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

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

CyberAssist

Agenda

- Section 1: Cybersecurity: Why it is Important?
- Section 2: Cybersecurity Maturity Model Certification
- Section 3: CMMC Assessment Process
- Section 4: Incident Reporting
- Section 5: Cybersecurity Best Practices
- Section 6: Risk Management and Assessing Risk
- Resource Guide: Glossary, Acronym Guide and Resources for Additional Information
- Survey

Cybersecurity: Why is it Important?

Section 1

Disclaimer and Overview

- The intent of this training is to build awareness for Defense Industrial Base (DIB) suppliers of the Cybersecurity Maturity Model Certification (CMMC) requirements 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.
- 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. Refer to the *Resources Guide* provided in this training for the most updated information.
- 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

Section Topics and Objectives

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

Topics covered in this section:

- What is Cybersecurity?
- CIA Triad
- Why it is important?
- Are your IT environments protected? Is your information protected?
- Section Summary

The objectives of this section are:

- Provide understanding of the importance of cybersecurity;
- Provide understanding of the CIA Triad; and
- Provide understanding of who is at risk.

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

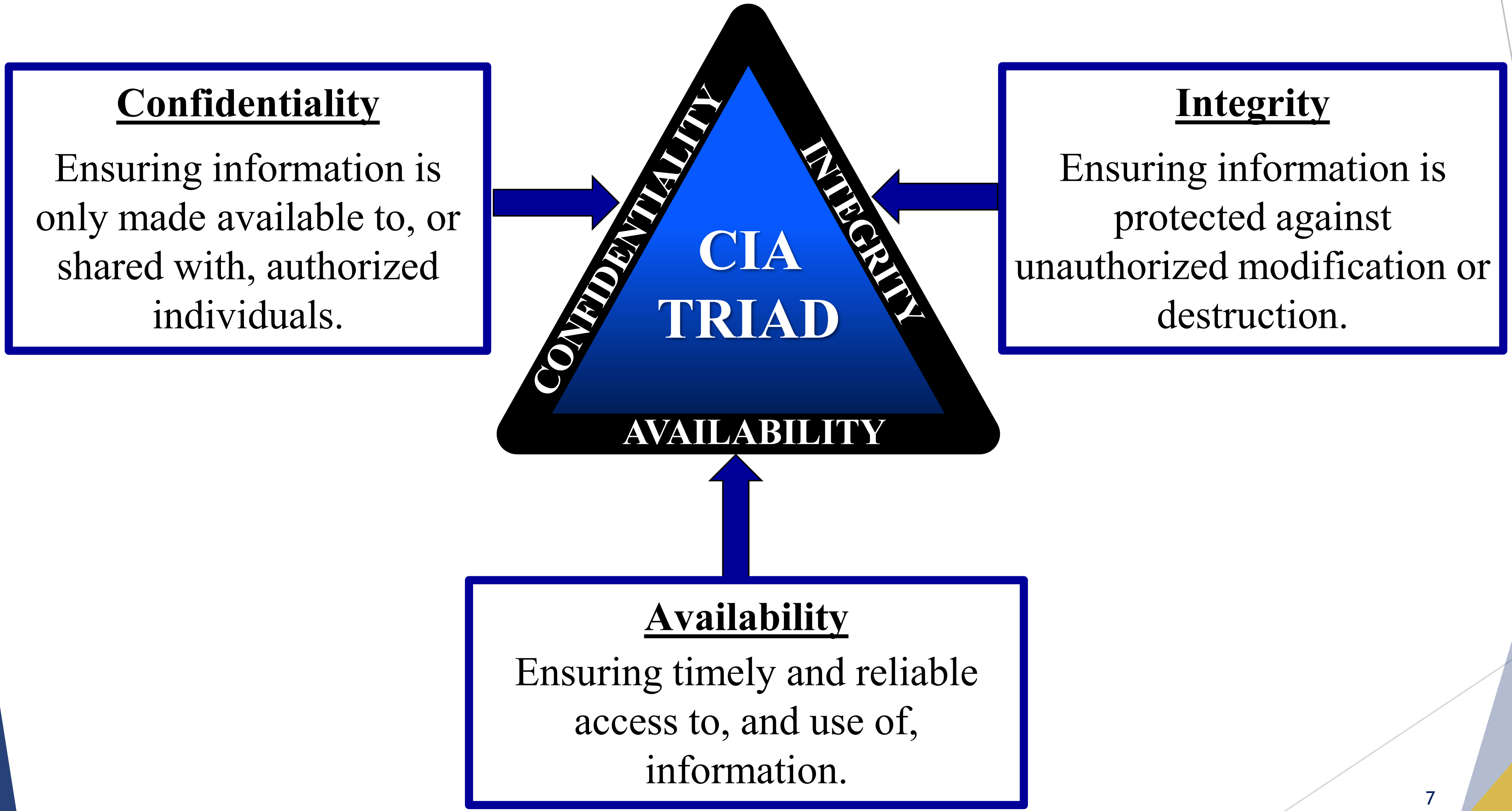
1 = CMMC L1 Content
2 = CMMC L2 Content
3 = CMMC L3 Content
A = CMMC All Levels Content
✚ = Non-CMMC Content/Extra

What is Cybersecurity?

- All the tools we use and actions we take to keep computers, networks, and information **safe and available** for those who need it, and unavailable for those who should not have it.
- That means **protecting** hardware, software, people, and data from everything from cyber attacks to earthquakes.

Cybersecurity is about keeping our information technology (IT) resources secure (confidential, available, and unaltered).

CIA Triad



Confidentiality

Ensuring information is only made available to, or shared with, authorized individuals.

Integrity

Ensuring information is protected against unauthorized modification or destruction.

Availability

Ensuring timely and reliable access to, and use of, information.

Why is it Important?

Evolving Threats

Increasing Potential Impact

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

Increasingly Unstable Threats

ADVANCED PERSISTENT THREATS (APT)

BROADBASED & CRIMINAL

INSIDER

HACKTIVISTS

ROGUE ACTORS

The Only Constant is Change

Cybersecurity attacks continue to increase in frequency and sophistication for the Aerospace and Defense industry

Are your IT environments protected?
Is your information secure?

As a DIB Partner, now is the time to understand your cybersecurity posture so that you can make sound, risk-based decisions about investing in cybersecurity protections.

- Identify and secure information through cybersecurity best practices.
- Understand and identify your risks and the types of cyber threats and vulnerabilities that affect your business.

By understanding the threats and vulnerabilities that affect your business, the business owners can make sound, risk-based decisions about investing in cybersecurity protection.

Section Summary

- Cybersecurity is about keeping our digital data, systems, and activities secure (confidential, available, and unaltered)
- Cybersecurity attacks continue to increase in frequency and sophistication for the Aerospace and Defense industry and supply chain
- Everyone is at risk when it comes to cyber attacks, but small businesses are more likely targets because of perceived limited resources to protect the business and its infrastructure
- For questions on the content, please send them to DIB SCC Cyber Training

Next: Section 2 - Cybersecurity Maturity Model Certification

Cybersecurity Maturity Model Certification (CMMC)

Section 2

Section Topics and Objectives

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

Topics covered in this section:

- Cybersecurity Maturity Model Certification (CMMC)
- Protecting U.S. Government Information: Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)
- CMMC Rulemaking, Ecosystem, & Standards Acceptance
- CMMC Domains

The objectives of this section 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.

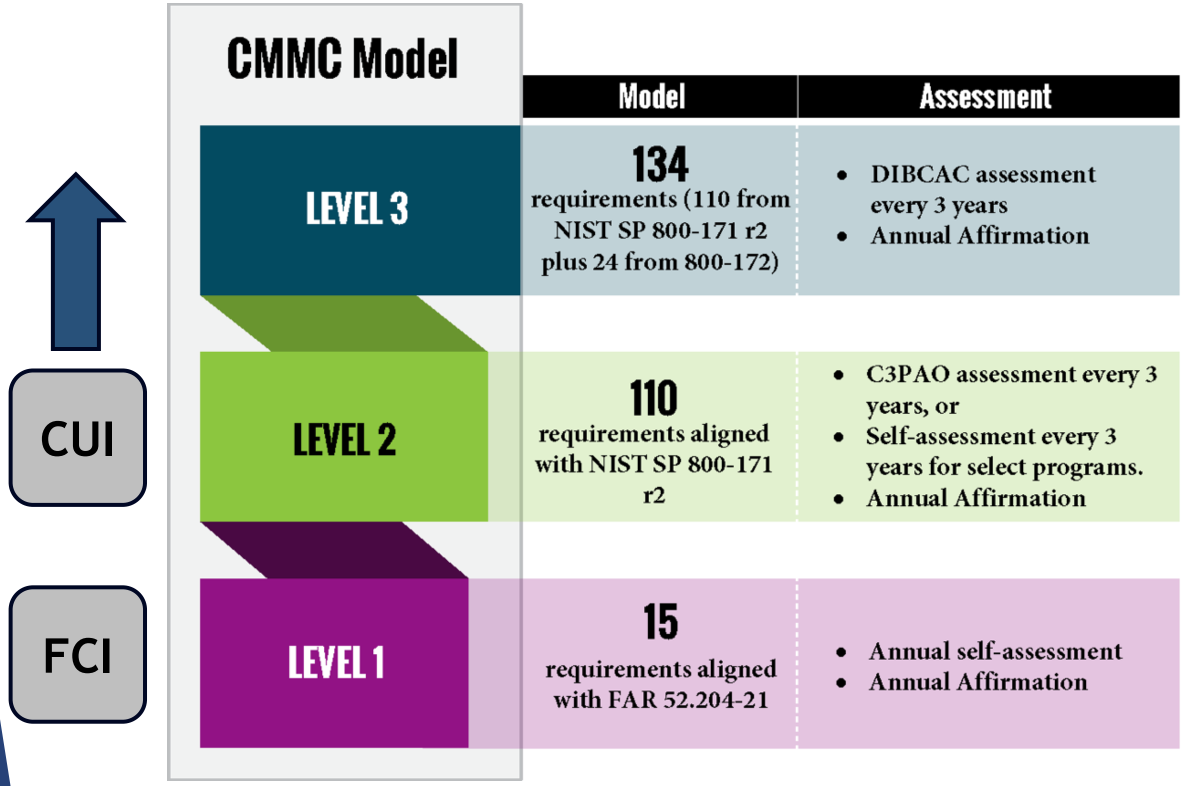
Content Legend

1 = CMMC L1 Content
2 = CMMC L2 Content
3 = CMMC L3 Content
A = CMMC All Levels Content
✚ = Non-CMMC Content/Extra

CyberAssist

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

	Model	Assessment
LEVEL 3	**134** requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	• DIBCAC assessment every 3 years • Annual Affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171 r2	• C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs. • Annual Affirmation
LEVEL 1	**15** requirements aligned with FAR 52.204-21	• Annual self-assessment • Annual Affirmation

FCI = Federal Contract Information
CUI = Controlled Unclassified Information

Available CMMC Status Levels:

- CMMC Final Level 1 (Self)
- CMMC Conditional Level 2 (Self)
- CMMC Final Level 2 (Self)
- CMMC Conditional Level 2 (C3PAO)
- CMMC Final Level 2 (C3PAO)
- CMMC Conditional Level 3 (DIBCAC)
- CMMC Final Level 3 (DIBCAC)

Source: Cybersecurity Maturity Model Certification Model Overview Version 2.13 | September 2024, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverviewv2.pdf

FCI and CUI

Definitions

1

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 contractors to implement 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

- 15 FAR controls map to 17 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 controls
- CMMC Resources and Documentation

2

3

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)

Note: This clause is not applicable to contractors when it has been determined that CUI is neither managed nor stored in the contractor's environment.

2

3

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

Key Regulations

- 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.
- The DoD has issued a class deviation to DFARS Clause 252.204-7012 to allow contracting officials to continue to assess against NIST SP 800-171 Rev 2 and allow for a deliberate transition to Rev 3.
- Rev 3 will be incorporated into CMMC through a future rulemaking. (CMMC FAQs Q16)

Note: This clause is not applicable to contractors when it has been determined that CUI is neither managed nor stored in the contractor's environment.

A

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

Key Regulations

- 32 CFR Part 170: “With this final rule, DoD establishes the Cybersecurity Maturity Model Certification (CMMC) Program in order to verify contractors have implemented required security measures necessary to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The mechanisms discussed in this rule will allow the Department to confirm a defense contractor or subcontractor has implemented the security requirements for a specified CMMC level and is maintaining that status (meaning level and assessment type) across the contract period of performance. This rule will be updated as needed, using the appropriate rulemaking process, to address evolving cybersecurity standards requirements, threats, and other relevant changes.” **Source:** 32 CFR Part 170, 10/15/2024, https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

Note: This clause is not applicable to contractors when it has been determined that FCI nor CUI is not processed, transmitted, nor stored in the contractor's environment.

A

Protecting U.S. Government Information: CUI/FCI (cont'd)

Key Regulations

- 48 CFR Parts 204, 212, 217, and 252: "DoD is issuing a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate contractual requirements related to the final Cybersecurity Maturity Model Certification program rule, titled Cybersecurity Maturity Model Certification Program. This final DFARS rule also partially implements a section of the National Defense Authorization Act for Fiscal Year 2020 that directed the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. defense industrial base.." **Source:** 48 CFR Parts 204, 212, 217, and 252, 09/10/2025, https://www.govinfo.gov/content/pkg/FR-2025-09-10/pdf/2025-17359.pdf

Note: This clause is not applicable to contractors when it has been determined that FCI nor CUI is not processed, transmitted, nor stored in the contractor's environment.

CMMC Contract Requirements

Government Contracting Officer

- Shall include CMMC Levels in solicitation except for COTS.
- Shall NOT award to offeror that does not have current CMMC status at required level
- Validate any new CMMC UIDs, as necessary

Prime Contractors

- Required to achieve, at time of award, CMMC status at level or higher of solicitation for all information systems, as defined by *CMMC UIDs, used that will process, transmit, or store FCI or CUI
- Maintain CMMC status at level or higher through the life of the award.
- Communicate any changes to CMMC UIDs to the Contracting Officer.
- Flow down the clause with level requirements based on FCI or CUI sharing

Subcontractors

- Obtain and maintain the CMMC status at level or higher for the life of the award.
- Provide CMMC UIDs to prime contractors.
- Flow down the clause with level requirements based on FCI or CUI sharing.

*Cybersecurity Maturity Model Certification Unique Identifier (CMMC UID) means a 10 alpha-numeric characters assigned to each CMMC assessment and reflected in the Supplier Performance Risk System (SPRS) for each contractor information system.

CMMC Contract Non-Compliance Risks

Risk Area	Potential Impact(s)
Contract Eligibility	Inability to bid or renew DoD contracts
Legal	FCA fines, whistleblower suits, treble damages
Financial	Lost revenue, higher insurance, breach costs
Regulatory	Fines from multiple agencies (e.g., DoD, SEC, FTC, etc.)
National Security	Criminal prosecution, debarment
Reputation	Loss of trust, negative media coverage

A

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

Key Documents

- NIST SP 800-171 Rev 2 and NIST SP 800-171A
- CMMC Resources and Documentation
- Class Deviation to DFARS Clause 252.204-7012
- 32 CFR Part 170
- 48 CFR Parts 204, 212, 217 and 252
- For more information on the CUI categories, refer to the following CUI Registries
  - (NARA), http://www.archives.gov/cui/registry/category-list.html
  - (DoD), https://www.dodcui.mil/Home/DoD-CUI-Registry/

CMMC Rulemaking

Overview

A

Cybersecurity Maturity Model Certification (CMMC)

DoD Policy Final

32 Code of Federal Regulations (CFR) 170

Authorizes the DoD to implement the CMMC program, framework and components

- DoD published the final rule in Oct 2024 with an effective date of Dec 2024

How - DoD Policy, Process, & Procedures for **CMMC Program**

*NOTE: COTS has specific exemptions if met per DoD guidelines.

What – Contracts/Subcontracts **CMMC Requirements** w/CUI

DoD Requirements

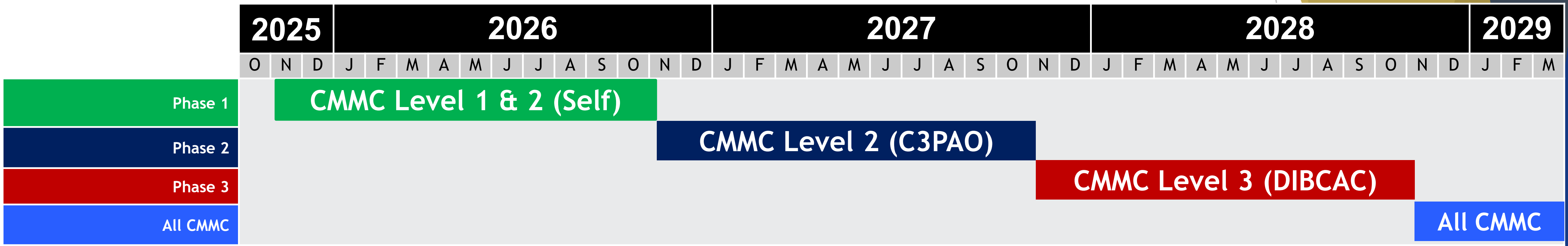
48 CFR DFARS 252.204-7021 & 7025

Establishes the requirements for incorporating CMMC into DoD contracts*

- DoD published the Final Rule in September 2025
- CMMC Phase 1 implementation of self-assessments to begin Nov 10, 2025

Source: Department of Defense CMMC Program| October 2024, https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

CMMC 2.0 Phased Approach



2025 | 2026 | 2027 | 2028 | 2029

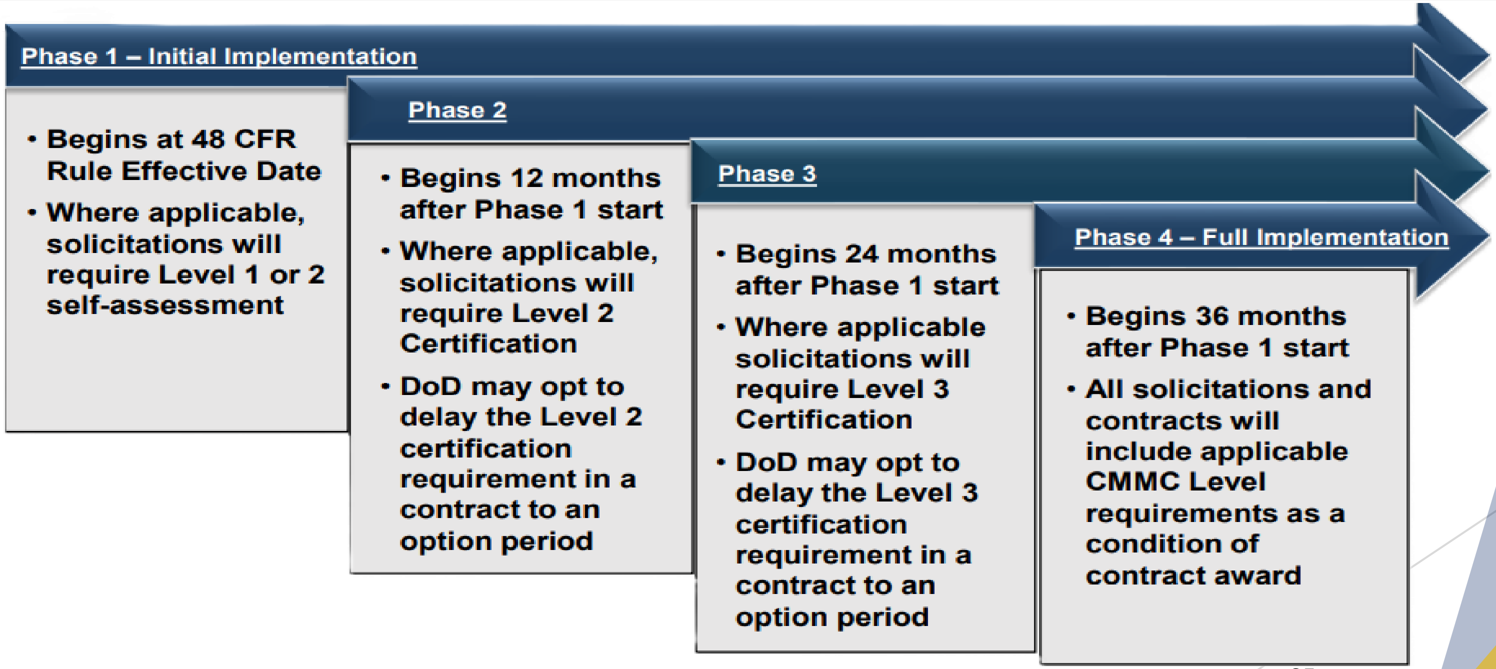
O N D | J F M A M J J A S O N D | J F M A M J J A S O N D | J F M A M J J A S O N D | J F M

Phase 1 — CMMC Level 1 & 2 (Self)

Phase 2 — CMMC Level 2 (C3PAO)

Phase 3 — CMMC Level 3 (DIBCAC)

All CMMC — All CMMC



Phase 1 – Initial Implementation

- Begins at 48 CFR Rule Effective Date
- Where applicable, solicitations will require Level 1 or 2 self-assessment

Phase 2

- Begins 12 months after Phase 1 start
- Where applicable, solicitations will require Level 2 Certification
- DoD may opt to delay the Level 2 certification requirement in a contract to an option period

Phase 3

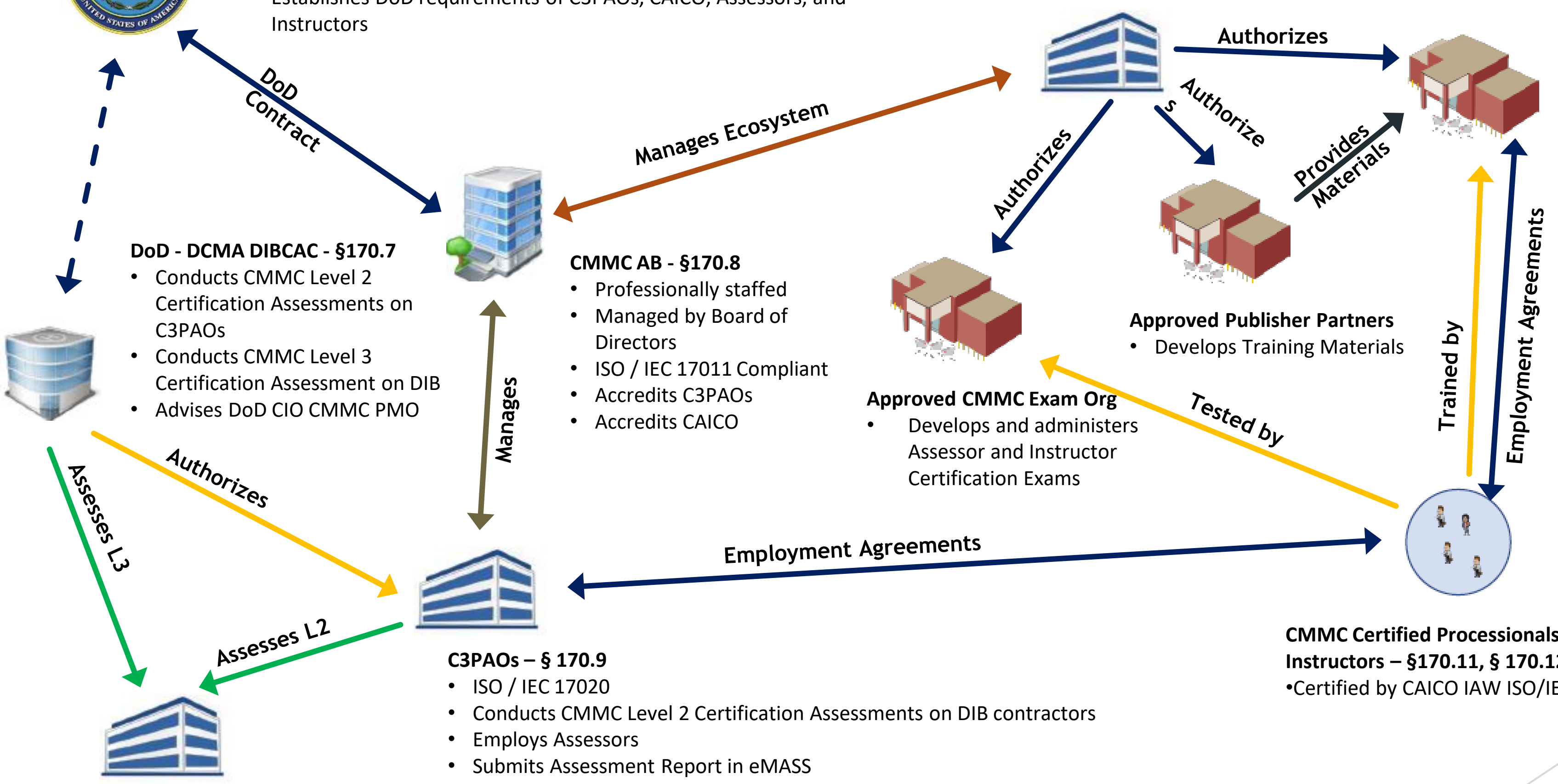
- Begins 24 months after Phase 1 start
- Where applicable solicitations will require Level 3 Certification
- DoD may opt to delay the Level 3 certification requirement in a contract to an option period

Phase 4 – Full Implementation

- Begins 36 months after Phase 1 start
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

DoD may implement CMMC Level 2 (C3PAO) requirements in Phase 1 procurements or Level 3 requirements in Phase 2 procurements, which may limit competitors or drive cost

CMMC Ecosystem



DoD – DoD CIO CMMC PMO - § 170.6

- Provides oversight of the CMMC Program, to include the CMMC AB
- Develops and maintains the CMMC Model Overview, Assessment Guides, Scoping Guides, and Hashing Guide
- Scheme Owner for ISO/IEC Requirements
- Establishes DoD requirements of C3PAOs, CAICO, Assessors, and Instructors

CMMC Assessor and Instructor Certification Organization - §170.10

- ISO/IEC 17024
- Certifies CMMC Certified Professionals, Assessors, and Instructors
- Defines knowledge areas required for CCPs, CCA,s and CCIs with input from DoD
- QCs curriculum developed by ecosystem

Approved Training Providers

- Trains Certified Professionals
- Trains Assessors
- Trains Instructors

DoD - DCMA DIBCAC - §170.7

- Conducts CMMC Level 2 Certification Assessments on C3PAOs
- Conducts CMMC Level 3 Certification Assessment on DIB
- Advises DoD CIO CMMC PMO

CMMC AB - §170.8

- Professionally staffed
- Managed by Board of Directors
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO

Approved Publisher Partners

- Develops Training Materials

Approved CMMC Exam Org

- Develops and administers Assessor and Instructor Certification Exams

CMMC Certified Processionals, Assessors & Instructors – §170.11, § 170.12 and 170.13

•Certified by CAICO IAW ISO/IEC 17020

C3PAOs – § 170.9

- ISO / IEC 17020
- Conducts CMMC Level 2 Certification Assessments on DIB contractors
- Employs Assessors
- Submits Assessment Report in eMASS
- Issues CMMC certificate to DIB contractor

Organization Seeking Certification

- Has contract for specific CMMC Level
- Identifies and coordinates with appropriate 3rd Party (C3PAO/DIBCAC)

*https://dodcio.defense.gov/Portals/0/Documents/CMMC/CMMC101.pdf

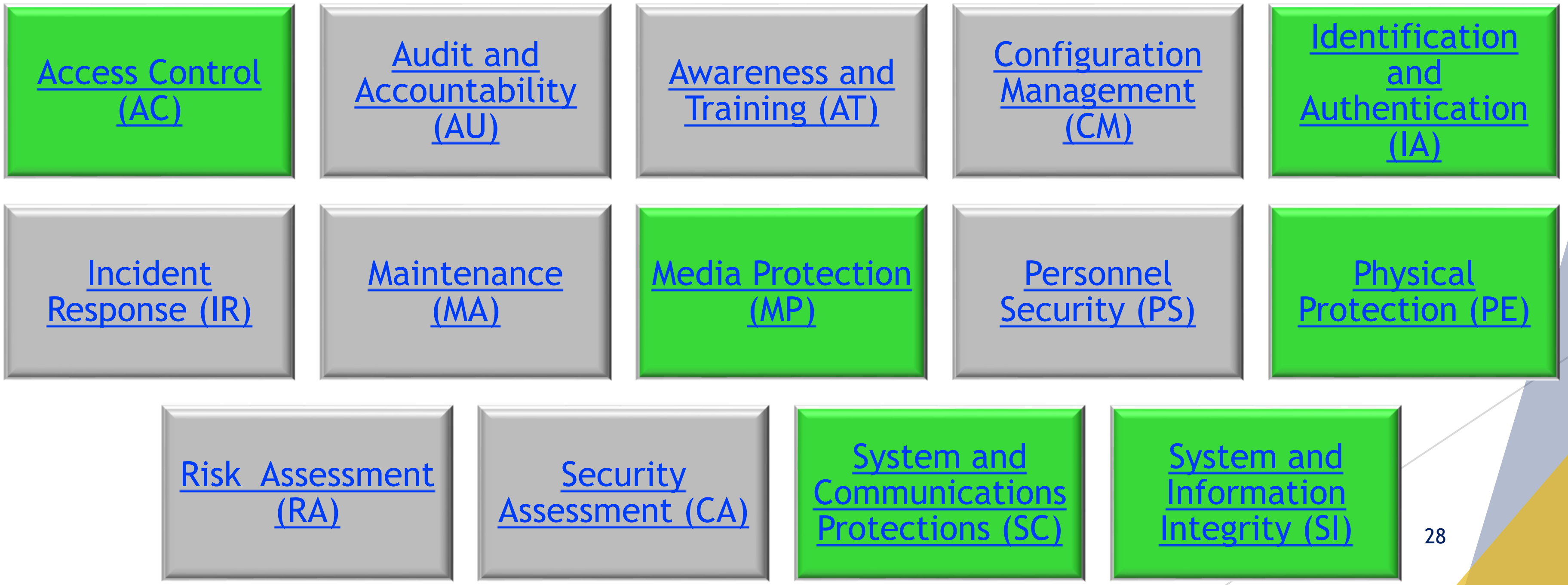
The CMMC Model

Domains and Requirements

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 security requirements for that domain. From there, you can narrow it down by level. Green cells include L1 security requirements. Green and gray cells include L2 or higher security requirements.

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 2.13 | September 2024, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview.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?

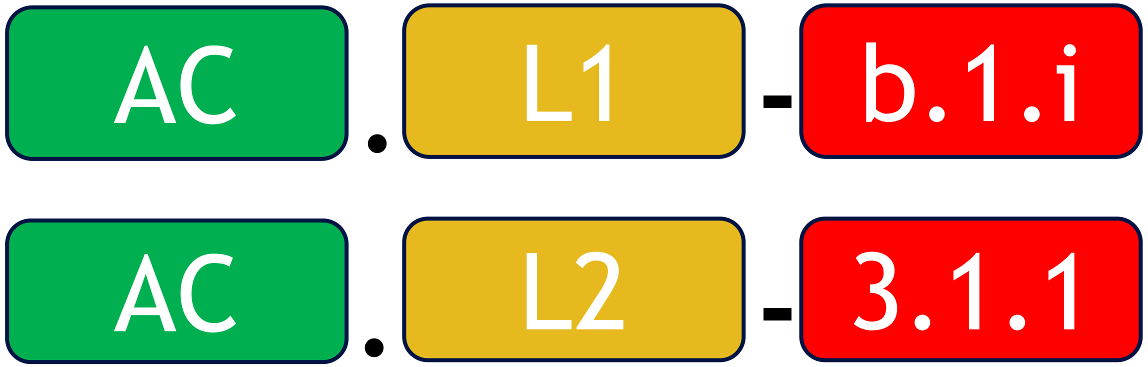
*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

CMMC Enumeration/Numbering Defined

Each requirement 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.

Examples of the breakdown of a CMMC security requirement:



AC.L1-b.1.i

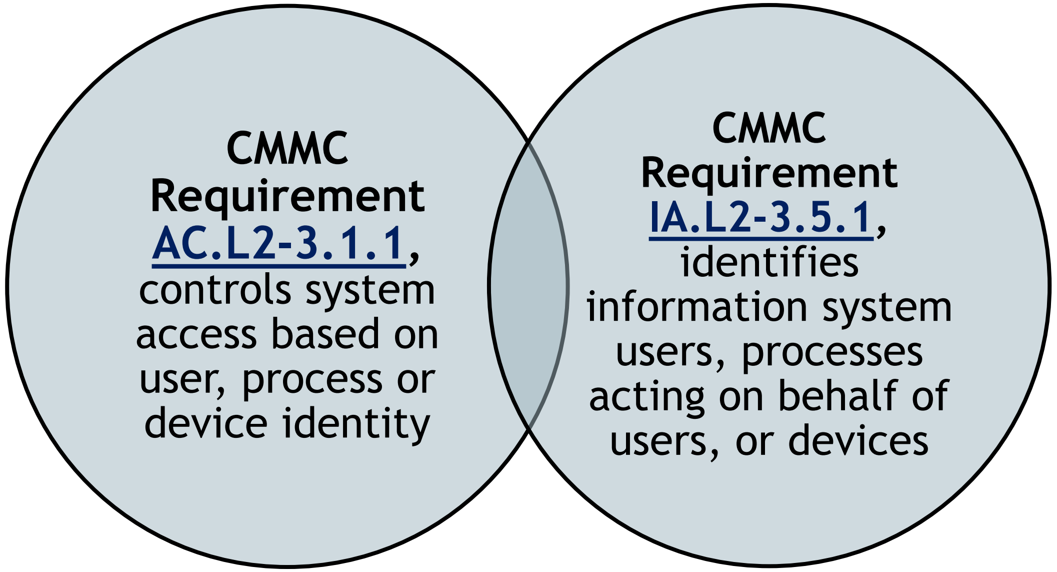
AC.L2-3.1.1

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 2.13 | September 2024, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview.pdf

CMMC Practice Interconnectivity

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



CMMC Requirement AC.L2-3.1.1, controls system access based on user, process or device identity

CMMC Requirement IA.L2-3.5.1, identifies information system users, processes acting on behalf of users, or devices

AC.L2-3.1.1 leverages IA.L2-3.5.1 which provides a vetted and trusted identity for access control required by AC.L2-3.1.1.

Section 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.
  - 32 CFR CMMC Program Final Rule was published Oct 2024 with Effective Date of Dec 2024.
  - CMMC DFARS Requirements (Contract Rules 252.204-7021 and 252.204-7025) were published Sept 9, 2025, with an Effective Date of Nov 10, 2025.
  - 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: Section 3 – Assessment Process

CMMC Assessment Process

Section 3

CyberAssist

Section Topics and Objectives

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

Topics covered in this section:

- General CMMC Assessment Process Flow
- Assessment Level Identification
- Identify Assessment Scope
- CMMC Assessment Asset Categories
- CMMC Assessment Activities
- CMMC L1, L2, and L3 Process Flows and requirements

The objectives of this section are:

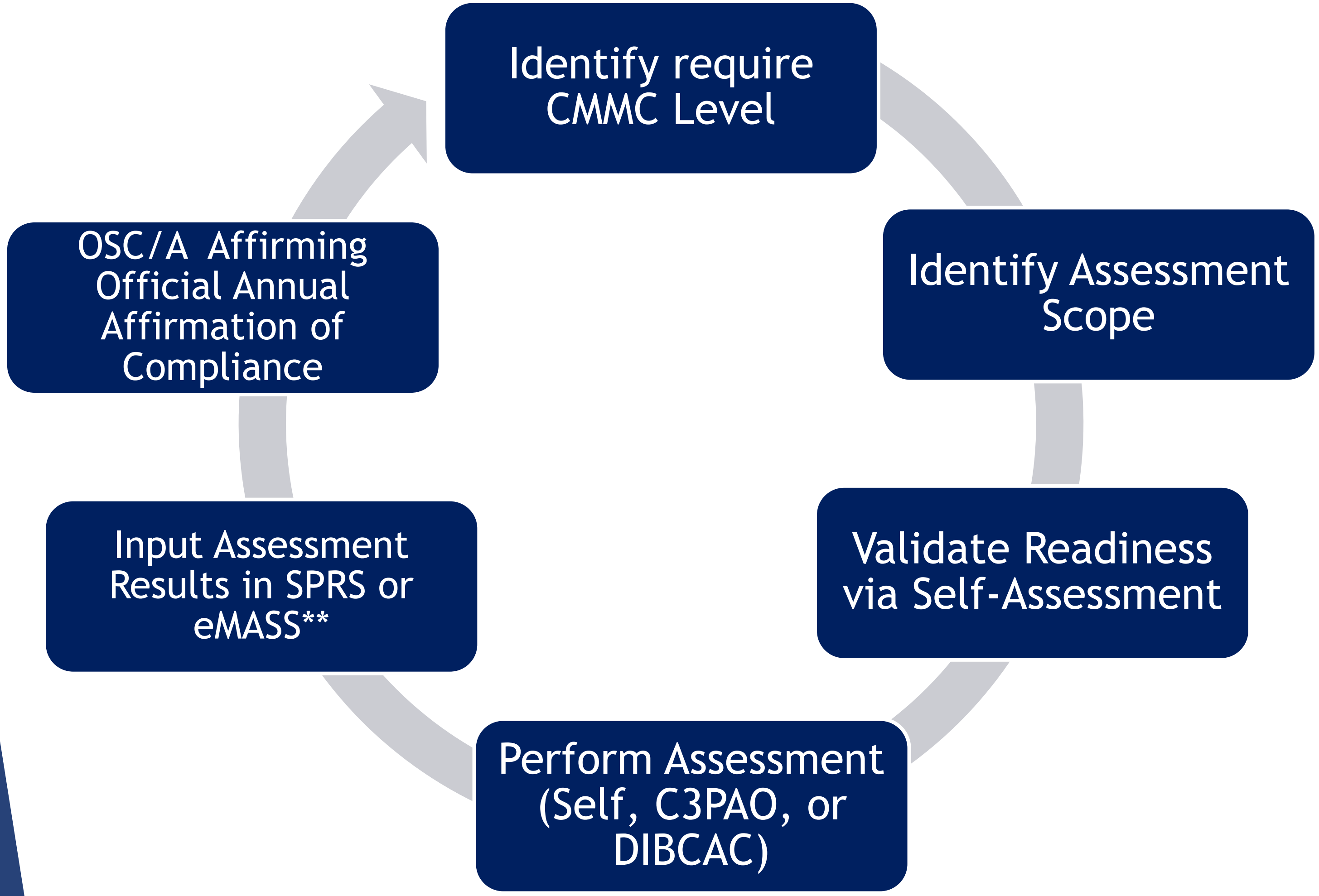
- Provide understanding of the CMMC assessment process;
- Provide understanding of the CMMC certification process; and
- Provide understanding of how to prepare for CMMC assessments and certifications.

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

1 = CMMC L1 Content
2 = CMMC L2 Content
3 = CMMC L3 Content
A = CMMC All Levels Content
✚ = Non-CMMC Content/Extra

General CMMC Assessment Process Flow


Identify require CMMC Level
Identify Assessment Scope
Validate Readiness via Self-Assessment
Perform Assessment (Self, C3PAO, or DIBCAC)
Input Assessment Results in SPRS or eMASS**
OSC/A Affirming Official Annual Affirmation of Compliance

DoD Estimated Contractors at Each Level

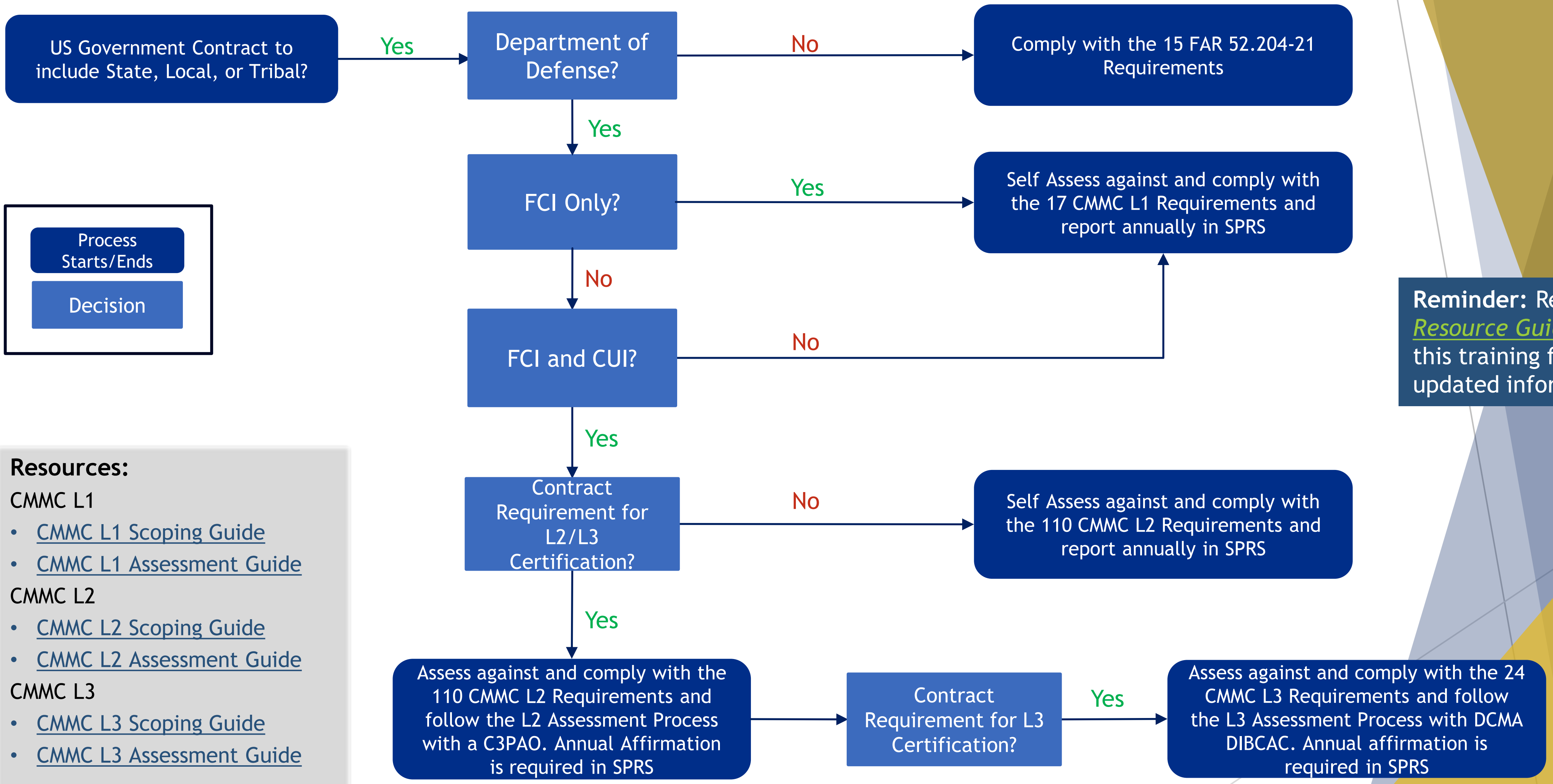
CMMC Level	% Contracts
L1 - Self Assess	~62%
L2 – Self Assess	~2%
L2 - Certified	~35%
L3 - Certified	~1%

Reminder: Refer to the *Resource Guide* provided in this training for the most updated information.

**Depends on assessment type, see notes.

Source: Cybersecurity Maturity Model Certification Model Overview Version 2.13 | September 2024, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview.pdf

Assessment Level Identification



US Government Contract to include State, Local, or Tribal?

Yes

Department of Defense?

No

Comply with the 15 FAR 52.204-21 Requirements

Yes

FCI Only?

Yes

Self Assess against and comply with the 17 CMMC L1 Requirements and report annually in SPRS

No

FCI and CUI?

No

Yes

Contract Requirement for L2/L3 Certification?

No

Self Assess against and comply with the 110 CMMC L2 Requirements and report annually in SPRS

Yes

Assess against and comply with the 110 CMMC L2 Requirements and follow the L2 Assessment Process with a C3PAO. Annual Affirmation is required in SPRS

Contract Requirement for L3 Certification?

Yes

Assess against and comply with the 24 CMMC L3 Requirements and follow the L3 Assessment Process with DCMA DIBCAC. Annual affirmation is required in SPRS

Process Starts/Ends

Decision

Resources:

CMMC L1

- CMMC L1 Scoping Guide
- CMMC L1 Assessment Guide

CMMC L2

- CMMC L2 Scoping Guide
- CMMC L2 Assessment Guide

CMMC L3

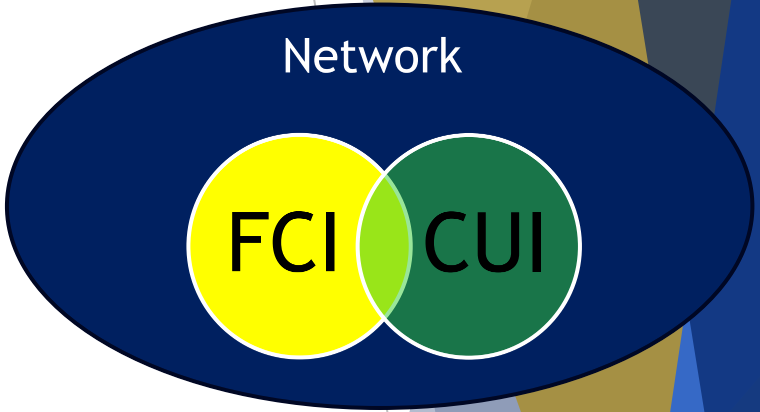
- CMMC L3 Scoping Guide
- CMMC L3 Assessment Guide

Reminder: Refer to the *Resource Guide* provided in this training for the most updated information.

Source: Cybersecurity Maturity Model Certification Model Overview Version 2.13 | September 2024, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview.pdf

Identify Assessment Scope

- Prior to conducting any CMMC assessment, the assessment scope needs to be identified.
- The scope will always include assets that:
  - **Process** – FCI/CUI can be used by an asset
  - **Store** – FCI/CUI is inactive or at rest
  - **Transmit** – FCI/CUI is being transferred from one asset to another asset
- Consider people, technology, facilities and external service providers (ESP) within the boundary scope
- Use the CMMC Scoping Guides for additional details and specifics for each CMMC Level's additional requirements



Source: CMMC Scoping Guide – Level 1, Version 2.13 | September 2024, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL1.pdf

CMMC Assessment Asset Categories

- Use the appropriate CMMC Assessment and Scoping Guides to understand requirements and to categorize all assets.

CMMC L1	CMMC L2	CMMC L3
• In-Scope Assets • FCI Assets • Out-of-Scope Assets • Specialized Assets	• In-Scope • CUI Assets • Security Protection Assets (SPA)* • Contractor Risk Managed Assets (CRMA)** • Specialized Assets** • Out-of-Scope Assets	• In-Scope Assets • CUI Assets • Security Protection Assets (SPA)* • Specialized Assets • Out-of-Scope Assets

- For all assets (people, facilities, technologies, service providers), the contractor is required to:
  - Document assets inventory
  - Document assets in System Security Plan (SSP) and
  - Provide a network diagram of the assessment scope (to include assets) to facilitate scoping discussions during the pre-assessment.

* Security Protection Assets (SPA) are assessed against related requirements only if outside of scoping boundary

** Contractor Risk Managed Assets must be ready to be assessed against all requirements

Source: CMMC Scoping Guide - Level 1, Version 2.13 | September 2024, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL1.pdf

A

CMMC Assessment Activities (All Levels)

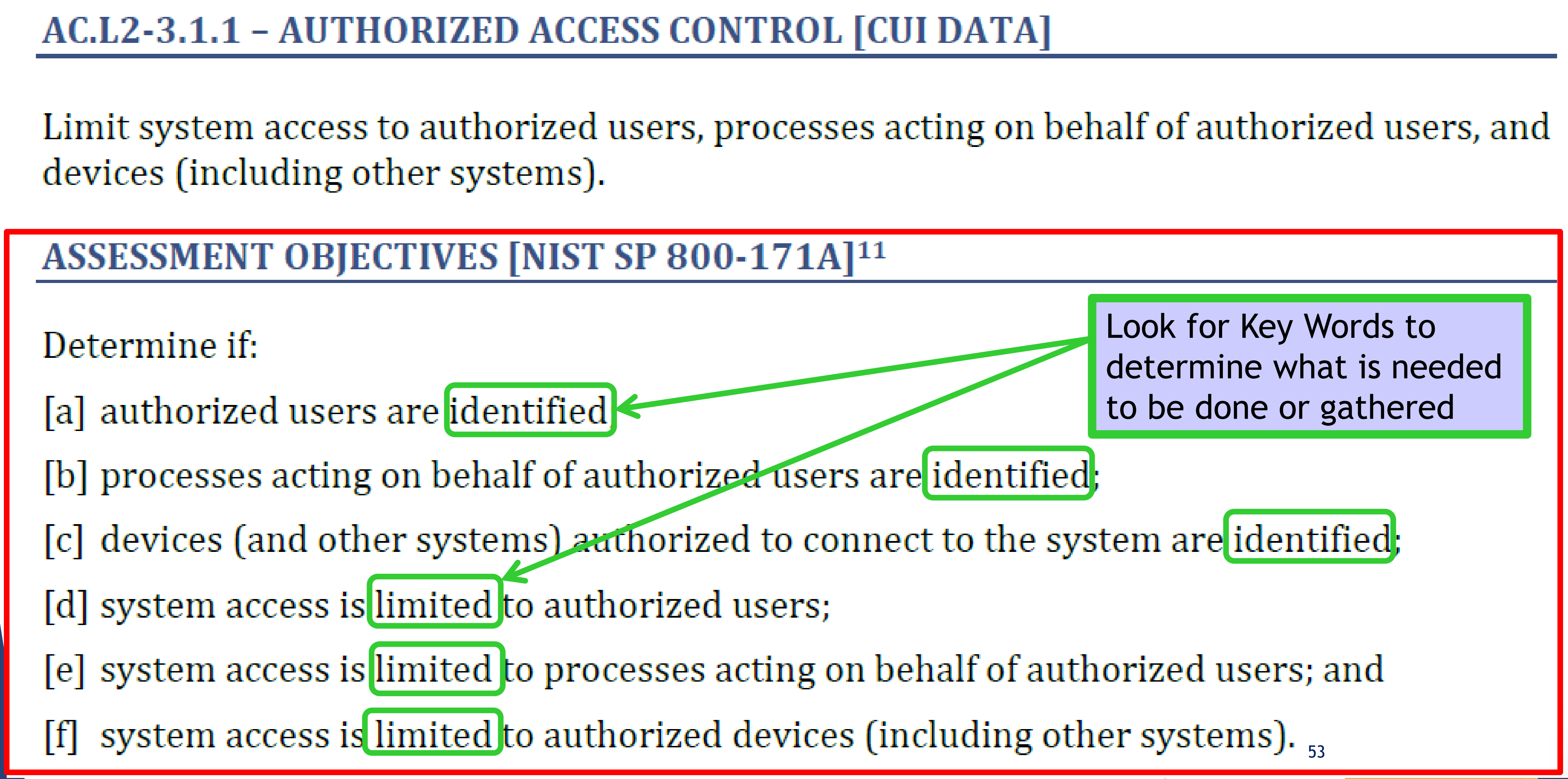
- OSCs should become intimately familiar with the CMMC Assessment Guides along with the Assessment Objectives associated with each security requirement
- Each security requirement will require the use of at least two assessment methods to validate assessment objectives to identify objective evidence.
  - **Assessment Objectives** identify the specific list of objectives that must be satisfied to receive a rating of MET for the security requirement or process, which means your company has completed the objectives for that security requirement 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
- Assessment of CMMC security requirement results in one of three possible findings:
  - MET
  - NOT MET
  - NOT APPLICABLE*
- All Applicable CMMC practices will need a finding of MET* to demonstrate CMMC compliance

* Not Applicable may be possible on select requirements

Source: CMMC Assessment Guide – Level 1, Version 2.13 | September 2024,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1.pdf

A

Security Requirement and Assessment Objectives



AC.L2-3.1.1 – AUTHORIZED ACCESS CONTROL [CUI DATA]

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A][11]

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

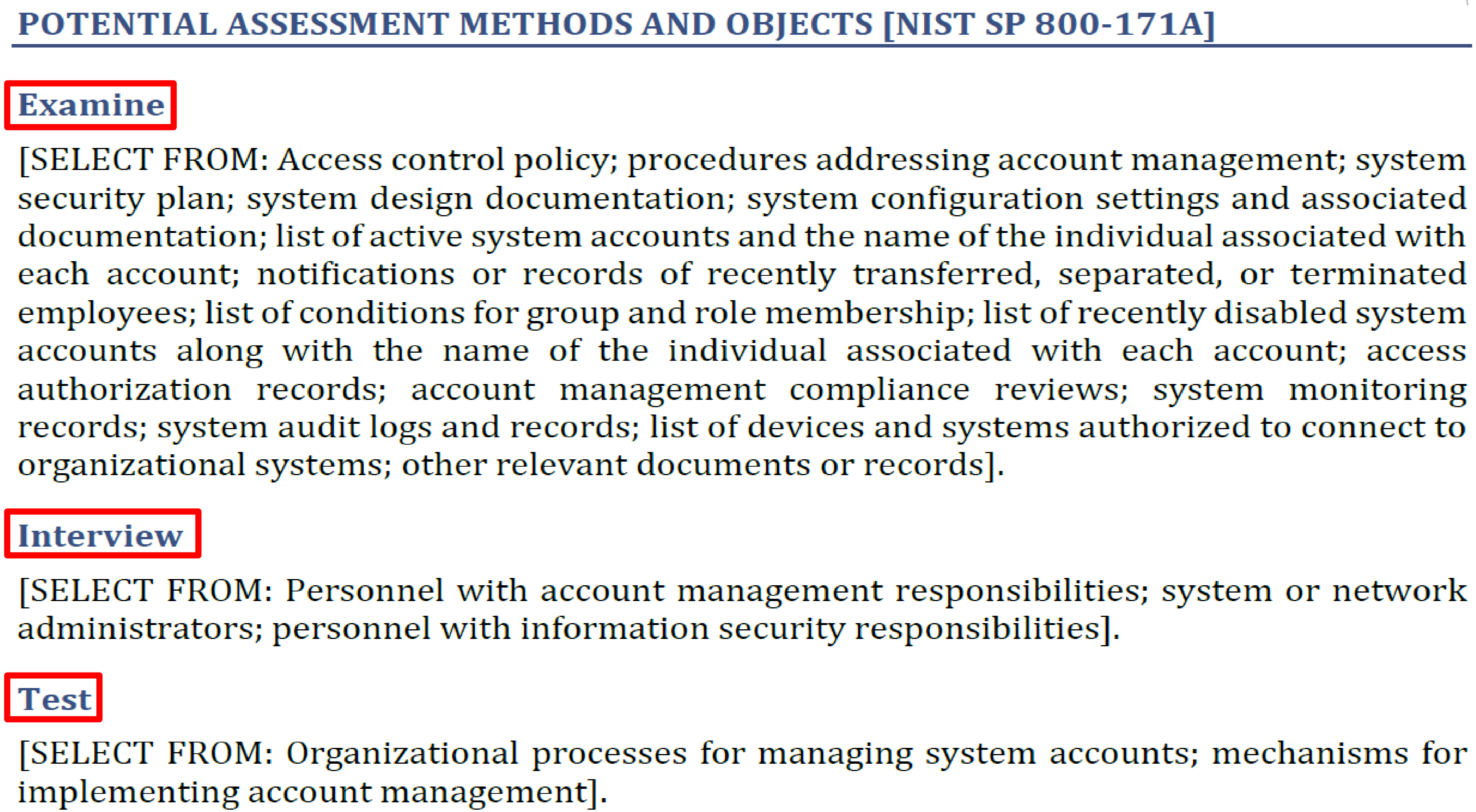
[f] system access is limited to authorized devices (including other systems).

53

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

Source: CMMC Assessment Guide – Level 1, Version 2.13 | September 2024,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1.pdf

Potential Assessment Methods and Objects



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].

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].

Potential Objects

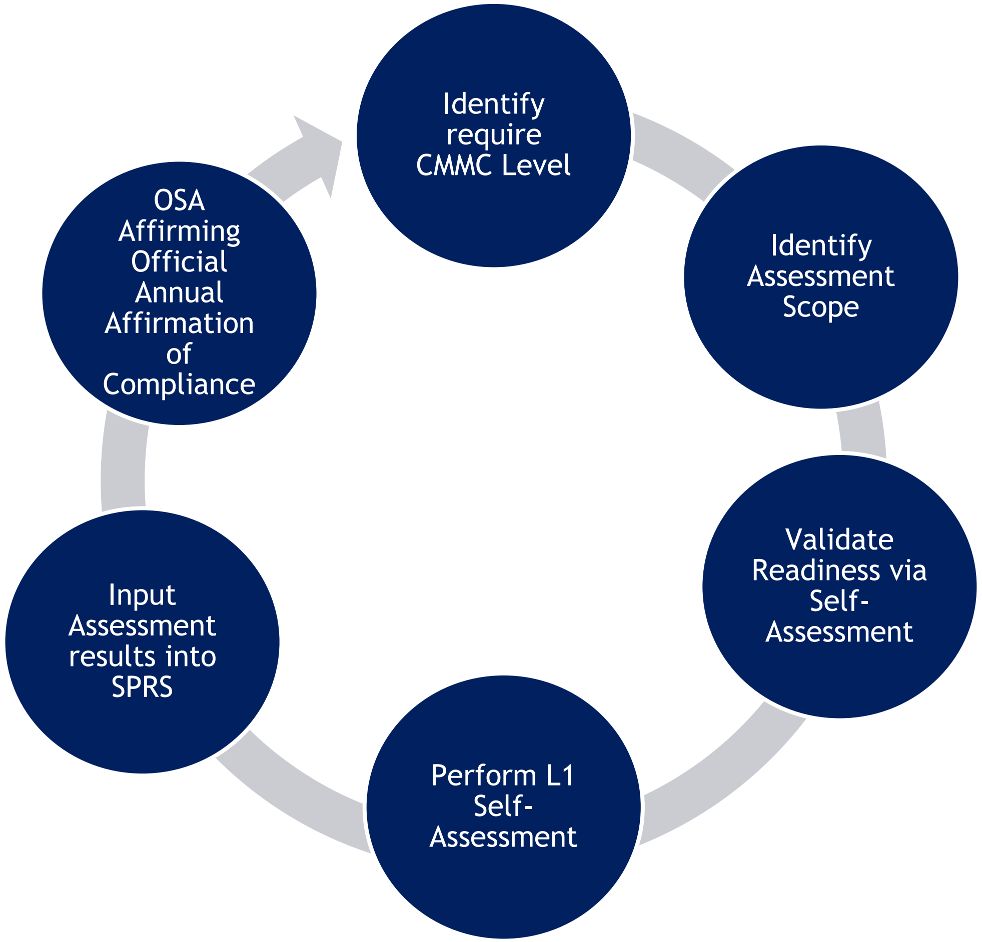
Source: CMMC Assessment Guide – Level 1, Version 2.13 | September 2024,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1.pdf

CMMC Level 1

Assessment Process

1

CMMC L1 Assessment Process Flow



Identify require CMMC Level

Identify Assessment Scope

Validate Readiness via Self-Assessment

Perform L1 Self-Assessment

Input Assessment results into SPRS

OSA Affirming Official Annual Affirmation of Compliance

Note: CMMC Program Final Rule is published, however Title 48 (DFARS rule) is still in rulemaking. Certain aspects and requirements of this clause may change. Refer to the *Resources Guide* provided in this training for the most updated information.

1

Identify Self-Assessment Scope – CMMC L1

- Prior to conducting self-assessment, the scope needs to be identified, CMMC Scoping Guide – Level 1

Assets in scope for a Level 1 self-assessment include, all assets that process, store, or transmit Federal Contract Information (FCI) including people, technology, facilities and external service providers (ESP).

Out-of-Scope Assets:
Assets that do not process, store, or transmit FCI are excluded from the Level 1 self-assessment.

Note:
Specialized Assets, are **not** part of the Level 1 self-assessment scope and are not assessed against CMMC requirements.

Source: CMMC Scoping Guide – Level 1, Version 2.13 | September 2024,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL1.pdf

Assessment Specifics – CMMC L1

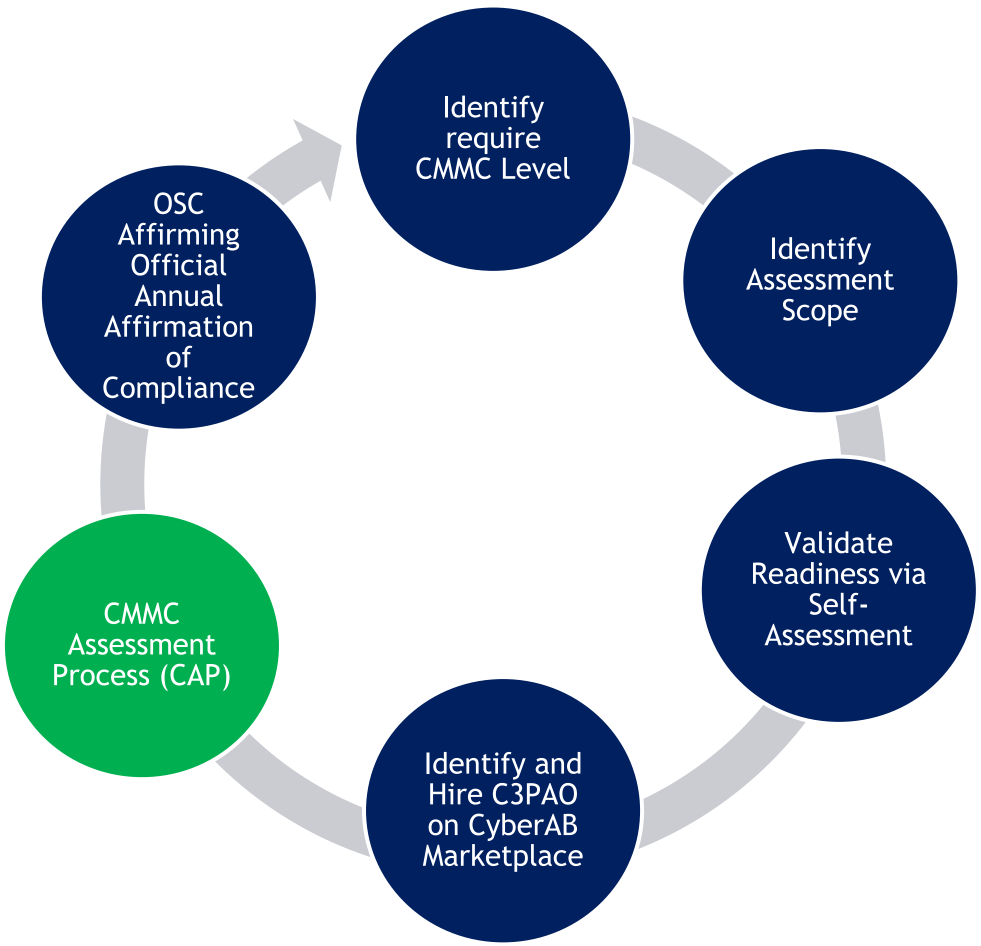
- There are no documentation requirements for L1 self-assessments including In-scope, Out-of-scope, and Specialized assets.
- Asset Categories
  - In-Scope: assets that process, store, or transmit Federal Contract Information (FCI)
  - Out-of-Scope: assets that does not process, store, or transmit FCI. These assets are not part of L1 self-assessment scope
  - Specialized Assets: assets that can process, store, or transmit FCI but are unable to be fully secured. Specialized Assets are not part of L1 self-assessment scope.
- Security Requirements
  - 15 required by FAR Clause 52.204-21
    - 17 security requirements from NIST SP 800-171 R2 / CMMC L1
  - Plan of Action and Milestones (POA&MS) are not permitted

Source: CMMC Assessment Guide – Level 1, Version 2.13 | September 2024,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1.pdf

CMMC Level 2

Assessment Process

CMMC L2 Assessment Process Flow



Identify require CMMC Level

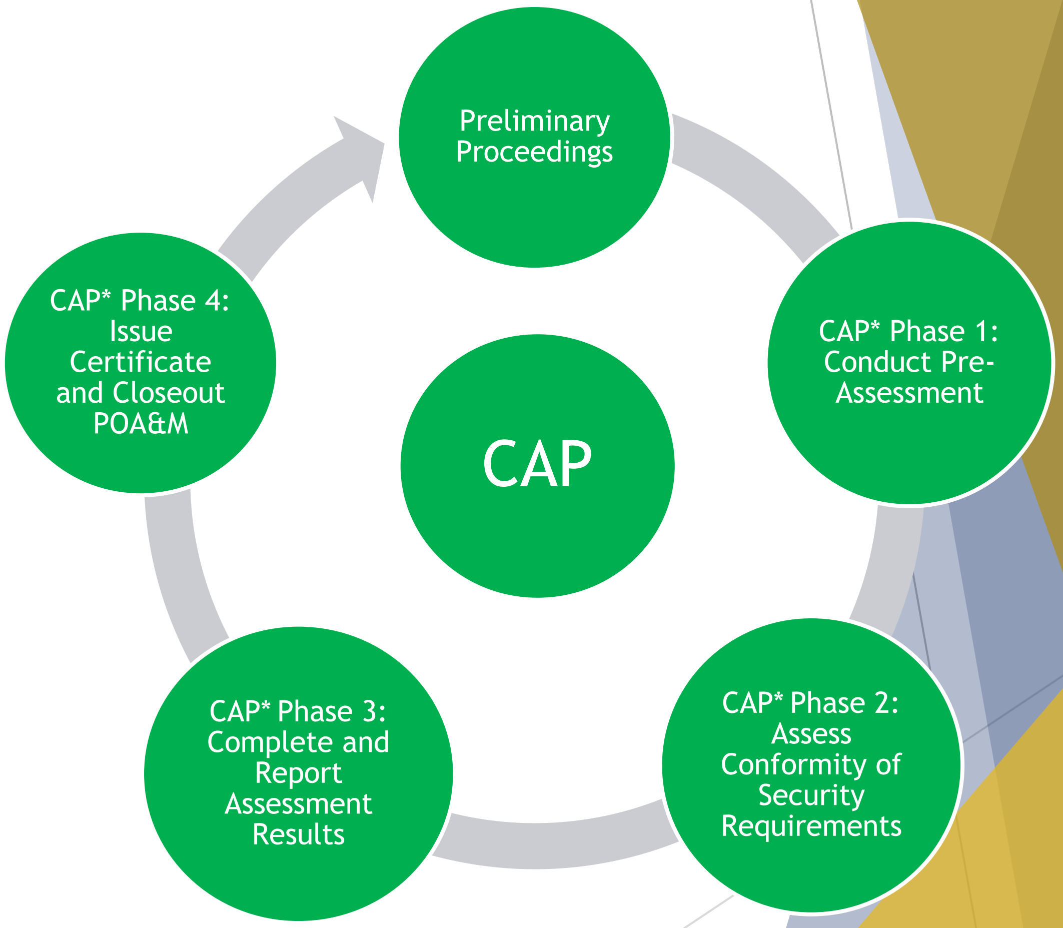
Identify Assessment Scope

Validate Readiness via Self-Assessment

Identify and Hire C3PAO on CyberAB Marketplace

CMMC Assessment Process (CAP)

OSC Affirming Official Annual Affirmation of Compliance



CAP

Preliminary Proceedings

CAP* Phase 1: Conduct Pre-Assessment

CAP* Phase 2: Assess Conformity of Security Requirements

CAP* Phase 3: Complete and Report Assessment Results

CAP* Phase 4: Issue Certificate and Closeout POA&M

*DoD/CyberAB CMMC Assessment Process (CAP)

Note: CMMC Program Final Rule is published, however Title 48 (DFARS rule) is still in rulemaking. Certain aspects and requirements of this clause may change. Refer to the *Resources Guide* provided in this training for the most updated information.

Identify Assessment Scope – CMMC Level 2

- Identify the scope, CMMC Assessment Scope Level 2 and the CMMC Level 2, Asset Categories are:

CUI Assets	Security Protection Assets*	Contractor Risk Managed Assets	Specialized Assets
Assets that process, store, or transmit Controlled Unclassified Information (CUI).	Assets providing security functions or capabilities within the contractor's CMMC Assessment Scope, regardless of CUI involvement. These include: • People • Technology • Facilities	Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place.	Assets that may or may not handle CUI, including: • Government Property • Internet of Things (IoT) Devices • Restricted Information Systems • Test Equipment

- For all assets (people, facilities, technologies, service providers), the contractor is required to:
  - Document assets inventory
  - Document assets in System Security Plan (SSP), and
  - Provide a network diagram of the assessment scope (to include assets) to facilitate scoping discussions during the pre-assessment.

Source: CMMC Scoping Guide – Level 2, Version 2.13 | September 2024,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf

CMMC Assessment Process (CAP) – CMMC L2

Phase 1

- □ Review SSP
- □ Validate CMMC Assessment Scope
- □ Confirm availability of evidence
- □ Determine readiness for Assessment
- □ Compose Assessment team
- □ Complete Pre-Assessment form
- □ Conduct Quality Assurance Review of Pre-Assessment and planning information
- □ Upload Pre-Assessment form into CMMC eMass
- □ Adverse determination of Assessment Readiness

Phase 2

- □ Conduct In-Brief Meeting
- □ Assess Implementation of Security Requirements
- □ Apply Sampling Values for Depth and Coverage
- □ Conduct Assessment Scoring
- □ Address External Service Providers (ESPs)
- □ Address Cloud Service Providers (CSPs)
- □ Conduct Quality Assurance Reviews
- □ Convene Daily Checkpoint Meetings

Phase 3

- □ Compile and Compose Assessment Results
- □ Conduct Quality Assurance Review
- □ Convene Out-Brief Meeting
- □ Upload Certification results into CMMC eMASS
- □ Administer Assessment Appeals (if required)

Phase 4

- □ Generate Certificate of Status
- □ Issues Certificate of CMMC Status
- □ Close-Out POA&M (if required)

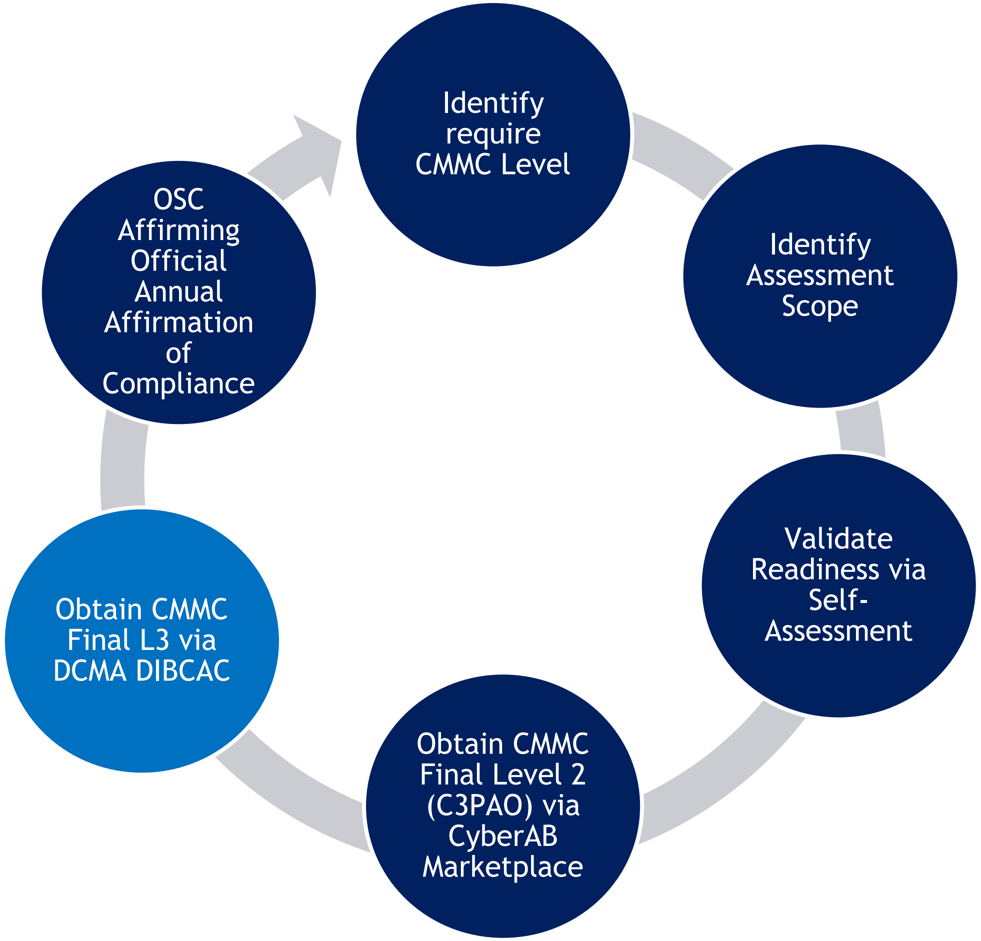
Source: CMMC Assessment Process, Version 2.0 | December 2024, https://cyberab.org/Portals/0/CMMC%20Assessment%20Process%20v2.0.pdf?ver=fEk1pUK1Fg26fVtopxv_DA%3d%3d

CMMC Level 3

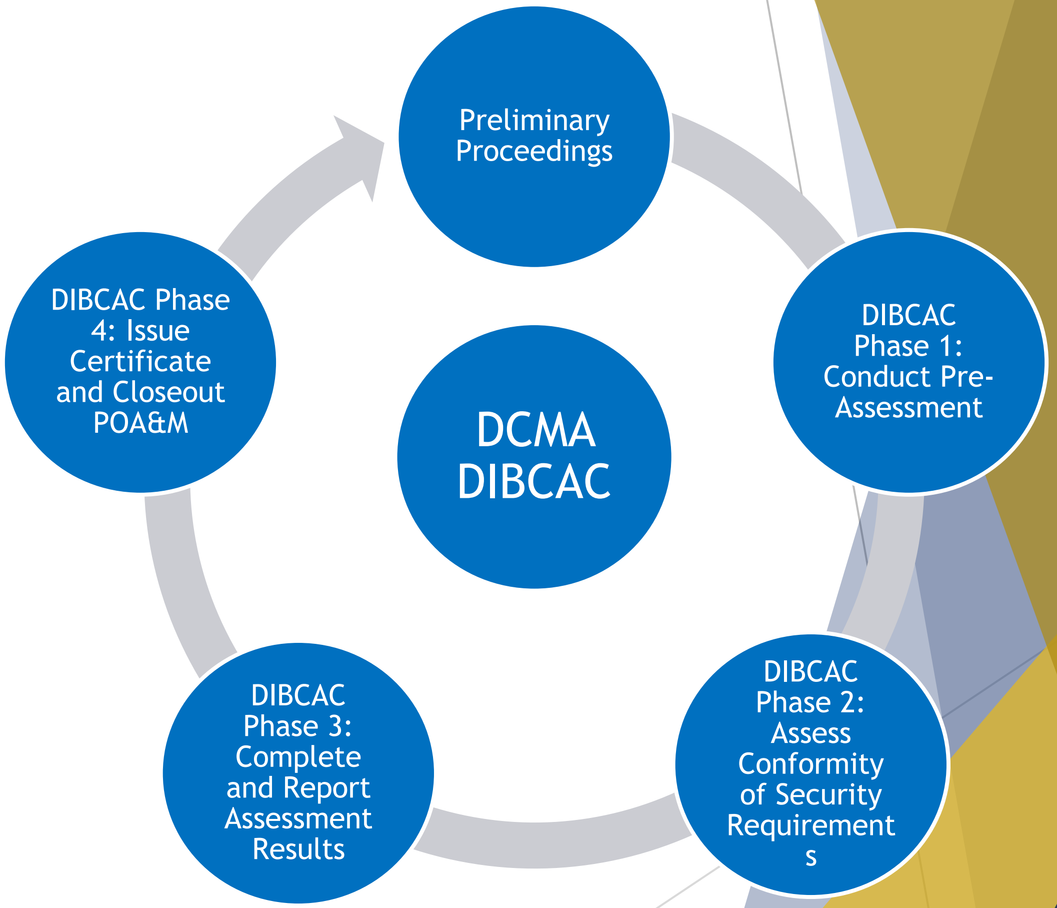
Assessment Process

3

CMMC L3 Assessment Process Flow



Identify require CMMC Level
Identify Assessment Scope
Validate Readiness via Self-Assessment
Obtain CMMC Final Level 2 (C3PAO) via CyberAB Marketplace
Obtain CMMC Final L3 via DCMA DIBCAC
OSC Affirming Official Annual Affirmation of Compliance



DCMA DIBCAC
Preliminary Proceedings
DIBCAC Phase 1: Conduct Pre-Assessment
DIBCAC Phase 2: Assess Conformity of Security Requirement s
DIBCAC Phase 3: Complete and Report Assessment Results
DIBCAC Phase 4: Issue Certificate and Closeout POA&M

*DoD/CyberAB CMMC Assessment Process (CAP)

Note: CMMC Program Final Rule is published, however Title 48 (DFARS rule) is still in rulemaking. Certain aspects and requirements of this clause may change. Refer to the *Resources Guide* provided in this training for the most updated information.

CyberAssist

3

DCMA DIBCAC Assessment Process

Phase 1

- □ Review SSP
- □ Validate CMMC Assessment Scope
- □ Confirm availability of evidence
- □ Determine readiness for Assessment
- □ Compose Assessment team
- □ Complete Pre-Assessment form
- □ Conduct Quality Assurance Review of Pre-Assessment and planning information
- □ Upload Pre-Assessment form into CMMC eMass
- □ Adverse determination of Assessment Readiness

Phase 2

- □ Conduct In-Brief Meeting
- □ Assess Implementation of Security Requirements
- □ Apply Sampling Values for Depth and Coverage
- □ Conduct Assessment Scoring
- □ Address External Service Providers (ESPs)
- □ Address Cloud Service Providers (CSPs)
- □ Conduct Quality Assurance Reviews
- □ Convene Daily Checkpoint Meetings

Phase 3

- □ Compile and Compose Assessment Results
- □ Conduct Quality Assurance Review
- □ Convene Out-Brief Meeting
- □ Upload Certification results into CMMC eMASS
- □ Administer Assessment Appeals (if required)

Phase 4

- □ Generate Certificate of Status
- □ Issues Certificate of CMMC Status
- □ Close-Out POA&M (if required)

Source: CMMC Assessment Process, Version 2.0 | December 2024, https://cyberab.org/Portals/0/CMMC%20Assessment%20Process%20v2.0.pdf?ver=fEk1pUK1Fg26fVtopxv_DA%3d%3d

Assessment Specifics – CMMC L3

- Pre-Requisites
  - Must have a Final Level 2 CMMC Third-Party Assessment Organization (C3PAO) CMMC status for the same CMMC Assessment Scope as the L3 assessment
    - The CMMC L3 assessment scope may be a subset of the L2 assessment scope
  - Assets designated as Contractor Risk Managed Assets (CRMAs) in the L2 assessment scope will be treated as CUI assets in the L3 assessment.
  - Assessment requirements for Specialized Assets differ between L2 and L3
  - Organizations Seeking Certifications (OSCs) may have CRMAs and Specialized Assets assessed by a C3PAO during the L2 certification assessment.
  - Defense Contract Management Agency (DCMA) Defense Industrial Base Cyber Assessment Center (DIBCAC) may check any L2 security requirements of any in-scope asset as part of the L3 assessment.
  - OSCs need to assess and comply against the 24 L3 security requirements.
  - Contact the DCMA DIBCAC via contacts provided here: https://www.dcma.mil/DIBCAC/

Source: CMMC Assessment Scope – Level 3, Version 2.13 | September 2024,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL3.pdf

Assessment Specifics – CMMC L3 (cont’d)

Asset Categories

CUI Assets

Assets that process, store, or transmit Controlled Unclassified Information (CUI).

For L3, it also include assets that can, but are not intended to, process, store, or transmit CUI (defined as Contractor Risk Managed Assets)

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

Specialized Assets

Assets that can process, store, or transmit CUI 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.

Source: CMMC Assessment Guide – Level 1, Version 2.13 | September 2024,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1.pdf

A

How to Prepare for CMMC (All Levels)

Recommendations prior to contract award:

- Understand contract requirements: FAR 52.204-21, CMMC requirements, FCI, CUI and other applicable clauses and standards, and CMMC requirements (Section 2)
- Be aware of contractual reporting requirements (Section 4)
- Identify possible data types and locations, access, and security as well as documenting all assets and asset categories
- Keep following cybersecurity best practices (Section 5)
- Perform your self-assessment
- Update Supplier Performance Risk System (SPRS) self-assessment yearly
- Understand subcontractor compliance requirements and keep up to date with regulatory changes
- Be aware of flow down requirements for subcontractors*

This Photo by Unknown Author is licensed under CC BY-SA-NC

Recommendations for after contract award:

- Keep self-assessment score up to date (annually)
- Senior Affirming Official attests the organization is satisfying and will maintain its specified cybersecurity requirements annually.
- Keep asset list, documentation and 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

*Note: Exception for Commercial of the shelf (COTS) products

Section 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: Section 4 – Incident Reporting

Incident Reporting

Section 4

CyberAssist

Section Topics and Objectives

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

Topics covered in this section:

- Common Cyber Incidents
- Cyber Incident Reporting Tips
- Cyber Incident Reporting – CMMC Level 2 & 3

The objectives of this section are:

- Provide understanding of common cyber incidents; and
- Provide understanding of cyber incident reporting tips.

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

1	= CMMC L1 Content
2	= CMMC L2 Content
3	= CMMC L3 Content
A	= CMMC All Levels Content
✚	= Non-CMMC Content/Extra

Cyber Incident Reporting

Our customers count on our products and services to support their mission each and every time. This includes timely reporting if information is compromised or exposed to unauthorized parties.

Cyber incident reporting is the process of reporting any actual or potential cyber incidents to the appropriate authority or organization.

Common Cyber and Security Incidents

The most common types of cyber and security incidents include:

- social engineering (e.g., phishing email)
- emailing sensitive information to unauthorized people
- unauthorized access to sensitive information from outside the organization (e.g., via compromised account credentials)
- lost laptops and mobile devices
- insider threats
- malware / ransomware

1

Cyber Incident Reporting Tips

It is recommended to report all cyber incidents even if they do not trigger a mandatory reporting requirement.

- Prompt reporting of actual and suspected security incidents can help prevent or limit the severity of an incident

Report incidents in a timely manner to avoid harm to your company's reputation and resources

▶ Comply with contract requirements for prompt incident reporting (e.g., 72 hours after discovery)

▶ Notify stakeholder points of contact per contract requirements (typically the buyer or subcontract manager / administrator)

▶ Follow any specific internal reporting requirements for your organization

Security incidents may include loss, theft, misuse, tampering, corruption, unauthorized disclosure of information, or when an individual violates controls intended to limit their access to information.

2

3

Cyber Incident Reporting – CMMC Level 2 & 3

- Organizations seeking to achieve CMMC Level 2, to be eligible for DoD subcontracts involving CUI should be aware…
  - Contracts involving CUI invoke DFARS 252.204-7012 with mandatory cyber incident reporting requirements
  - Report incidents to DoD (DIBNet site) within 72 hours of discovery
  - A Medium Assurance Certificate is required to report a cyber incident, applying to the DIB CS Program is not a prerequisite to report
  - DoD DIBNet and DFARS 252.204-7012 provide detailed guidance on required actions following a cyber incident

Ensure regulatory reporting requirements are understood when advancing to CMMC Level 2 (managing CUI)

Next: Section 5 - Cybersecurity Best Practices

Cybersecurity Best Practices

Section 5

Section Topics and Objectives

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

Topics covered in this section:

- The Importance of Cybersecurity Awareness
- Top 10 High Value Controls
- Threat Scenario Example: Phishing
- Cyber Attack Methods and Mitigation
- Threat Scenario Shop Floor Example

The objectives of this section are:

- Provide understanding of cybersecurity awareness;
- Identifies the top 10 high value controls;
- Provides a real-life scenario to help with understanding the threat; and
- Provide understanding of cyber attacks – threat actors, methods and mitigations.

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

1 = CMMC L1 Content

2 = CMMC L2 Content

3 = CMMC L3 Content

A = CMMC All Levels Content

✚ = Non-CMMC Content/Extra

The Importance of Cybersecurity Awareness

Cybersecurity awareness is the process of learning and building knowledge about keeping IT resources secure by maintaining the confidentiality, integrity, and availability of those IT resources. Building the awareness and knowledge on how to protect those IT resources that store and process information from:

- **Threats:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Source: NIST SP 800-30 Rev 1
- **Vulnerabilities:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Source: NIST SP 800-30 Rev 1

Top 10 High Value Controls

The DIB SCC Task Force Working Group has prioritized a set of *Top 10 High Value Controls* that are separate from the CMMC domains but help facilitate many of the practices within CMMC.

Click on each of the controls to obtain additional information on the implementation and assessment of these controls.

Next, we will present a threat scenario to help your understanding.

1. Administrative Rights and Privileges
2. Antivirus/Malware
3. Default Passwords
4. DNS Mitigations
5. Email Filtering
6. Employee Training and Awareness
7. Multi-Factor Authentication
8. Patching
9. Perimeter Hardening
10. Web Content Filtering

Source: https://ndisac.org/dibscc/implementation-and-assessment/top-10-high-value-controls/

Threat Scenario Example: Phishing

Most cyber attacks will involve an element of social engineering in which the adversary attempts to use psychological manipulation to gain your trust and manipulate you into disclosing information or performing an action that could compromise security.

How can the threat actors initiate contact?

Email

Phone

Social Media & Text Messages

Face-to-face

What should you look out for?

- Requests to provide information or click on embedded links or attachments which could lead to legitimate-looking fraudulent websites that attempt to deceive you into entering information

Maintain a healthy level of skepticism and scrutinize all unexpected messages, even if they appear to come from someone you know.

Cyber Attack Methods and Mitigation

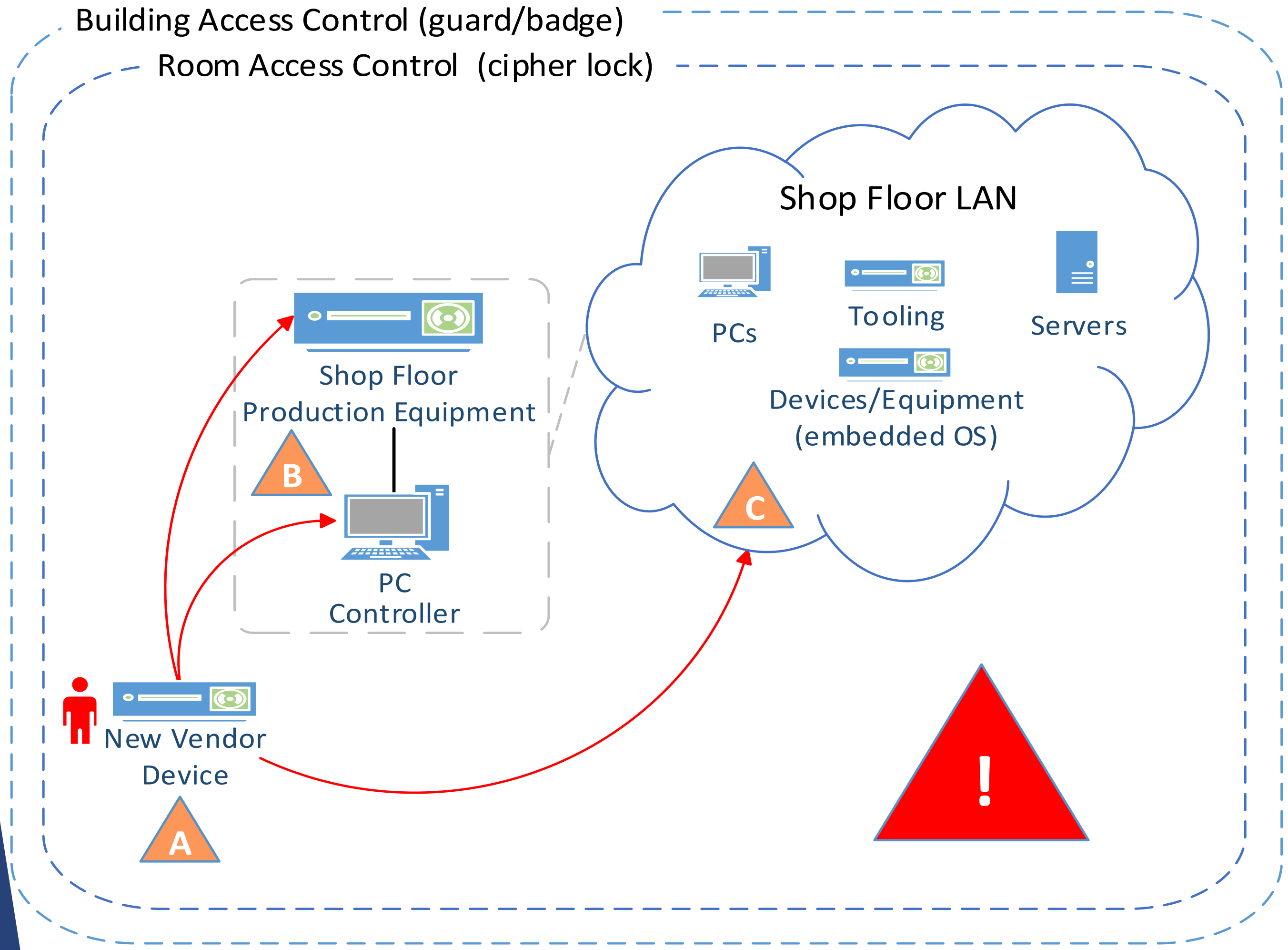
Regardless of the exploit method an adversary uses, following some simple security practices
will help you defend your company, your customers and yourself against their attacks.

- Secure and protect all IT assets and printed information.
- Do not open unexpected email, click on unexpected links or attachments, or reply to spam.
- Be mindful of what you share on social media and use privacy settings to restrict who can see it.
- Verify an individual’s identity, authorization, and need to know before providing personal or company information.

- Be aware of your surroundings. Control line-of-site access and the volume of your voice/audio so that unauthorized people cannot view or hear information.
- Promptly report actual and suspected information protection and cybersecurity incidents.

Threat Scenario Example: Shop Floor

Note: This example is based on a real-world example TSMC outage/attack



Building Access Control (guard/badge)
Room Access Control (cipher lock)
Shop Floor LAN
PCs
Tooling
Servers
Devices/Equipment (embedded OS)
C
Shop Floor Production Equipment
B
PC Controller
New Vendor Device
A
!

A — A company allows one of their vendors to introduce test, diagnostic, or new equipment directly into the production environment. The device contains software that spawns malicious processes (e.g., malware, ransomware).

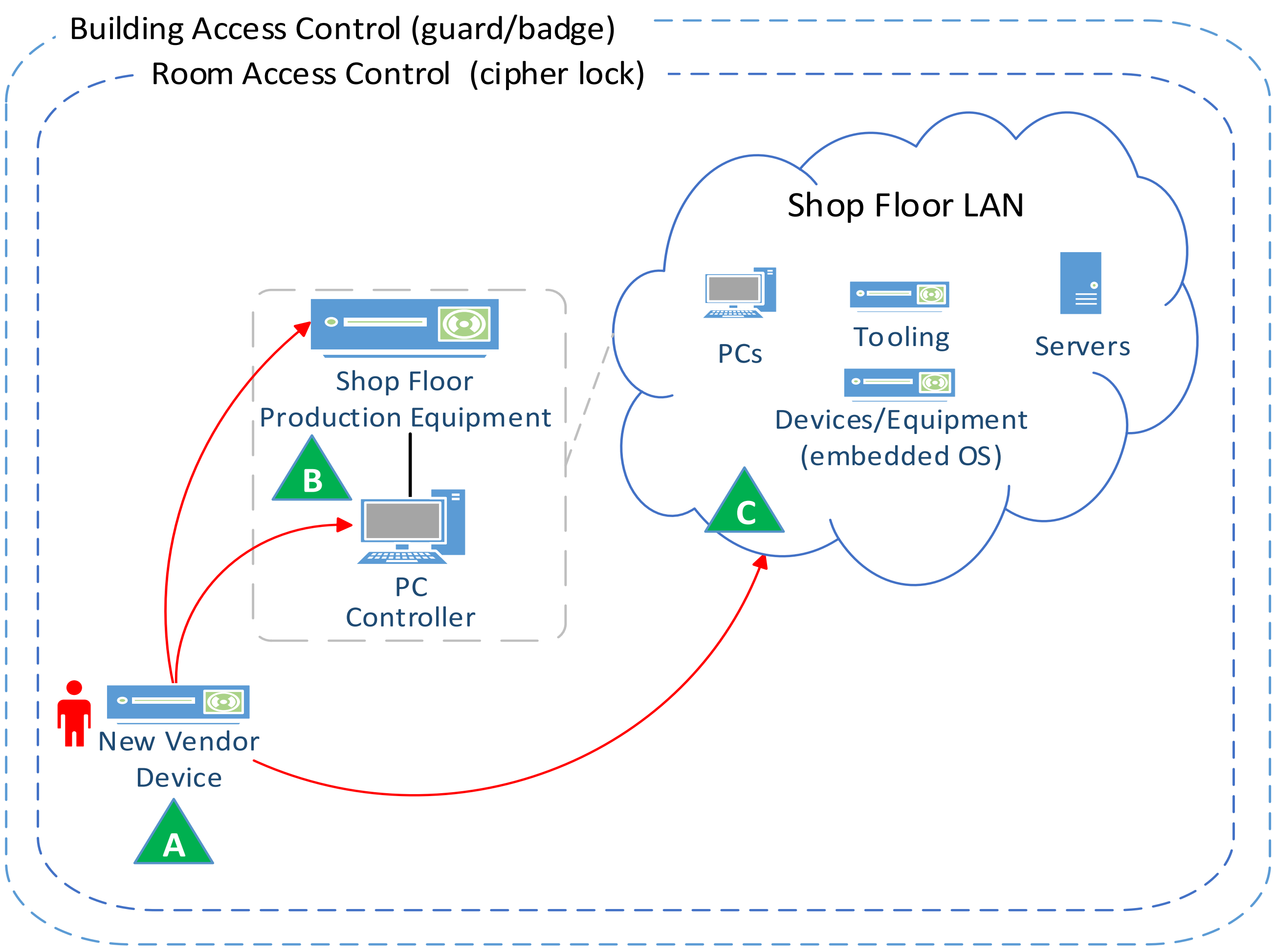
B — Once the device is connected to a shop floor production device or PC, it scans the machine to determine if a vulnerable OS and patch level are present. If so, these devices are compromised and are used for further attack propagation.

C — Compromised production device or PC is used to scan the entire local network (connected devices) to determine if additional vulnerable machines can be compromised. If so, they are compromised.

! — Compromised devices are encrypted with adversary keys and are unusable. Equipment can no longer be operated, **production stops**!

The infection, which was eventually contained, delayed shipments of its products and wiped as much as $171 million off its revenue!

Threat Scenario Example: Shop Floor with Implemented CMMC Practices


Building Access Control (guard/badge)
Room Access Control (cipher lock)
Shop Floor LAN
PCs
Tooling
Servers
Devices/Equipment (embedded OS)
C
Shop Floor Production Equipment
B
PC Controller
New Vendor Device
A

Access Control

AC.L1-3.1.1 Limit information system access to authorized users, **processes acting on behalf of authorized users, or devices** (including other information systems).

System and Information Integrity

SI.L1-3.14.1 Identify, report, and correct system flaws in a timely manner (patch).

SI.L1-3.14.2 Provide protection from malicious code at designated locations within organizational information systems.

SI.L1-3.14.4 Update malicious code protection mechanisms when new releases are available.

SI.L1-3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Section Summary

- Using good cybersecurity practices not only helps protect your company from cyber attacks, but also your defense contractor customers
- Cybersecurity threats can come from inside or outside your company
- Being aware of threats and how to mitigate them keeps your business running
- Cybersecurity is about making sure that untampered data is available and accessible only to the people who require the data
- For questions on the content, please send them to DIB SCC Cyber Training

Next: Section 6 – Risk Management and Assessing Risk

Risk Management and Assessing Risk

Section 6

Section Topics and Objectives

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

Topics covered in this section:

- Risk Management 101
- Risk Identification
- Risk Evaluation and Measurement
- Risk Control Management and Implementation
- Risk Management Key Points

The objectives of this section are:

- Provide understanding of risk management;
- Provide understanding of risk identification; and
- Provide understanding of risk control management and implementation.

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

- 1 = CMMC L1 Content
- 2 = CMMC L2 Content
- 3 = CMMC L3 Content
- A = CMMC All Levels Content
- ✚ = Non-CMMC Content/Extra

Risk Management 101

- Risk management applies to many aspects of a business.
  - Internal risks (weaknesses) - controllable
  - External risks (threats) – typically uncontrollable
  - Negative (weaknesses and threats)
  - Positive (opportunities)
- The ultimate goal is to minimize the effects of risks on your business.
  - Business continuity
  - Greater stability
  - Better cash flow
  - Longevity
- Stages of Risk Management
  - Risk Identification
    - Internal vs. External Risks
  - Risk Evaluation
  - Risk Measurement
  - Risk Control Management and Implementation

Risk Identification

- Internal Risks
  - Employee Risks
    - Illness and death
    - Theft and fraud
    - Low employee morale
    - Personal conflicts
    - Complacency
    - Insider threat
  - Equipment and Information Technology Risks
    - Old equipment
    - Patching
    - Cybersecurity
  - Other
    - Other technologies such as phones
    - Injuries and damage to business
    - Cash flow
    - Visibility

- External Risks
  - Competition and Market Risks
    - Market changes
    - Loss of employees
    - Rent increase
  - Business Environment Risks
    - Laws and ordinances (federal, state, local)
    - Weather and natural disasters
    - Community changes
    - Visibility
  - Non-Employee Risks
    - Unprovoked violence
    - Theft of goods and services
    - Malicious Cyber Threat Actor

Risk Evaluation and Measurement

- Evaluate SWOT (Strengths, Weaknesses, Opportunities, Threats)
- Identify Warning Signs
  - Excessive debt to equity ratio
  - Reliance on small number of customers, products, vendors
  - Cash flow issues
  - Irregularities in records (timekeeping, accounting, bank)
  - Irregularities in reports (computers, users)
  - High turnover rate
- Risk Measurement
  - Likelihood vs impact

Risk Control Management and Implementation

- Equipment
- Vendors
- Business Continuity
- IT Systems
- Competition
- Accounting and Cash Flow
- Employee Management
- Business Work Strategy
- Exit Strategy

Risk Management Key Points

1. Risks associated with a small business, or any business, can be characterized as internal or external.
2. Begin assessing risks by listing events or resources that could impact continued operations and cash flow.
3. The costs to insure or minimize risks should be weighed against the potential impact of the risk.
4. A business continuity plan should be part of your overall business plan.
5. Strategies to avoid risks can include: communication, setting expectations, support systems, staff training, insurance, risk assessment, and contingency planning.
6. Be honest in reviewing your business for risk and know the warning signs.
7. Seek assistance from others.
8. Include an exit strategy in your initial business plan and revisit that strategy from time to time.

Note: For more information on risk management, there is a free NIST training course (approximately three hours): Risk Management Framework for Systems and Organizations Introductory Course

Section Summary

- **Ultimate goal on Risk Management:** To control the effects of risks on your business
- There are four stages for Risk Management:
  - Risk Identification
  - Risk Evaluation
  - Risk Measurement
  - Risk Control Management and Implementation
- Risks associated with business can be characterized as internal or external

Resource Guide

Glossary, Acronym Guide and Additional Resources for More Information

Glossary

Access Control (AC): The process of granting or denying specific requests to:

- obtain and use information and related information processing services; and
- enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

Source: FIPS 201, CNSSI 4009

Advanced Persistent Threat (APT): An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:

- pursues its objectives repeatedly over an extended period of time,
- adapts to defenders' efforts to resist it, and
- is determined to maintain the level of interaction needed to execute its objectives.

Source: NIST SP 800-39

Affirming Official: The senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations. (CMMC-custom term, Source: 32 CFR § 170.4)

Assessment: The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. Source: NIST SP 800-37 Rev. 2

Source: CMMC Glossary,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont’d)

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. Source*

Availability: Ensuring timely and reliable access to and use of information. Timely, reliable access to data and information services for authorized users. Source: CNSSI 4009

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. Source*

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Source: 44 U.S. Code Sec 3542

Configuration Management (CM): A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. Source: NIST SP 800-53 Rev 5

Controlled Unclassified Information (CUI): 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)

*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

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

Contractor (Defense Contractor): Any individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the DoD to furnish services, supplies, or construction. Source: 32 C.F.R. 158.3

Covered Defense Information (CDI): A term used to identify information that requires protection under DFARS Clause 252.204-7012. Unclassified controlled technical information (CTI) or other information, as described in the CUI Registry, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies and is:

- Marked or otherwise identified in the contract, task order, or delivery order and provided to contractor by or on behalf of, DoD in support of the performance of the contract; OR
- Collected, developed, received, transmitted, used, or stored by—or on behalf of—the contractor in support of the performance of the contract.

Source: DFARS Clause 252.204-7012

The Cyber 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

Source: CMMC Glossary,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont’d)

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Source: NSPD-54/HSPD-23

Cybersecurity Maturity Model Certification: Set of standards established by the DoD against which an OSC is to be assessed.

CMMC Assessment Process: Provides procedures and guidance for CMMC C3PAOs conducting official CMMC Assessments of organizations seeking CMMC certification.

CMMC Assessors and Instructors Certification Organization (CAICO): 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.

CMMC Third Party Assessment Organization (C3PAO): n Entity that is certified to be contracted to and OSC to provide consultative advice OR certified assessments.

CMMC Certified Assessor (CCA): 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).

CMMC Certified Professional (CCP): A person who has successfully completed all certification program requirements as outlined by the CAICO for becoming a Level 1 CMMC Assessor.

Source: CMMC Glossary,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont’d)

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Source: NSPD-54/HSPD-23

Cybersecurity Maturity Model Certification: Set of standards established by the DoD against which an OSC is to be assessed.

CMMC Unique Identifier (UID): 10 alpha-numeric characters assigned to each CMMC assessment and reflected in the Supplier Performance Risk System (SPRS) for each contractor information system.

CMMC Assessment Process: Provides procedures and guidance for CMMC C3PAOs conducting official CMMC Assessments of organizations seeking CMMC certification.

CMMC Assessors and Instructors Certification Organization (CAICO): 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.

CMMC Third Party Assessment Organization (C3PAO): n Entity that is certified to be contracted to and OSC to provide consultative advice OR certified assessments.

CMMC Certified Assessor (CCA): 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).

Source: CMMC Glossary,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

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)

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)

Defense Industrial Base (DIB): The worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. Source: DIB Sector-Specific Plan, DHS CISA

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)

Department of Defense Unique Identification: Assigned to each assessment. It is an alpha numeric string of ten digits. The first two letters delineate the confidence level of the assessment. Basic, Medium, and High confidence levels start with SB, SM, SH respectively (Source: https://www.sprs.csd.disa.mil/pdf/SPRS_Government.pdf)

Source: CMMC Glossary,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_20211217_508.pdf

Glossary (cont'd)

Event: Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. Source: CNSSI 4009

External Service Provider: External people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (*e.g.*, log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. (CMMC-custom term, Source: 32 CFR § 170.4)

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)

Federal Contract Information (FCI): 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 websites) or simple transactional information, such as necessary to process payments. Source: 48 CFR § 52.204-21

Hacktivists: Can be similar in expertise to rogue actors, or can bring more expertise… but **Organized around a cause**

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. 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

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont’d)

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Source: NIST SP 800-171 Rev 2

Incident Response (IR): The actions the organization takes to prevent or contain the impact of an incident to the organization while it is occurring or shortly after it has occurred. Source: CERT RMM v1.2

Integrity: The security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation). Source: NIST SP 800-33

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Source: NIST 800-171 Rev 2

*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

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

Insider Threat: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the organization or the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities. Source: CNSSD No. 504 (adapted)

Maintenance: Any act that either prevents the failure or malfunction of equipment or restores its operating capability. Source: NIST SP 800-82 Rev 2

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. Source*

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. Source*

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. Source*

Phishing emails: Broad-based messages sent indiscriminately to very large numbers of recipients with the expectation that at least a small percentage will respond.

*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

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

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. Source*

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)

Practice: An activity or set of activities that are performed to meet the defined CMMC objectives. Source: CMMC

Organization: An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements). Source: NIST SP 800-37 Rev 1

Organization Seeking Assessment: The entity seeking to undergo a self-assessment or certification assessment for a given information system for the purposes of achieving and maintaining any CMMC Status. The term OSA includes all Organizations Seeking Certification (OSCs). (CMMC-custom term, Source: 32 CFR § 170.4)

Organization Seeking Certification: The Organization that is going through the CMMC assessment process to receive a level of Certification for a given environment.

Registered Practitioner: Professionals who provide CMMC implementation consultative services.

*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

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

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.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

- the adverse impacts that would arise if the circumstance or event occurs and
- the likelihood of occurrence.

System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems. Such risks reflect the potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation. Source: FIPS 200 (adapted)

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. Source: NIST SP 800-171

Risk Management (RM): The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes:

- establishing the context for risk-related activities,
- assessing risk,
- responding to risk once determined, and
- monitoring risk over time. Source: CNSSI 4009

Source: CMMC Glossary,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

Rogue actors: Anyone who developed hacking skills.

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. Source*

Social engineering: The practice of psychologically manipulating people into performing actions or divulging information that could compromise security.

Spear phishing emails: A method by which attackers (organized perpetrators out for financial gain, trade secrets or national security information) target specific individuals or organizations seeking unauthorized access to data.

Supply chain: A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. Source: CNSSI 4009

System and Communication 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. 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

Source: CMMC Glossary,
https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont’d)

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.

System Security Plan: The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. Source: CNSSI 4009

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Source: NIST SP 800-30 Rev 1

Threat actor: An individual or a group posing a threat. Source: NIST SP 800-150

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Source: NIST SP 800-30 Rev 1

*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

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Acronym Guide

AC: Access Control

AU: Audit and Accountability

AT: Awareness and Training

C3PAO: CMMC Third-Party Assessment Organization

CA: Security Assessment

CAICO: CMMC Assessors and Instructors Certification Organization

CAP: CMMC Assessment Process

CCA: CMMC Certified Assessor

CCP: Certified CMMC Professional

CFR: Code of Federal Regulations

CM: Configuration Management

CMMC: Cybersecurity Maturity Model Certification

CDI: Covered Defense Information

CUI: Controlled Unclassified Information

DCMA: Defense Contract Management Agency

DIB: Defense Industrial Base

DIBCAC: Defense Industrial Base Cyber Assessment Center

DFARS: Defense Federal Acquisition Regulation Supplement

DoD: Department of Defense

DoD CUI: Department of Defense Controlled Unclassified Information

DoD UID: Department of Defense Unique Identification

ESP: External Service Provider

FAR: Federal Acquisition Regulation

FCI: Federal Contract Information

IA: Identification and Authentication

IR: Incident Response

IT: Information Technology

MA: Maintenance

MP: Media Protection

OSA: Organization Seeking Assessment

OSC: Organizations Seeking Certification

PS: Personnel Security

Acronym Guide (cont’d)

PE: Physical Protection

POAM: Plan of Action and Milestones

RA: Risk Assessment

RP: Registered Practitioner

RPO: Registered Provider Organization

SC: System and Communications Protection

SPRS: Supplier Performance Risk System

SI: System and Information Integrity

SSP: System Security Plan

The Cyber AB: The Cyber Accreditation Body

Resources Available for More Information

The following resources provides additional information and the latest news related to CMMC and cybersecurity. We recommend you reference these resources for the latest information and guidance on CMMC and cybersecurity.

- DoD CMMC page: https://dodcio.defense.gov/CMMC/
- DIB SCC Cyber Assist site: https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/
- CMMC Level 1: https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/level-1/
- CMMC AB Town Halls: https://cyberab.org/News-Events/Town-halls
- Supplier Performance Risk System: https://www.sprs.csd.disa.mil/
- CMMC Self-Assessment Guide (Level 1): https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1v2.pdf
- CMMC Assessment Guide (Level 2): https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL2v2.pdf
- CMMC Assessment Guide (Level 3): https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL3v2.pdf
- NIST Risk Management Framework Training: https://csrc.nist.gov/Projects/risk-management/rmf-training
- National Archives (NARA) CUI Information: https://www.archives.gov/cui
- CUI Program Blog: https://isoo.blogs.archives.gov/
- Federal Register: https://www.federalregister.gov/
- A full list of CMMC-custom terms can be found in 32 CFR § 170.4 Acronyms and definitions

Resources Available for More Information (cont'd.)

- Capability Maturity Model Integration (CMMI): https://cmmiinstitute.com
- CERT Resilience Management Model (CERT-RMM): https://cert.org/resilience
- National Defense Information Sharing and Analysis Center (NDISAC): https://ndisac.org/
- NIST News Feb. 2021: https://www.nist.gov/news-events/news/2021/02/nist-offers-tools-help-defend-against-state-sponsored-hackers
- National Institutes of Standards and Technology (NIST) - Cybersecurity: https://www.nist.gov/cybersecurity
- Center for Internet Security (CIS): https://www.cisecurity.org/
- Federal Trade Commission, Cybersecurity for Small Business: https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf
- Department of Homeland Security (DHS): https://www.dhs.gov/
- Cybersecurity & Infrastructure Security Agency (CISA): https://www.cisa.gov/
- U.S. Computer Emergency Readiness Team: https://us-cert.cisa.gov/
- Small Business Administration: https://www.sba.gov/
- Cloud Computing FAQs: https://ndisac.org/dibscc/cyberassist/awareness/cloud-computing-faqs/
- National Cyber Security Centre (Information for Small and medium sized organisations): Small & medium sized organisations - NCSC.GOV.UK
- Protecting Your Small Business: Ransomware
- Protecting Your Small Business: Phishing
- Protecting Your Small Business: Multi-Factor Authentication