
# CMMC Assessment Scope

## Level 2

Version 2.0 | December 2021

# NOTICES



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center, and under Contract No. HQ0034-13-D-0003 and Contract No. N00024-13-D-6400 with the Johns Hopkins University Applied Physics Laboratory LLC, a University Affiliated Research Center.

# Identifying the CMMC Assessment Scope

This document provides information on the categorization of assets that, in turn, inform the specification of assessment scope for a Cybersecurity Maturity Model Certification (CMMC) assessment. The ensuing sections discuss CMMC asset categories as well as the associated requirements for Defense Industrial Base (DIB) contractors and CMMC assessments.

## CMMC Asset Categories

The *CMMC Assessment Guide – Level 2* maps contractor assets into one of five categories. Table 1 describes each asset category, contractor requirements, and assessment requirements. Additional information about each asset category is provided in the ensuing sections.

**Table 1. CMMC Asset Categories Overview**

| Asset Category | Asset Description | Contractor Requirements | CMMC Assessment Requirements |
|---|---|---|---|
| *Assets that are in the CMMC Assessment Scope* | | | |
| **Controlled Unclassified Information (CUI) Assets** | • Assets that process, store, or transmit CUI | • Document in the asset inventory<br>• Document in the System Security Plan (SSP)<br>• Document in the network diagram of the CMMC Assessment Scope<br>• Prepare to be assessed against CMMC practices | • Assess against CMMC practices |
| **Security Protection Assets** | • Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI | | |
| **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<br>• Assets are not required to be physically or logically separated from CUI assets | • Document in the asset inventory<br>• Document in the SSP<br>  ○ Show these assets are managed using the contractor's risk-based security policies, procedures, and practices<br>• Document in the network diagram of the CMMC Assessment Scope | • Review the SSP in accordance with practice CA.L2-3.12.4<br>  ○ If appropriately documented, do not assess against other CMMC practices<br>  ○ If contractor's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited spot check to identify risks<br>  ○ The limited spot check(s) shall not materially increase the assessment duration nor the assessment cost<br>  ○ The limited spot check(s) will be within the defined assessment scope |
| **Specialized Assets** | • Assets that may or may not process, store, or transmit CUI<br>• Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment | | • Review the SSP in accordance with practice CA.L2-3.12.4<br>• Do not assess against other CMMC practices |
| *Assets that are not in the CMMC Assessment Scope* | | | |
| **Out-of-Scope Assets** | • Assets that cannot process, store, or transmit CUI | • Assets are required to be physically or logically separated from CUI assets | • None |

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

The contractor is required to document all asset categories that are part of the assessment scope in an asset inventory and provide a network diagram of the 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 applicable CMMC practices.

In addition, the contractor is required to:

- document these assets in asset inventory;
- document these assets in the SSP; and
- provide a network diagram of the 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 contractor's CMMC Assessment Scope. Identifying Security Protection Assets is a critical part of scoping a CMMC engagement.

Security Protection Assets are part of the assessment scope and are required to conform to applicable CMMC practices, regardless of their physical or logical placement. 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 does contribute to meeting the CMMC practice requirements. 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<br>• Managed service provider personnel who perform system maintenance<br>• Enterprise network administrators |
| **Technology** | • Cloud-based security solutions<br>• Hosted Virtual Private Network (VPN) services<br>• SIEM solutions |
| **Facility** | • Co-located data centers<br>• Security Operations Centers (SOCs)<br>• Contractor office buildings |

In addition, the contractor is required to:

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

## Contractor Risk Managed Assets

Contractor Risk Managed Assets are capable of, but are not intended to, process, store, or transmit 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 CMMC Assessment Scope. These assets are managed using the contractor's risk-based information security policy, procedures, and practices and are not assessed against CMMC practices.

At a minimum, the contractor is required to:

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

An assessor may review the documentation of policy and procedures to ensure these assets do not process, store, or transmit CUI. Contractor Risk Managed Assets are reviewed in the SSP in accordance with CMMC practice CA.L2-3.12.4, but are not assessed against other CMMC practices.

If contractor's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited spot check to identify risks. The limited spot check(s) shall not materially increase the assessment

duration nor the assessment cost. The limited spot check(s) will be within the defined Assessment Scope.

## Specialized Assets

The following are considered specialized assets for a CMMC Level 2 assessment when properly documented.

- **Government Property** is all property owned or leased by the government. Government property includes both government-furnished and contractor-acquired property. Government property includes material, equipment, special tooling, special test equipment, and real property. Government property does not include intellectual property or software [Reference: Federal Acquisition Regulation (FAR) 52.245-1].
- **IoT or Industrial Internet of Things (IIoT)** 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 [Reference: iot.ieee.org/definition; National Institute of Standards and Technology (NIST) 800-183].
- **OT**[1] is used in manufacturing systems, industrial control systems (ICS), or supervisory control and data acquisition (SCADA) systems. OT may include programmable logic controllers (PLCs), computerized numerical control (CNC) devices, machine controllers, fabricators, assemblers, and machining.
- **Restricted Information Systems** can include systems [and associated Information Technology (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).
- **Test Equipment** 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. The contractor must document these assets in the SSP and detail how they are managed using the contractor's risk-based information security policy, procedures, and practices.

At a minimum, the contractor is required to:

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

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

A Certified Assessor will review the SSP to verify that specialized assets are managed using the contractor's risk-based information security policy, procedures, and practices and accounted for within the contractor's Assessment Scope.

### Out-of-Scope Assets

Out-of-Scope Assets cannot process, store, or transmit CUI because they are physically or logically separated (as detailed in the Separation Techniques section below) from CUI assets or are inherently unable to do so.

Out-of-Scope Assets are outside of the CMMC Assessment Scope and should not be part of the CMMC assessment engagement. These assets are out of scope when evaluating their conformity with applicable CMMC practices. There are no documentation requirements for Out-of-Scope Assets.

Out-of-Scope Assets do not provide security protections to CUI assets.

## Defining the CMMC Assessment Scope

After categorizing their assets, the contractor then specifies the CMMC Assessment Scope.

The CMMC Assessment Scope includes all assets in the contractor's environment that will be assessed in accordance with Table 1. Organizations will be required to provide documentation to the Certified Assessor that specifies the 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
- Contractor Risk Managed Assets
- Specialized Assets

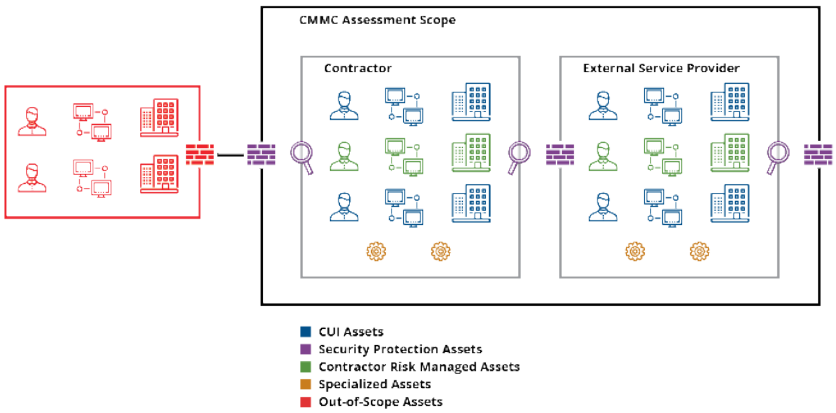


**Figure 1. CMMC Assessment Scope**

## 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 an asset is physically (wired or wirelessly) connected to another asset or set of assets, but software configuration prevents data from flowing along the physical connection path. Examples of mechanisms that provide controlled logical access include:

- firewalls; and
- Virtual Local Area Networks (VLANs).

**Physical separation** occurs when an asset is not physically (wired or wirelessly) connected to another asset or set of assets. Data may be transferred manually using human control (e.g., a USB drive). Examples of mechanisms that provide controlled physical access include:

- gates;
- locks;
- badge access; and
- guards.

## Use Cases

The following use cases demonstrate two scenarios in which one or more assessment scopes are specified.

### FCI and CUI Within the Same CMMC Assessment Scope

If the contractor processes, stores, or transmits Federal Contract Information (FCI) and CUI within the same assessment scope, the contractor can obtain a single certification. Because the contractor processes, stores, or transmits CUI, CMMC Level 2 is the minimum certification level needed. To achieve this:

- The contractor defines the CMMC Assessment Scope to only those assets that process, store, or transmit FCI and CUI, or provides security protections for such assets.

The assessor certifies that the contractor has implemented the CMMC Level 1 and 2 practices to the assets within that CMMC Assessment Scope.

### FCI and CUI Within Different CMMC Assessment Scopes

If the contractor processes, stores, or transmits FCI within one assessment scope, but processes, stores, and transmits CUI within another assessment scope, the contractor may choose to conduct two separate CMMC activities. In this scenario, the contractor may want to perform a CMMC Level 1 self-assessment for the boundary containing FCI (e.g., the enterprise network), but obtain a CMMC Level 2 certification for the boundary or enclave of its network within which all CUI must be processed, stored, or transmitted. To achieve this:

- The contractor defines a CMMC Self-Assessment Scope for only those assets that process, store, or transmit FCI. The contractor performs a self-assessment of CMMC Level 1 practices applied to the assets within that CMMC Self-Assessment Scope. The *CMMC Self-Assessment Scope – Level 1* document provides information on specifying the CMMC Self-Assessment Scope.
- The contractor specifies a CMMC Assessment Scope for only those assets that process, store, or transmit CUI. The Certified Assessor certifies that the contractor has implemented the CMMC Level 1 and 2 practices to the assets within that CMMC Assessment Scope.

## External Service Provider Considerations

An ESP can be within the scope of applicable CMMC practices if it meets CUI asset criteria. Special considerations for a contractor 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 contractor's responsibility. In some instances, cloud service providers might expose configuration settings and parameters that the consumer can use to meet CMMC practice objectives.
- Consider the standards that the ESP conforms to and/or what accreditations it has (e.g., FedRAMP, SOC 2, and CMMC Certification).
- Consider the agreements in place with the ESP, such as service-level agreements, memoranda of understanding, and contracts that support the contractor's information security objectives.


OFFICE OF THE UNDER SECRETARY OF DEFENSE
ACQUISITION AND SUSTAINMENT
CYBERSECURITY MATURITY MODEL
CERTIFICATION