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

Assessment Process

Module 3

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:

- CMMC Assessment Level Identification
- Anticipated CMMC Level 2 Assessment Process
- Pre-Regulation Assessment - Joint Surveillance
- Identify Assessment Scope
- Practice and Assessment Objective Review
- CMMC Certification Process
- How to Prepare for CMMC Level 2

The objectives of this module are:

- Provide understanding of the CMMC Level 2 assessment process;
- Provide understanding of the CMMC certification process; and
- Provide understanding of how to prepare for CMMC Level 2.

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

CyberAssist

Acronyms & Definitions

Acronym	Full Name	Definition
C3PAO	CMMC Third Party Assessment Organization	An Entity that is certified to be contracted to and OSC to provide consultative advice OR certified assessments.
CAICO	CMMC Assessors and Instructors Certification Organization	The CAICO is the dedicated CMMC entity facilitating the training, examination, and professional certification for individuals within the CMMC Ecosystem. The CAICO is a wholly owned subsidiary of the CMMC Accreditation Body, Inc. and operates as a nonprofit organization with federal tax-exempt status.
CAP	CMMC Assessment Process	Provides procedures and guidance for CMMC C3PAOs conducting official CMMC Assessments of organizations seeking CMMC certification.
CCA	Certified CMMC Assessor	A person who has successfully completed all certification program requirements as outlined by the CAICO for becoming a Level 2 CMMC Assessor. A Provisional Assessor (PA) will become a CCP and then a CCA by passing the associated certification exam(s).
CCP	Certified CMMC Professional	A person who has successfully completed all certification program requirements as outlined by the CAICO for becoming a Level 1 CMMC Assessor.
CMMC	Cybersecurity Maturity Model Certification	Set of standards established by the DoD against which an OSC is to be assessed.

Source: https://cyberab.org/CMMC-Ecosystem/Terminology

Acronyms & Definitions (cont'd)

Acronym	Full Name	Definition
CUI	Controlled Unclassified Information	Information that requires safeguarding or dissemination control pursuant to and consistent with laws, 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 Atomic Energy Act of 1954, as amended. Source: NIST SP800-171 Rev 2
The Cyber AB	The Cyber Accreditation Body (formerly CMMC Accreditation Body)	The Cyber AB is the official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) Ecosystem and the sole authorized non-governmental partner of the U.S. Department of Defense in implementing and overseeing the CMMC conformance regime.
DCMA	Defense Contract Management Agency	Agency that provides contract administration services for the Department of Defense, other federal organizations and international partners, and is an essential part of the acquisition process from pre-award to sustainment. (DCMA.mil)
DFARS	Defense Federal Acquisition Regulation Supplement	The DFARS provides DoD implementation and supplementation of the Federal Acquisition Regulation (FAR). The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public. (osd.mil)

Source: https://cyberab.org/CMMC-Ecosystem/Terminology

Acronyms & Definitions (cont'd)

Acronym	Full Name	Definition
DIBCAC	Defense Industrial Base Cyber Assessment Center	Leads the Department of Defense's (DoD) contractor cybersecurity risk mitigation efforts. DIBCAC assesses DoD contractors' compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 as well as, the DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements. (DCMA.mil)
FAR	Federal Acquisition Regulation	The Federal Acquisition Regulations System is established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies. (acquisition.gov)
FCI	Federal Contract Information	Federal contract information means information, not intended for public release, that is provided by or generated for the 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 Web sites) or simple transactional information, such as necessary to process payments. Source: 48 CFR § 52.204-21
OSC	Organization Seeking Certification	The Organization that is going through the CMMC assessment process to receive a level of Certification for a given environment.

Source: https://cyberab.org/CMMC-Ecosystem/Terminology

Acronyms & Definitions (cont'd)

Acronym	Full Name	Definition
POAM/POA&M	Plan(s) of Action and Milestones	A document that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones. (nist.gov)
RP	Registered Practitioner	Professionals who provide CMMC implementation consultative services.
RPO	Registered Provider Organization	An organization authorized to represent itself as familiar with the basic constructs of the CMMC Standard, with a CMMC-AB provided logo, to deliver non-certified CMMC Consulting Services. Signifies that the organization has agreed to the CMMC-AB Code of Professional Conduct.
SPRS	Supplier Performance Risk System	The authoritative source to retrieve supplier and product PI (performance information) assessments for the DoD acquisition community to use in identifying, assessing, and monitoring unclassified performance." (DoDI 5000.79)

Source: https://cyberab.org/CMMC-Ecosystem/Terminology

Assessment Level Identification

- When CMMC "goes live," organizations will need to determine the appropriate assessment path and level, given the type of information they have access to or develop
  - **Federal Contract Information (FCI) only**
    - Self-assessment of CMMC Level 1 (L1) practices using the CMMC Self-Assessment Guide - Level 1 for additional guidance
  - **Controlled Unclassified Information (CUI) identified as Non-critical to national security ***
    - Self-assessment of CMMC L2 practices using the CMMC L2 Assessment Guide
  - **CUI identified as Critical to national security ***
    - Requires certification by an authorized C3PAO from the Cyber AB Marketplace
  - **CUI identified as requiring enhanced protections***
    - Requires CMMC L3 certification by DCMA DIBCAC*

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

Anticipated CMMC L2 Assessment Process

- Pre-assessment
  - Identify assessment boundary at OSC
  - Self-assess CMMC L2 and remediate any findings or gaps
    - Optional: Hire RPO to perform assessment and recommend remediations
- Once all practices are sufficiently and adequately documented and performed
  - Identify authorized C3PAO through the Cyber AB Marketplace
  - Contract with C3PAO
  - Identify assets and scoping boundary to be assessed
  - Schedule and perform assessment by C3PAO
- Post assessment
  - Receive assessment results
    - No gaps, receive CMMC L2 Certification
    - Gaps found, remediate and request reassessment
  - Keep documentation and boundary scope assets updated to meet CMMC L2 practices during 3-year certification period

Pre-Regulation Assessment – Joint Surveillance

- Prior to release of updated regulation, the DoD is recommending companies volunteer for the Joint Surveillance program
- The Joint Surveillance program pairs an OSC-selected authorized C3PAO with DCMA DIBCAC for the OSC's assessment
  - Acceptance into Joint Surveillance program will be scheduled based on DCMA availability and prioritization
- C3PAO leads the assessment with oversight by DCMA DIBCAC
- Upon completion, OSC receives updated DIBCAC High score in SPRS

Joint Surveillance Program – C3PAO/DCMA DIBCAC Assessment

Step 1: OSC identifies Assessment Scope Boundaries

Step 2: OSC contracts with an authorized C3PAO from the Cyber AB Marketplace

Step 3: C3PAO coordinates with DCMA DIBCAC and Cyber AB to identify possible scheduling dates

Step 4: Once dates and assessment scope are agreed upon by all parties

- OSC gathers artifacts and securely shares with C3PAO and DIBCAC
- C3PAO and DIBCAC perform readiness review of provided artifacts (virtual)
- Once virtual review is complete, the OSC, C3PAO and DIBCAC will perform on-site assessment(s) at one or more previously agreed upon locations of the OSC
  - OSC's primary business location will typically be the meeting site
  - Secondary sites may include data center(s) and/or manufacturing site(s) but must be agreed upon and scheduled by all parties

Step 5: After the assessment

1. DCMA DIBCAC/C3PAO will upload the OSC scores to SPRS
2. SPRS score is valid for 3 years; however, senior leadership certification is required yearly
3. OSC may need to work POAMs and perform re-evaluation at a future date

Identify Assessment Scope

- Prior to conducting assessment, the scope needs to be identified, CMMC Assessment Scope Level 2
- Assets that are included in the CMMC Assessment Scope and are assessed against CMMC practices:
  - **CUI Assets -**assets that process, store and transmit CUI
  - **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
- Assets that are part of the Assessment Scope but not CMMC Practices and MUST show that these assets are managed using the contractor's risk-based security policies, procedures and practices
  - **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
  - **Specialized Assets** – Assets that may or may not process, store, or transmit CUI, e.g., government property, Internet of Things (IoT) devices

Source: CMMC Assessment Guide – Level 2, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf

Identify Assessment Scope (cont'd)

- Assets that are Out-of-Scope of the Assessment
  - Out-of-Scope Assets – Assets that cannot process, store, or transmit CUI and are physically or logically separated.
- For all assets, the contractor is required to:
  - Document these assets in asset inventory;
  - Document these assets in System Security Plan (SSP); and
  - Provide a network diagram of the assessment scope (to include these assets) to facilitate scoping discussions during the pre-assessment.
- Identifying Security Protection Assets is a critical part of scoping a CMMC engagement. (People, technology, facilities)

Source: CMMC Assessment Guide – Level 2, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf

Practice and Assessment Objective Review

- Organizations should become familiar with the CMMC Assessment Guide Level 2, and the Assessment Objectives associated with each practice
- Each practice and associated assessment objectives will likely necessitate the use of at least two of the three assessment methods (examine, interview, test) to validate the adequacy (the right evidence) and sufficiency (enough of the right evidence) of each practice and associated assessment objectives.
  - **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

Source: CMMC Assessment Guide – Level 2, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf

Practice and Assessment Objective Review (cont'd)

- **Assessment <u>Methods</u>** define the nature and the extent of the assessor's actions –
  - Examine (Artifact)
  - Interview (Observation/Affirmation)
  - Test (Demonstrate)
- **Assessment <u>Objects</u>** identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals

- Assessment of CMMC practice results in one of three possible findings:
  - MET
  - NOT MET
  - NOT APPLICABLE
- All Level 2 practices will need a finding of MET or NOT APPLICABLE, to demonstrate CMMC Level 2 compliance

Source: CMMC Assessment Guide – Level 2, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf

Practice and 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).

Look for Key Words to determine what is needed to be done or gathered

Source: CMMC Assessment Guide – Level 2, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf

Potential 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: CMMC Assessment Guide – Level 2, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf

CMMC Certification Process

- Cyber AB, https://cyberab.org/
- The Cyber AB Marketplace is the **ONLY** authorized resource to assist in training, RPO, and C3PAO services
- The Cyber AB will provide information and set requirements for prospective CMMC C3PAOs and individual assessors.

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

How to Prepare for CMMC Level 2

Recommendations prior to contract award:

- Understand contract requirements: FAR 52.204-21, CMMC requirements, CUI and other applicable clauses and standards, and CMMC requirements (Module 2)
- Be aware of contractual reporting requirements (Module 4)
- Identify possible data types and locations, access, and security
- Keep following cybersecurity best practices (Module 5)
- Perform your self-assessment
- Update SPRS self-assessment yearly
- Engage C3PAO for certification (for critical national security systems)
- 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)
- Keep certification up to date
- Monitor any changes to your environment
- Follow and maintain reporting requirements
- Be aware of flow down requirements for subcontractors, e.g., limit data flow down to only what is needed

Module Summary

- Understanding the CMMC assessment process:
  - Identifying the assessment scope
  - Understanding the four phases of the CMMC assessment process
- For questions on the content, please send them to DIB SCC Cyber Training.

Next: Module 4 – Incident Reporting