CMMC Scoping Guide

Level 1

Version 2.13 | September 2024

DoD-CIO-00005 (ZRIN 0790-ZA21)

24-T-2769

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 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 1 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 2 self-assessment or certification assessment can be found in the *CMMC Scoping Guide – Level 2* 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 1 self-assessment and the professionals or companies that will support them in those efforts.

Identifying the CMMC Assessment Scope

Level 1 Assessment Scope

Prior to a Level 1 self-assessment the OSA must specify the CMMC Assessment Scope. The CMMC Assessment Scope defines which assets within the OSA's environment will be assessed and the details of the self-assessment. There are no documentation requirements for Level 1 self-assessments including In-Scope, Out-of-Scope, and Specialized Assets.

In-Scope Assets

Assets in scope for a Level 1 self-assessment, as defined in 32 CFR § 170.19(b), are all assets that process, store, or transmit Federal Contract Information (FCI).

- **Process** – FCI is used by an asset (e.g., accessed, entered, edited, generated, manipulated, or printed).
- **Store** – FCI 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** – FCI is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods).

These assets are part of the CMMC Assessment Scope and are assessed against all Level 1 requirements.

Out-of-Scope Assets

Assets out of scope for a Level 1 self-assessment, as defined in 32 CFR § 170.19(b)(2), are those that do not process, store, or transmit FCI. These assets are outside of the CMMC Assessment Scope and are not part of the assessment.

Specialized Assets

Specialized Assets, as defined in 32 CFR § 170.19(b)(2)(ii), are those assets that can process, store, or transmit FCI 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. Specialized Assets are not part of the Level 1 self-assessment scope and are not assessed against CMMC requirements. The following assets, defined in 32 CFR § 170.4, are considered specialized assets for a Level 1 self-assessment.

- **Government Furnished Equipment** (GFE) has the same meaning as "government-furnished property" as defined in 48 CFR § 45.101. Government-furnished property means property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a

deliverable under a cost contract when accepted by the Government for continued use under the contract.

- **Internet of Things (IoT) or Industrial Internet of Things (IIoT)** is defined is NIST SP 800-172A. These 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].
- **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: NIST SP 800-160v2 Rev 1] NOTE: Operational Technology (OT) specifically includes Supervisory Control and Data Acquisition (SCADA); this is a rapidly evolving field. [Source: NIST SP 800-82r3]
- **Restricted Information Systems** means systems [and associated Information Technology (IT) components comprising the system] that are configured based entirely 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.

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

Additional Guidance on Level 1 Scoping

In accordance with 32 CFR § 170.19(b)(3), to appropriately scope a Level 1 self-assessment, the OSA should consider the people, technology, facilities, and external service providers within its environment that process, store, or transmit FCI.

- **People** – May include, but are not limited to, employees, contractors, vendors, and external service provider personnel.
- **Technology** – May include, but are not limited to, servers, client computers, mobile devices, network appliances (e.g., firewalls, switches, APs, and routers), VoIP devices, applications, virtual machines, and database systems.
- **Facilities** – May include, but are not limited to, physical office locations, satellite offices, server rooms, datacenters, manufacturing plants, and secured rooms.
- **External Service Provider (ESP)** – as defined in 32 CFR § 170.4, means external people, technology, or facilities that an OSA utilizes for provision and management of comprehensive IT and/or cybersecurity services on behalf of the OSA.

In accordance with 32 CFR § 170.19(b)(1), assets that process, store, or transmit FCI and which are not Specialized Assets are in the CMMC Assessment Scope. Using the asset types approach allows an OSA to determine how they will satisfy the Level 1 requirements. FCI is a broad category of information; therefore, the self-assessment may need to address a wide array of assets.

For example, identifying the people within the OSA who process, store, or transmit FCI, will assist with fulfillment of the assessment of the following Level 1 security requirement:

- *IA.L1-b.1.v – Identify information system users, processes acting on behalf of users, or devices.*

As another example, identification of all technologies may inform assessment of the following Level 1 security requirements:

- *AC.L1-b.1.iii – Verify and control/limit connections to and use of external information systems.*
- *SC.L1-b.1.x – Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.*

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[2] do not require a new assessment, but rather are covered by the annual affirmations to the continuing compliance with requirements.

[2] It is recommended that an OSA develop a SSP as a best practice at Level 1. However, it is not required in order to conduct a Level 1 self-assessment.

This page intentionally left blank.


DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
CYBERSECURITY MATURITY MODEL
CERTIFICATION