Considerations

An External Service Provider (ESP) can be within the 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 32 CFR § 170.19 for an OSC 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 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.
- As set forth in 32 CFR § 170.18(c)(5), if the OSC uses 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, the OSC must ensure the Cloud Service Provider’s offering either:
    1. is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace, **OR**
    2. 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.
- If the OSC seeking CMMC Level 3 Certification utilizes an ESP, other than a CSP, the ESP must have a CMMC Level 3 Certification as set forth in 32 CFR § 170.19(c)(2). If the

ESP is **internal** to the OSC, the CMMC requirements being covered should be listed in the OSC's SSP to show connection to its in-scope environment.

OFFICE OF THE UNDER SECRETARY OF DEFENSE
ACQUISITION AND SUSTAINMENT

CYBERSECURITY MATURITY MODEL
CERTIFICATION