CMMC Self-Assessment Scope

Level 1

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 Self-Assessment Scope

Level 1 Self-Assessment Scope

Prior to a Level 1 Cybersecurity Maturity Model Certification (CMMC) Self-Assessment, the contractor must specify the CMMC Self-Assessment Scope. The CMMC Self-Assessment Scope informs which assets within the contractor's environment will be assessed and the details of the self-assessment.

FCI Assets

Federal Contract Information (FCI) Assets process, store, or transmit FCI as follows:

- **Process** – FCI can be 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).

FCI Assets are part of the CMMC Self-Assessment Scope and are assessed against applicable CMMC practices.

Out-of-Scope Assets

Out-of-Scope Assets do not process, store, or transmit FCI. Out-of-Scope Assets are outside of the CMMC Self-Assessment Scope and should not be part of the CMMC self-assessment. These assets are out of scope when evaluating their conformity with applicable CMMC practices. There are no documentation requirements for Out-of-Scope Assets. Specialized assets, as discussed in the next section, are out of scope for a Level 1 Self-Assessment.

Specialized Assets

The following are considered specialized assets for a CMMC Level 1 self-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].
- **Internet of Things (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].

- **Operational Technology (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 IT components comprising the system) that are configured based entirely 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 not part of the Level 1 CMMC Self-Assessment Scope and are not assessed against CMMC practices.

Additional Guidance on Level 1 Scoping Activities

To appropriately scope a CMMC Level 1 self-assessment, the contractor should consider the people, technology, facilities, and external service providers within their environment that process, store, or transmit FCI.

- **People** – Employees, contractors, vendors, and external service provider personnel
- **Technology** – Servers, client computers, mobile devices, network appliances (e.g., firewalls, switches, APs, and routers), VoIP devices, applications, virtual machines, and database systems
- **Facilities** – Physical office locations, satellite offices, server rooms, datacenters, manufacturing plants, and secured rooms
- **External Service Provider (ESP) –** External people, technology, or facilities that the organization uses, including cloud services, co-located data centers, hosting providers, and managed security service providers.

Assets that process, store, or transmit FCI are considered in the self-assessment scope. Using the asset types approach allows a contractor to determine and iterate on how they will satisfy the CMMC Level 1 practices. Because FCI is a broad category of information, the contractor will likely focus the self-assessment on their entire environment.

For example, identifying the people within the contractor's organization that process, store, or transmit FCI, informs how that contractor performs the following practice:

- *IA.L1-3.5.1 – Identify information system users, processes acting on behalf of users, or devices.*

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

Another example is when the contractor considers all of its technology and external service providers, it will allow them to convey how they satisfy the following practices:

- *AC.L1-3.1.20 – Verify and control/limit connections to and use of external information systems.*
- *SC.L1-3.13.1 – 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.*


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