Defense Industrial Base (DIB) Sector Coordinating Council (SCC) Supply Chain Cyber Training

Cyber/Cybersecurity Maturity Model Certification (CMMC) v2.0

CyberAssist

Agenda

- Module 1: Cybersecurity: Why it is Important?
- Module 2: Cybersecurity Maturity Model Certification
- Module 3: Incident Reporting
- Module 4: Cybersecurity Best Practices
- Resource Guide: Glossary, Acronym Guide and Resources for Additional Information
- CMMC Domains
- Survey

Cybersecurity Maturity Model Certification (CMMC)

Level 1

Module 2

Disclaimer and Overview

Note: CMMC is still going through the rule-making process and certain aspects and requirements may change. Refer to the *Resources Guide* provided in this training for the most updated information.

- The intent of this training is to build awareness for Defense Industrial Base (DIB) suppliers of the likely requirements of the Cybersecurity Maturity Model Certification (CMMC) and their obligation to meet FAR 52.204-21 (basic cyber hygiene) and DFARS 252.204-7012 (specialized data handling and protection requirements).
- This training is self-paced and intended for a range of roles and responsibilities including, but not limited to, executives, project managers and technical staff from organizations seeking certification (OSC) and need to comply with CMMC. Currently, CMMC does not apply to any contractor.
- Note: Completion of this training DOES NOT certify your organization. This training is intended for the purposes of providing awareness of the subjects outlined above.
- The DIB Sector Coordinating Council (SCC) Supply Chain Task Force does not take responsibility for suppliers' certification by the CMMC 3rd Party Assessment Organization (C3PAO).
- This training focuses on U.S. regulations and industry best practices:
  - U.S. Department of Defense (DoD) Chief Information Officer (CIO) Cybersecurity Maturity Model Certification (CMMC) Information
  - National Institute of Standards & Technologies (NIST) publications
  - National Archives & Records Administration (NARA) definitions
  - DIB SCC Supply Chain Task Force – CyberAssist website

Module Topics and Objectives

Helpful Hint:
Refer to the Resource Guide for a Glossary and Acronym Guide

Topics covered in this module:

- Cybersecurity Maturity Model Certification (CMMC)
- Protecting U.S. Government Information: FCI and CUI
- CMMC Domains, CMMC Enumeration/Numbering Defined and Self-Assessment process
- How to Prepare for CMMC

The objectives of this module are:

- Provide understanding of the CMMC model;
- Provide understanding of FCI and CUI;
- Provide understanding of the self-assessment process; and
- Provide guidance on how to prepare for CMMC.

A legend has been provided to assist with determining the content that you will need to know for each of the CMMC levels and what is additional content that will assist your organization with your cybersecurity posture. The corresponding symbol will be located at the top left corner of the slide.

Content Legend

CyberAssist

Cybersecurity Maturity Model Certification (CMMC)

CMMC was created by the DoD in response to rising malicious cyber activity impacting Department of Defense (DoD) systems and data.

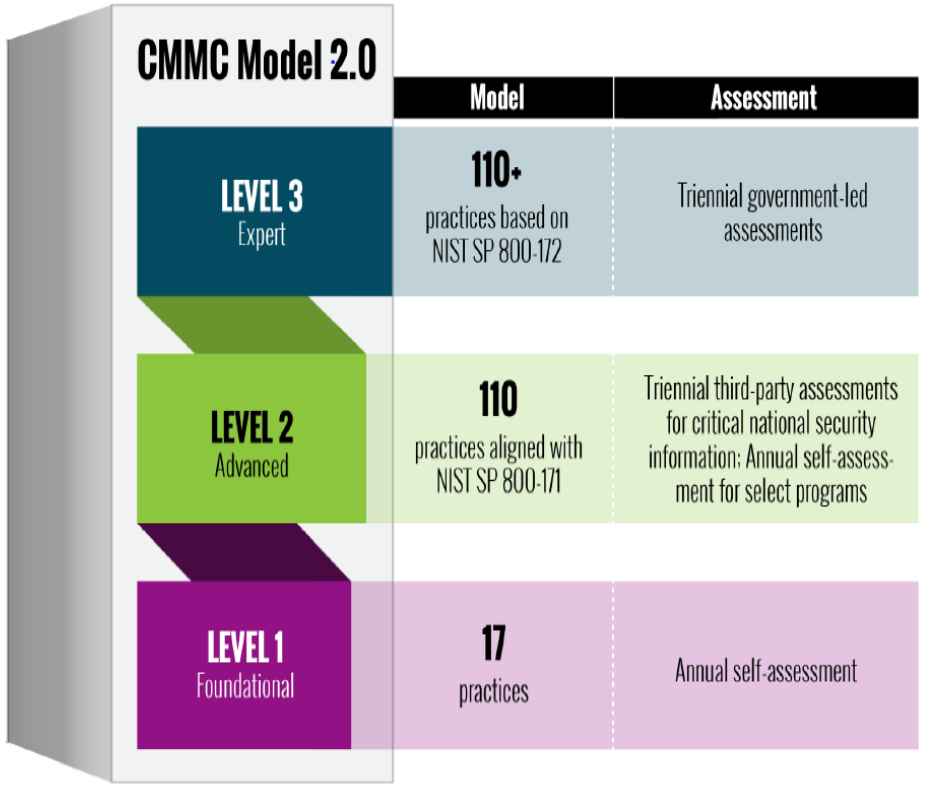


Figure 1. CMMC 2.0 Level Overview

- CMMC measures the implementation of cybersecurity requirements at three levels.
- CMMC Model 2.0 combines various cybersecurity standards and best practices and is built on NIST 800-171 and a sub-set of NIST 800-172.

Source: Cybersecurity Maturity Model Certification Model Overview Version 2.0 | December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf

Protecting U.S. Government Information: FCI

What is FCI?

- **FCI** is any U.S. Government information that is “not intended for public release” that is provided by or generated for the U.S. Government

Key Regulation?

- FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems

Key Documents?

- None, 15 FAR controls map to 17 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 controls
- CMMC Self-Assessment Guide - Level 1

Protecting U.S. Government Information: CUI

What is CUI?

- **CUI** is Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. Source: E.O. 13556 (adapted)

Key Regulation?

- DFARS 252.204-7012: Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting

Key Documents?

- NIST SP 800-171 and NIST SP 800-171A
- NIST SP 800-172 and NIST SP 800-172A (CMMC Level 3)
- CMMC Assessment Guide - Level 2
- For more information on the CUI categories, refer to the CUI Registry, http://www.archives.gov/cui/registry/category-list.html

Note: This clause does not apply to contractors where it has been determined that CUI is not managed in the contractor's environment

The CMMC Model

Domains, Practices and Self-Assessment Process

CMMC Domains

CMMC Domains (14)

Access Control (AC)	Audit and Accountability (AU)	Awareness and Training (AT)	Configuration Management (CM)	Identification and Authentication (IA)
Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)
Risk Assessment (RA)	Security Assessment (CA)	System and Communications Protections (SC)	System and Information Integrity (SI)	

Legend:
Green cells: Includes CMMC L1 practices
Gray cells: Includes CMMC L2 or higher practices

Note: The 6 CMMC domains highlighted in green are discussed in the following slides. For more information on the remaining 8 CMMC domains, refer to the *Supporting Material section* at the end of the training.

Access Control (AC)

Access control is the process of granting or denying requests to use information, to use information processing services and/or enter company facilities. System-based access controls are called logical access controls, who or what (in the case of a process) is permitted to have access to a system resource and type of access permitted.*

- ❑ Do you securely log into your company systems?
- ❑ Does your company limit system access to types of transactions and functions?
- ❑ Does your company restrict access to company facilities?
- ❑ What is sensitive information?
- ❑ Do you know how to handle and protect sensitive information?

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

Identification and Authentication (IA)

Identification and authentication is a technical measure that prevents unauthorized individuals or processes from entering a system. Identification and authentication is a critical building block of information security since it is the basis for most types of access control and for establishing user accountability.*

- ❑ How do users log into your systems?
- ❑ Does everyone have full administrative rights on all systems?
- ❑ Do you use any type of multifactor authentication (MFA)?
- ❑ Do you have any password requirements setup?
- ❑ Do you have a process for removing user accounts when an individual leaves the company?

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

Media Protection (MP)

Media protection is a requirement that addresses the defense of system media, which can be described as both digital and nondigital. Media protections can restrict access and make media available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media so that the information cannot be retrieved or reconstructed.*

- ❑ Do you sanitize systems before sending for disposal?
- ❑ Do you protect backups at off-site facilities?
- ❑ Do you protect your systems from removable media especially when coming from an unknown source?

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

Physical Protection (PE)

The term physical (and environmental) security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.*

- ❑ Do you track and monitor visitors?
- ❑ Is physical access to systems limited?
- ❑ Do you take security measures when working offsite?

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

System and Communications Protection (SC)

System and communications protection requirements provide an array of safeguards for the system, including the confidentiality information at rest and in transit. System and communications protection also establishes boundaries that restrict access to publicly accessible information within a system. Using boundary protections, a company can monitor and control communications at external boundaries as well as key internal boundaries within the system.*

- ❑ Do you have firewalls and other segregation on your network?
- ❑ Do you segregate public-facing systems from internal only systems?
- ❑ Do you use encryption when transmitting over the Internet?
- ❑ Do you limit the ability to connect to systems from outside the company?

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

System and Information Integrity (SI)

System and information integrity provides assurance that the information being accessed has not been meddled with or damaged by an error in the system.*

- ❑ Do you use Anti-malware/Anti-virus software and keep it updated?
- ❑ Do you monitor for system vulnerabilities and/or malicious attacks?

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

CMMC Enumeration/Numbering Defined

Each practice is specified using the convention of **DD.L#-REQ** where:

- **DD** is the two-letter domain abbreviation;
- **L#** is the level number; and
- **REQ** is the NIST SP 800-171 Rev 2 or NIST SP 800-172 security requirement number.

Example of the breakdown of a CMMC practice:

Description: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Source: Cybersecurity Maturity Model Certification Model Overview Version 2.0 | December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf

Identify Self-Assessment Scope

- Prior to conducting self-assessment, the scope needs to be identified, CMMC Self-Assessment Scope – Level 1 Guide
- FCI Assets are part of the CMMC Self Assessment Scope and are assessed against applicable CMMC practices.
  - **Process** - FCI can be used by an asset
  - **Store** - FCI is inactive or at rest
  - **Transmit** - FCI is being transferred from one asset to another asset
- Consider people, technology, facilities and external service provider (ESP) within the environment that process, store and transmit FCI

Source: Cybersecurity Maturity Model Certification Model Overview Version 2.0 | December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level1_V2.0_FINAL_20211202_508.pdf

Self-Assessment Observation Activities

- Self-Assessors should become intimately familiar with the CMMC Self-Assessment Guide Level 1, and the Assessment Objectives associated with each practice
- Each practice will require the use of at least two assessment methods to validate assessment objectives to identify objective evidence.
  - **Assessment Objectives** identify the specific list of objectives that must be satisfied to receive a rating of MET for the practice or process, which means your company has completed the objectives for that practice or process
  - **Assessment Methods** define the nature and the extent of the assessor's actions –
    - Examine (Artifact)
    - Interview (Observation/Affirmation)
    - Test (Demonstrate)
  - **Assessment Objects** identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals
- Self-assessment of CMMC practice results in one of three possible findings:
  - MET
  - NOT MET
  - NOT APPLICABLE
- All Level 1 practices will need a finding of MET or NOT APPLICABLE, to demonstrate CMMC Level 1 compliance

Source: Cybersecurity Maturity Model Certification Model Overview Version 2.0 | December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_FinalDraft_20211210_508.pdf

Practice and Self-Assessment Objectives Example

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

Source: Cybersecurity Maturity Model Certification Model Overview Version 2.0 | December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_FinalDraft_20211210_508.pdf

Potential Self-Assessment Methods and Objects for Practice Example

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

Potential Objects

Interview

[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

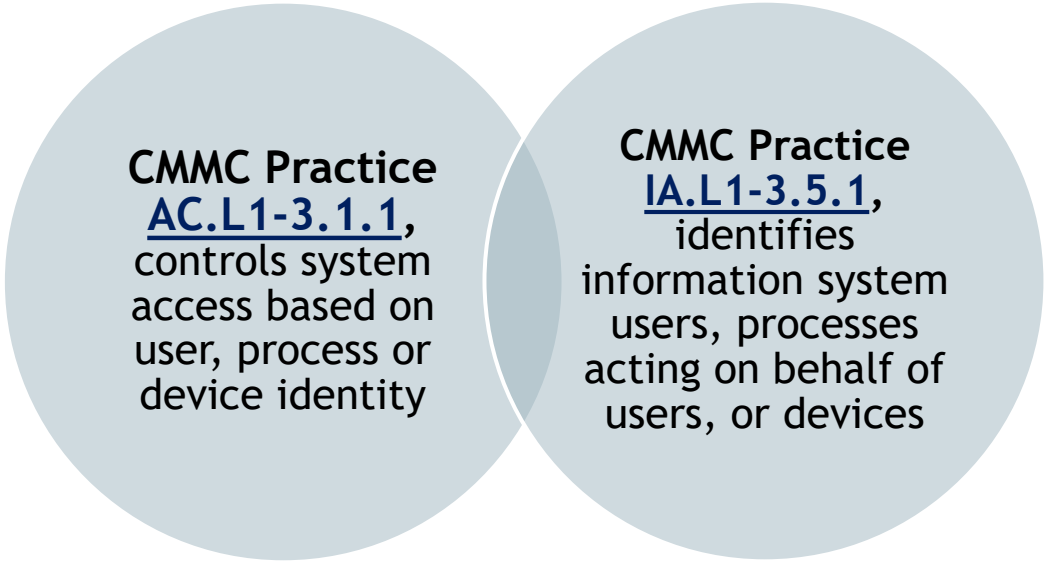
Test

[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

Source: Cybersecurity Maturity Model Certification Model Overview Version 2.0 | December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_FinalDraft_20211210_508.pdf

CMMC Practice Interconnectivity

The practices in CMMC are interconnected and work together to help provide good cyber hygiene. For example:



AC.L1-3.1.1 leverages IA.L1-3.5.1 which provides a vetted and trusted identity for access control required by AC.L1-3.1.1.

How to Prepare for CMMC Level 1

Recommendations prior to contract award:

- Understand contract requirements: FAR 52.204-21, FCI and other applicable clauses and standards (Module 2)
- Be aware of contractual reporting requirements (Module 3)
- Keep performing cybersecurity best practices (Module 4)
- Perform your self-assessment: CMMC Self-Assessment Level 1 Guide and CMMC Level 1 practices (Module 2)
- Submit self-assessment per DoD guidance TBD
- Understand subcontractor compliance requirements and keep up to date with regulatory changes

Recommendations for after contract award:

- Keep self-assessment score up to date (annually)
- Monitor any changes to your environment
- Follow and maintain reporting requirements
- Be aware of flow down requirements for subcontractors

Module Summary

- Understanding current and future regulatory requirements is imperative as a DoD supplier
- Specialized information types, such as FCI and CUI, must be handled and protected according to applicable requirements
- Understanding the CMMC model:
  - Breaking down parts of the model for further understanding
  - Providing steps to prepare for CMMC
- For questions on the content, please send them to Contact Us - DIB SCC CyberAssist.

Next: Module 3 - Incident Reporting