Department of Defense's Cybersecurity Maturity Model Certification (CMMC) and the CMMC Accreditation Body

What is CMMC?

Third-party assessment of a contractor’s cybersecurity maturity based on the CMMC model.

Targeted to be in 10 initial “pathfinder” contracts in September 2020.

Will be integrated into additional contracts over a 5-year period.

By 2026, CMMC requirements will be in all DoD contracts.

CYBERSECURITY MATURITY MODEL CERTIFICATION ACCREDITATION BODY

How did CMMC Begin?

“If we were doing all the necessary security controls, we wouldn’t be getting exfiltrated to the level that we are.”

*Katie Arrington, CISO for Assistant Sec. Def.
for Def. Acquisition, June 20, 2019*

Why is CMMC Necessary?

Cybersecurity incidents negatively impact US business

- **Cybersecurity incidents increase contract delivery costs, lengthen delivery timelines, and jeopardize business integrity:**
- Malicious cyber activity cost the US economy between $57 billion and $109 billion in 2016 (The Council of Economic Advisors)
- $3 trillion in annual cybercrime losses in 2015, estimated to grow to $6 Trillion by 2021 (Cybersecurity Ventures)
- The average data breach costs $3.9 Million worldwide, $8.9 Million in USA (Ponemon Institute)

Why is CMMC Necessary?

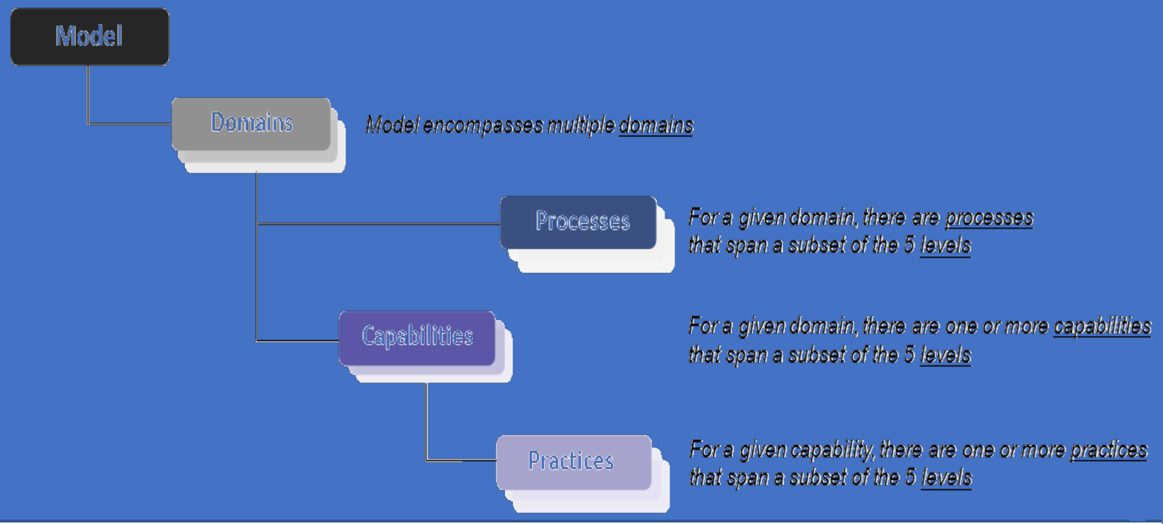
Cybersecurity is national security

- US electrical grid nearly taken offline
- Office of Personnel Management breached
- Military and industrial intellectual property stolen

Chengdu J-20 vs F-35

What is the CMMC Model?

- The CMMC Model defines a framework for measuring cybersecurity maturity with five maturity levels and aligns a set of policies and practices with the type and sensitivity of information to be protected and the associated range of threats
- Based on best practices from multiple cybersecurity standards, frameworks, and other references
- Focuses on protecting FCI and CUI



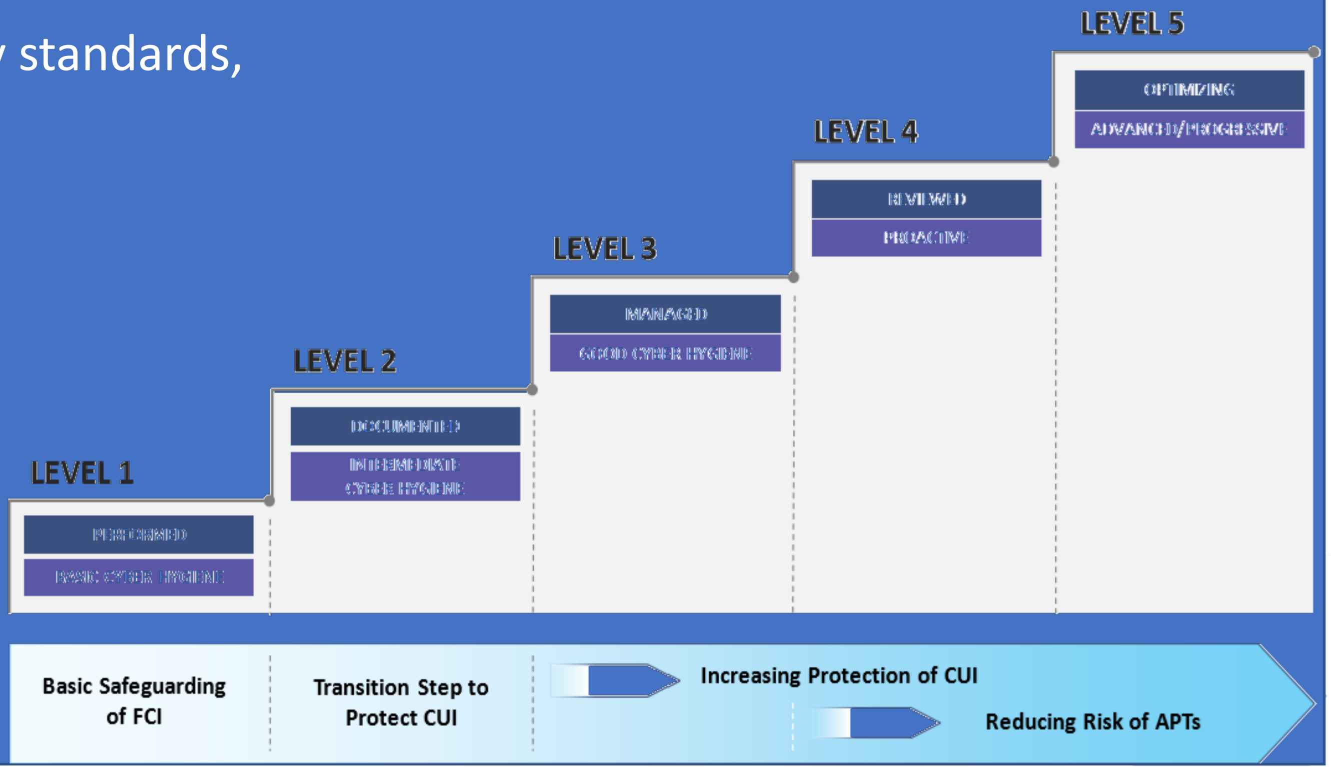
Model

Domains — *Model encompasses multiple domains*

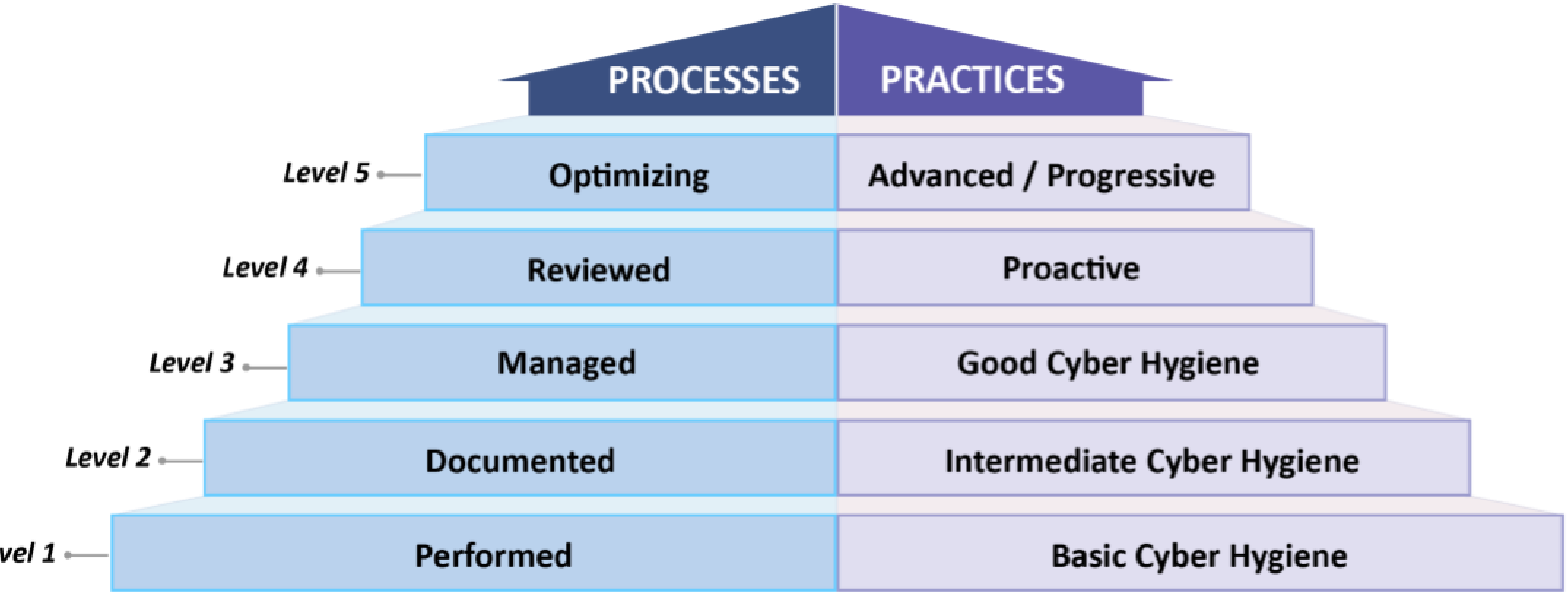
Processes — *For a given domain, there are processes that span a subset of the 5 levels*

Capabilities — *For a given domain, there are one or more capabilities that span a subset of the 5 levels*

Practices — *For a given capability, there are one or more practices that span a subset of the 5 levels*



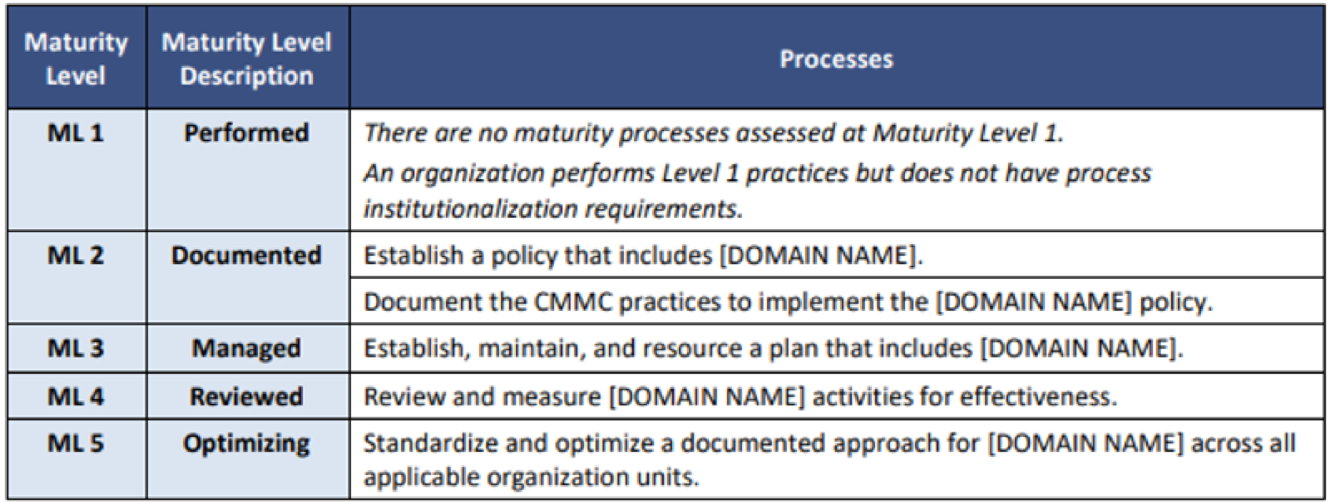
….with a number of Processes and Practices….



	PROCESSES	PRACTICES
Level 5	Optimizing	Advanced / Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
vel 1	Performed	Basic Cyber Hygiene

…to increase overall Cybersecurity Maturity

- There are Five Maturity Levels in CMMC (balances process, technology and maturity)
- Movement between levels require documented processes; these must be in place and verified
  - The documentation process frequently identifies areas where costs can be saved, and efficiencies realized.
  - This can take significant time to implement and, although CMMC requirements may not apply to them now, organizations should begin creating appropriate documentation now.
- Each level builds on the prior level
- CMMC Level 3 is required for contracts which include Controlled Unclassified Information



Maturity Level	Maturity Level Description	Processes
ML 1	**Performed**	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	**Documented**	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	**Managed**	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	**Reviewed**	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	**Optimizing**	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

Why Install the Accreditation Body?

- DoD asked industry to create a nonprofit, corporation-agnostic organization and the CMMC-AB was formed in January 2020.
- CMMC-AB is responsible for creating the CMMC Ecosystem, including:
  - Clarify the CMMC Standard (implementing the CMMC Model created by DoD)
  - Developing CMMC-related Testing and Accreditation Requirements
  - Licensing Training Organizations and Curriculum
  - Licensing Trainers
  - Licensing Certified 3rd Party Assessment Organizations ("C3PAOs")
  - Licensing Assessors
  - Issuing Certificates to Organizations Seeking Certification

https://www.cmmcab.org/

What is the CMMC Accreditation Body?

- Registered as a non-stock corporation in Maryland
- Consists of an all-volunteer Board Directors
- Directors are diverse (small business to large, some with govt experience)
- Directors serve as individuals and not representatives of their parent organizations

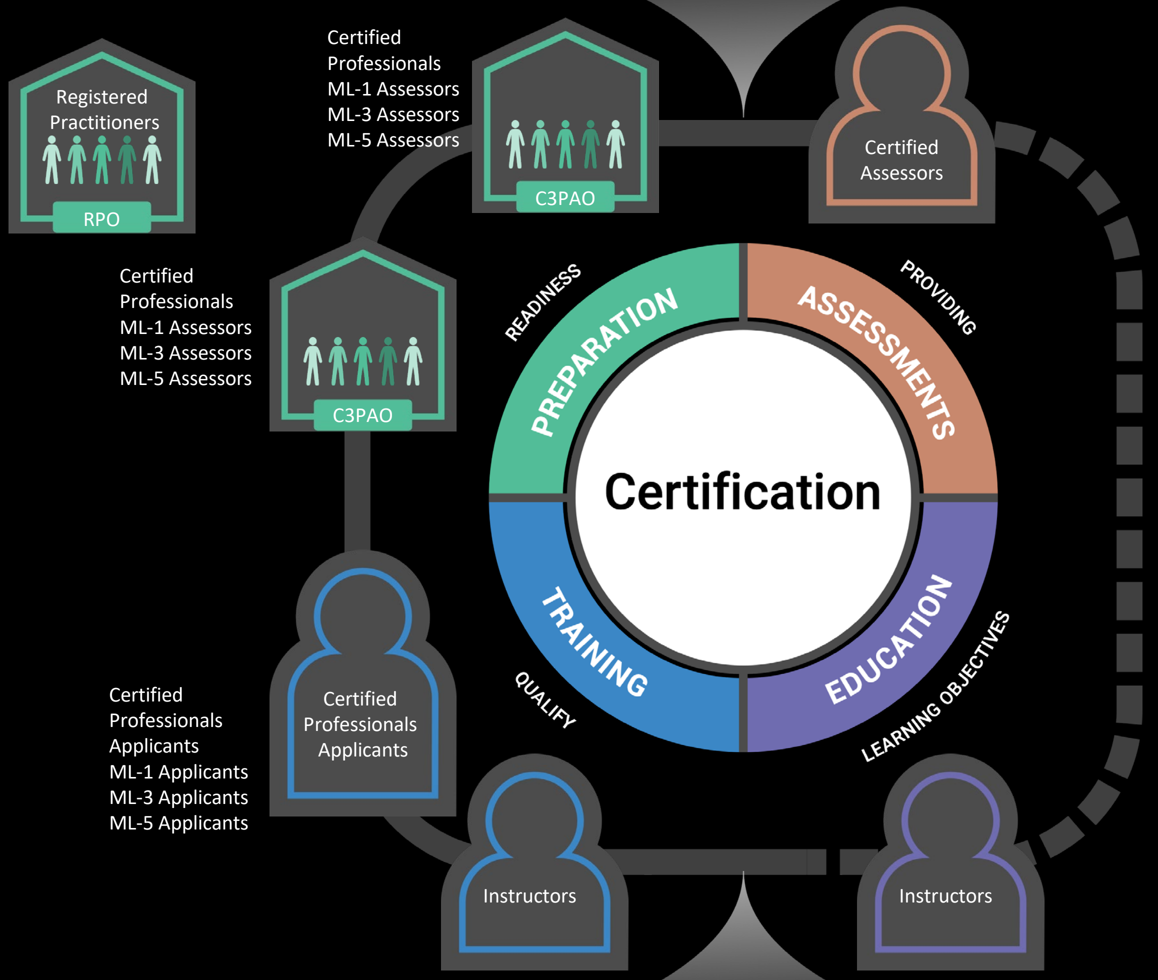
- Board founded on strong ethics and mission-focus
  - Directors *cannot* be individual assessors nor affiliated with a C3PAO
  - All Directors are subject to a strict Conflict of Interest Policy

CMMC-AB Main Focus: Operationalize the training, accreditation and certification aspects of the CMMC model and standard

CMMC-AB's ECOSYSTEM OF SUPPORT

Securing Our Nation's Supply Chain

OSC - Organizations Seeking Certification



Registered Practitioners

RPO

Certified Professionals
ML-1 Assessors
ML-3 Assessors
ML-5 Assessors

C3PAO

Certified Assessors

Certified Professionals
ML-1 Assessors
ML-3 Assessors
ML-5 Assessors

C3PAO

READINESS

PREPARATION

ASSESSMENTS

PROVIDING

Certification

TRAINING

QUALIFY

EDUCATION

LEARNING OBJECTIVES

Certified Professionals Applicants
ML-1 Applicants
ML-3 Applicants
ML-5 Applicants

Certified Professionals Applicants

Instructors

Instructors

DELIVERING

Trust

Contract Go/No Go Decisions

5 Year Rollout

Cyber Culture

TO

Organizations Seeking Certifications

FOR

DoD

International

Gov't Agencies

Defense Supply Chain

Licensed Training Providers

LTP

Master Instructors

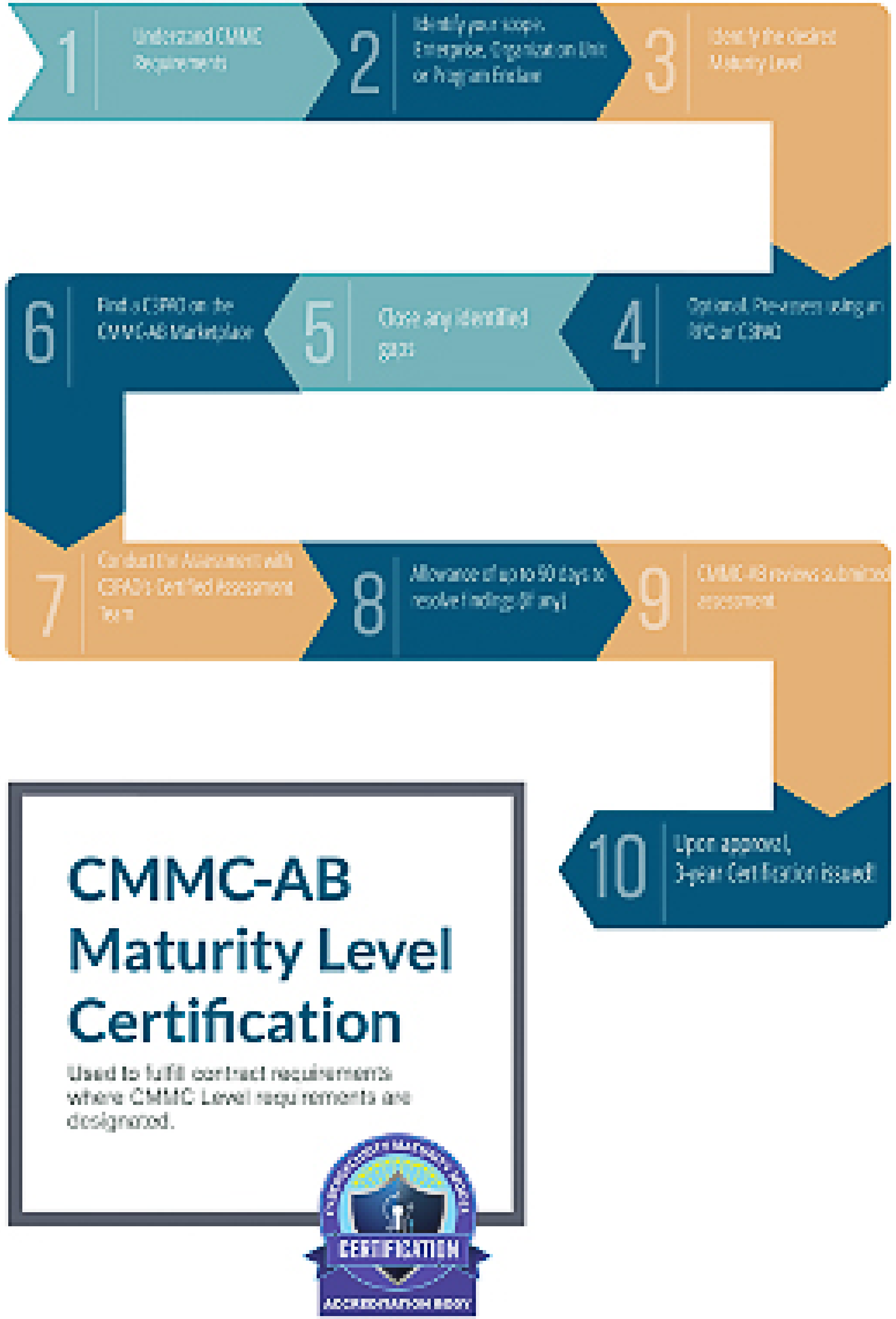
Licensed Publishing Partners

LPP

Universities | Community Colleges | Private Training Orgs

Organizations Seeking Certification (OSC)

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



1 Understand CMMC Requirements

2 Identify your scope: Enterprise, Organization Unit or Program Enclave

3 Identify the desired Maturity Level

4 Optional: Pre-assess using an RPO or C3PAO

5 Close any identified gaps

6 Find a C3PAO on the CMMC-AB Marketplace

7 Conduct the Assessment with C3PAO's Certified Assessment Team

8 Allowance of up to 90 days to resolve findings (if any)

9 CMMC-AB reviews submitted assessment

10 Upon approval, 3-year Certification issued!

CMMC-AB Maturity Level Certification

Used to fulfill contract requirements where CMMC Level requirements are designated.