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: Assessment Process - Interim
- Module 4: Incident Reporting
- Module 5: Cybersecurity Best Practices
- Module 6: Risk Management
- Resource Guide: Glossary, Acronym Guide and Resources for Additional Information
- CMMC Domains
- Survey

Cybersecurity Maturity Model Certification (CMMC)

Module 2

CyberAssist

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: Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)
- CMMC Domains

The objectives of this module are:

- Provide understanding of FCI and CUI; and
- Provide understanding of the CMMC model.

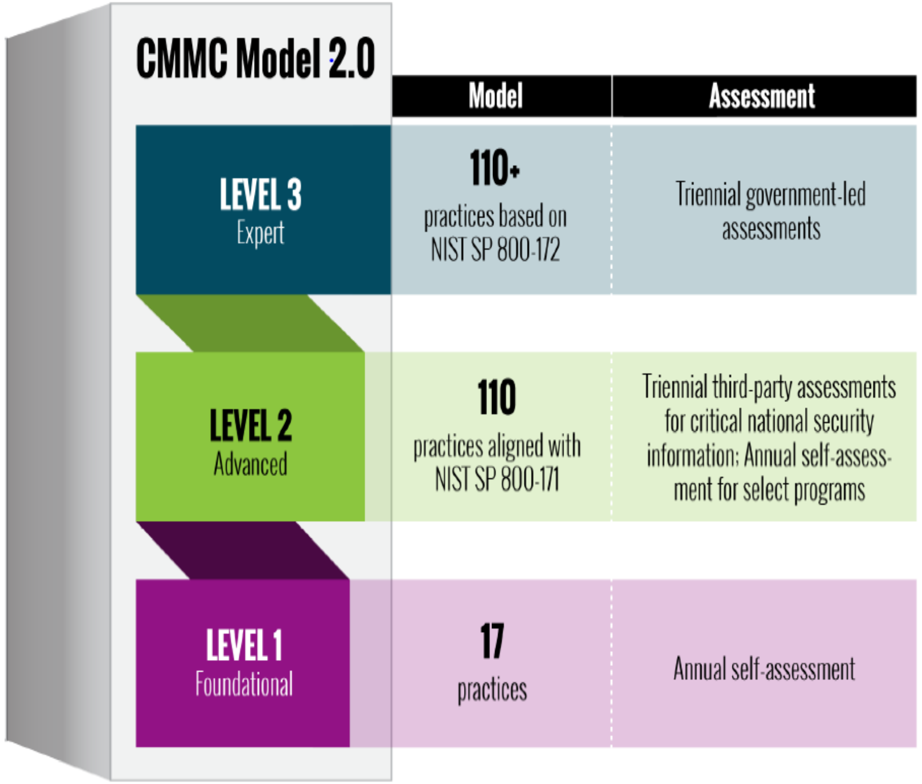
A legend has been provided to assist with determining the content that you will need to know for each of the CMMC levels and what is additional content that will assist your organization with your cybersecurity posture. The corresponding symbol will be located at the top left corner of the slide.

Content Legend

★ = CMMC L1 Content
◆ = CMMC L2 Content
⬬ = CMMC L3 Content
✚ = Non-CMMC Content/Extra

Cybersecurity Maturity Model Certification (CMMC)

CMMC was created by the DoD in response to rising malicious cyber activity impacting DoD systems and data.



CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

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 under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments. (FAR 52.204-21)

Key Regulation?

- FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems requires the basic safeguarding requirements and procedures to protect covered contractor information systems.

Definition: "Covered contractor information system" means an information system that is owned or operated by a contractor that processes, stores, or transmits FCI.

Key Documents?

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

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 requires contractors who handle CDI on non-federal systems in performance of contracts to implement adequate cybersecurity safeguarding controls (NIST SP 800-171), rapidly report cyber incidents to the federal government within 72 hours of discovery, and to flow these requirements to their subcontractors who receive or generate CDI on their internal system.

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

Protecting U.S. Government Information: CUI (cont’d)

DFARS 252.204-7012 invokes the NIST Special Publication 800-171 standard also known as “**Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.**”

- In total, 800-171 has 110 unique security requirements that are split among 14 broader sections, or “families.”
- Considering the volume and specificity of these requirements, any organization performing under contracts (or subcontracts) with the Defense Department must make sure that they have the requisite information security knowledge, expertise and resources to comply with NIST SP 800-171. Non-compliance, after all, could spell the end of a contractor’s relationship with the DoD.
- Department of Defense Controlled Unclassified Information (DoD CUI) previously known as Covered Defense Information (CDI) is one example of CUI. In explaining what steps must be taken to protect CUI, the NIST guidelines cover the protection of DoD CUI or CDI as mandated by the DFARS clause 252.204-7012

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

Protecting U.S. Government Information: CUI (cont’d)

Key Documents?

- NIST SP 800-171 and NIST SP 800-171A
- CMMC Level 2 Scoping Guide
- CMMC Level 2 Assessment Guide
- For more information on the CUI categories, refer to the CUI Registry (NARA), http://www.archives.gov/cui/registry/category-list.html; (DoD), https://www.dodcui.mil/Home/DoD-CUI-Registry/

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

The CMMC Model

Domains, Practices and Assessment Process

CyberAssist

CMMC Domains

- The CMMC model consists of 14 domains that align with the families specified in NIST SP 800-171.*
- When you click on one of the domains in the “CMMC Domains (14)” chart, you will be directed to the listing of all practices for that domain. From there, you can narrow it down by level.

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)	

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

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

Audit and Accountability (AU)

Companies should create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity and ensure that the actions of users can be uniquely traced to those users so they can be held accountable.*

- ❑ Are users uniquely identified in your systems?
- ❑ Do you perform any type of event reviews?
- ❑ Do you have any alerts setup when a failure occurs?

*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

Awareness and Training (AT)

The purpose of information security awareness, training, and education is to enhance security by raising awareness of the need to protect system resources, developing skills and knowledge so system users can perform their jobs more securely, and building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems.*

- ❑ Do you have any training on job duties or protection of information?
- ❑ Is the training recurring?

*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

Configuration Management (CM)

Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the System Development Life Cycle (SDLC).*

- ❑ Do you have any baseline configurations (software, hardware, etc.)?
- ❑ Do you setup any specific security settings?
- ❑ Do you review changes to your systems before they occur?
- ❑ Do you limit what software can be installed and run on your systems?

*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

Incident Response (IR)

Companies should establish an operational incident handling capability for company systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities and track, document, and report incidents to company management and/or authorities.*

- ❑ Do you have any processes for responding to any type of event that affects your business?
- ❑ Do you test this process?

*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

Maintenance (MA)

Companies should perform periodic and timely maintenance on company systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.*

- ❑ Do you patch your systems regularly?
- ❑ Do you sanitize systems before sending for repair?
- ❑ Do you monitor repair personnel?

*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

Personnel Security (PS)

Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to company assets through the malicious use or exploitation of their legitimate access to the company's resources. Companies should be vigilant when recruiting and hiring new employees, as well as when an employee transfers or is terminated.*

- ❑ Do you perform background checks on employees?
- ❑ Do you remove/disable access when an employee 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

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

Risk Assessment (RA)

Risk assessments identify and prioritize risks to company operations, assets, employees, and other organizations that may result from the operation of a system. Companies should periodically assess the risk to operations (e.g., mission, functions, image, and reputation), assets, and employees, which may result from the operation of company systems and the associated processing, storage, or transmission of company information.*

- ❑ Do you assess risk to your company and systems?
- ❑ Do you scan for and remediate systems vulnerabilities?
- ❑ Do you perform backups of systems?

*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

Security Assessment (CA)

A security requirement assessment is the testing and/or evaluation of the management, operational, and technical security requirements on a system to determine the extent to which the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*

❑ Do you periodically assess your security controls?

❑ Do you resolve any deficiencies found in security controls?

❑ Do you document how your systems are protected and interconnected?

*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?

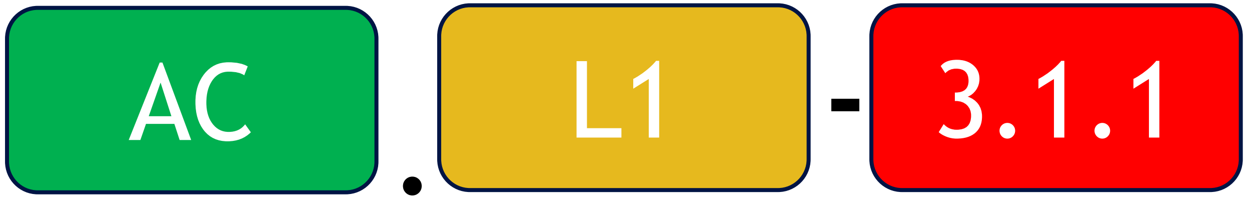
*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

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:



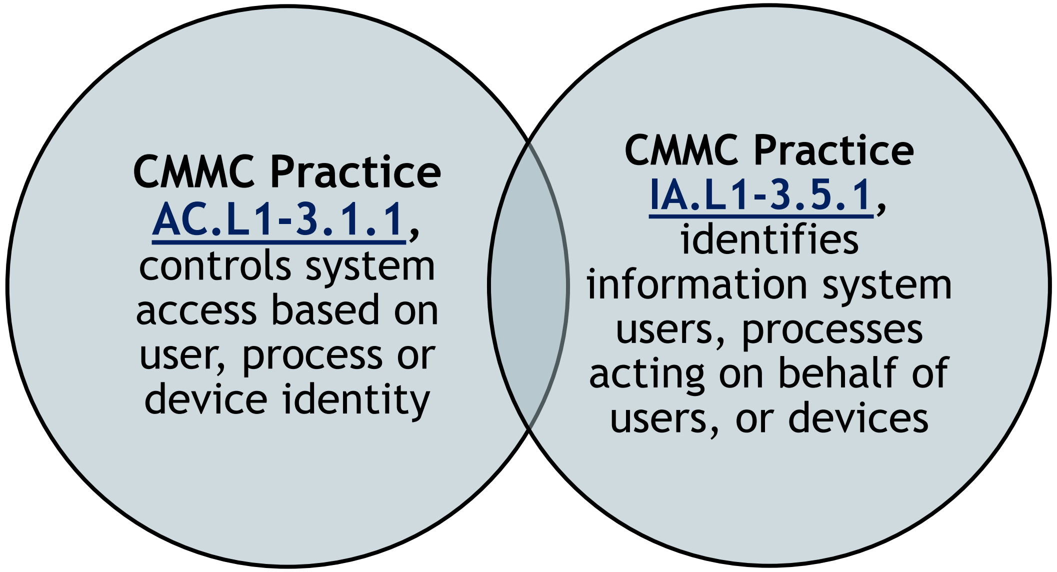
AC . L1 - 3.1.1

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

CMMC Practice Interconnectivity

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



CMMC Practice AC.L1-3.1.1, controls system access based on user, process or device identity

CMMC Practice IA.L1-3.5.1, identifies information system users, processes acting on behalf of users, or devices

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.

Module Summary

- Key Things to Remember:
  - Understand contract requirements and ensure compliancy with applicable regulations, e.g., FAR 52.204-21 and DFARS 252.204-7012.
  - CMMC is still going through the rule-making process and certain aspects and requirements may change.
  - Keep up to date on any changes by referencing any of the *Resources* outlined in this training.
- 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 DIB SCC Cyber Training.

Next: Module 3 – Assessment Process - Interim

CyberAssist