Fortalice®

Cybersecurity Maturity Model Certification (CMMC) Overview

Topics

- CMMC Overview - Why is it Important?
- CMMC Levels
- CMMC Compliance
- CMMC Timeline*
- CMMC Readiness - What is required?
- System Security Plan Tips
- POAM Development and Completion Tips
- How Fortalice Can Help
- References

What is CMMC and Why is it Important?

What is CMMC?:The Capability Maturity Model Certification (CMMC) is a framework that has multiple maturity levels ranging from **Basic Cybersecurity Hygiene** to **Advanced/Progressive. Focus today: Level 3- Good Cyber Hygiene**

Why is it important?:

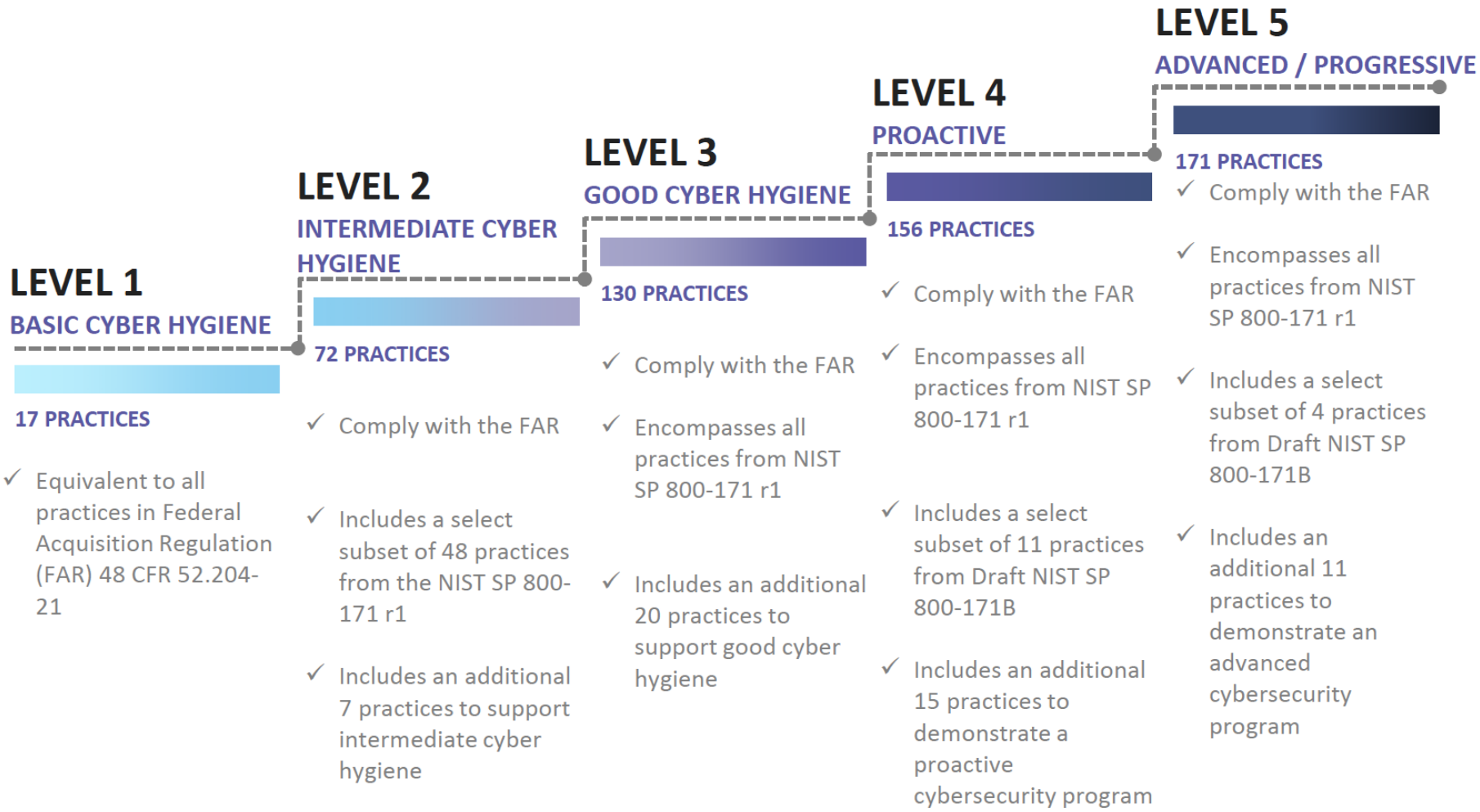
- The Department of Defense (DoD) intends to enhance the cybersecurity posture of the Defense Industrial Base (DIB)
  - Builds on the DFARS 52.204.21 and NIST 800-171
- Serves as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place.
- Intentional move **from self-certification** to **formal certification by approved assessor (C3PAO) to** analyze the company and assign a maturity level based on the state of its cybersecurity program.
  - Protects Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) data that resides on the Department's industry partners' networks.

REQUIRED by DOD: Applies to all defense contractors that handle CUI and/or FCI data. Includes prime and subs.*

Level 3: PROVE MATURITY OF A PROCESS; PROVIDE EVIDENCE (Policies, process, and documentation)

COTS- Out of scope* unless system manages, stores, transmits, collects, releases, and/or supports CUI/FCI data in some capacity

★ CMMC Levels


LEVEL 1
BASIC CYBER HYGIENE
17 PRACTICES
✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21
LEVEL 2
INTERMEDIATE CYBER HYGIENE
72 PRACTICES
✓ Comply with the FAR
✓ Includes a select subset of 48 practices from the NIST SP 800-171 r1
✓ Includes an additional 7 practices to support intermediate cyber hygiene
LEVEL 3
GOOD CYBER HYGIENE
130 PRACTICES
✓ Comply with the FAR
✓ Encompasses all practices from NIST SP 800-171 r1
✓ Includes an additional 20 practices to support good cyber hygiene
LEVEL 4
PROACTIVE
156 PRACTICES
✓ Comply with the FAR
✓ Encompasses all practices from NIST SP 800-171 r1
✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
✓ Includes an additional 15 practices to demonstrate a proactive cybersecurity program
LEVEL 5
ADVANCED / PROGRESSIVE
171 PRACTICES
✓ Comply with the FAR
✓ Encompasses all practices from NIST SP 800-171 r1
✓ Includes a select subset of 4 practices from Draft NIST SP 800-171B
✓ Includes an additional 11 practices to demonstrate an advanced cybersecurity program

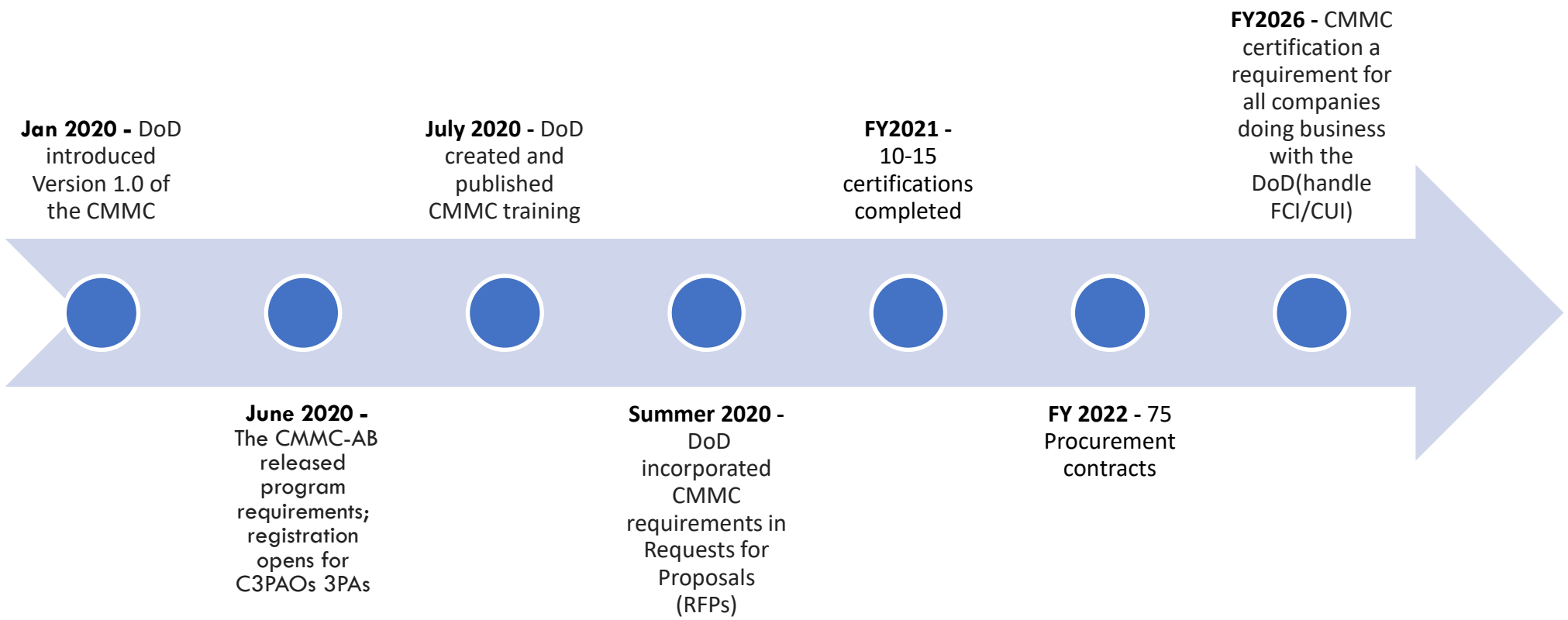
CMMC Level 3: NIST 800-171 Plus Additional Controls

Access Control	Identification and Authentication	Recovery
Asset Management	Incident Response	Risk Assessment
Awareness and Training	Maintenance	Security Assessment
Audit and Accountability	Media Protection	Situational Awareness
Configuration Management	Personnel Security	System and Communications Protection
Cybersecurity Governance	Physical Protection	System and Information Integrity

- 15 domains are based on cybersecurity "best practice" from NIST 800-171
- 20 additional controls
- Net New: AM, RE, SA
- Domains are comprised of capabilities

	Access Control	Asset Management	Audit and Accountability	Awareness and Training	Configuration Management	Cybersecurity Governance	Identity and Authorization	Incident Response	Maintenance	Media Protection	Personnel Security	Physical Protection	Recovery	Risk Management	Security Assessment	Situational Awareness	System & Comms Protection	Systems and Info Integrity
Capabilities	5	4	8	4	5	4	2	9	2	8	2	5	2	7	6	4	3	5
Practices	30	19	27	16	21	21	17	41	9	13	5	17	8	36	15	17	45	13
Level 1	5	2	2	0	2	2	2	3	1	1	2	4	0	0	1	2	2	4
Level 2	9	5	9	4	8	6	1	15	5	6	2	10	3	9	6	2	10	5
Level 3	11	7	7	5	4	4	9	7	2	5	0	3	3	6	2	3	13	0
Level 4	5	5	7	7	6	9	2	9	1	0	1	0	2	15	5	7	12	2
Level 5	0	0	2	0	1	0	3	7	0	1	0	0	0	6	1	3	8	2

CMMC Rollout



CMMC – Roles and Responsibilities

Role	Description
Assessor	Completed background training and approved to certify
C3PAO	Entity with at least two (2) formal assessors
CMMC Accreditation Board (AB)	Non-profit accreditation body Provides oversight Issues certification
Organization Seeking Certification (OSC)	Seeking formal maturity level designation

CMMC Accreditation Body

- The CMMC Accreditation Body (AB), a non-profit, independent organization, will accredit CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors.
- The CMMC AB will provide the requisite information and updates on its website (www.cmmcab.org).
- The CMMC AB plans to establish a CMMC Marketplace that will include a list of approved Certified Third-Party CMMC Audit Firms (C3PAOs) as well as other information.
- After the CMMC Marketplace is established, DIB companies will be able to select one of the approved C3PAOs and schedule a CMMC assessment for a specific level.

Main Deliverables

System Security Plan (SSP)

- System Overview
- Description of System
- System Environment
- Requirements - Implemented, To be implemented, Not Applicable
- DO NOT SEND TO THE DOD

Plan of Actions & Milestones (POAM)

- Lists all controls to be implemented
- Description
- Mitigation Plan
- Milestone Date
- Implementation date
- Accountable Resource(s)
- ~~Strikethrough all controls met on POAM~~
- **Level 3 Certification= NO POAM**
- DO NOT SEND TO THE DOD

Interim Period: Self-Assessments

- After 11/30/2020, DoD contracts may require contractors to register for self-assessment(* applicable to CUI and DFARS 7012 clause)
- Self Assessment comprised of 800-171 control status
- Submitted through SPRS
- **Contractors should be prepared and ready to submit in case contracts require this**

CMMC Readiness – Pre-Assessment

In preparation for CMMC Level 3 compliance, an organization should conduct a readiness assessment.
Readiness considerations:

- Evaluation based on 17(previously 18) domains and best practice
- Review of information security documents and policies
- Review System Security Plan (SSP) and perform gap analysis against industry best practice
- Review Plan of Action and Milestones (POAM); update as necessary. Goal is to mitigate all open items on the POAM.
- Verify control implementation and identify supporting documentation per process/control
- Consider engaging a third party to evaluate your organization's cyber maturity if you think you need additional guidance

How Fortalice Can Help

- CMMC Readiness Assessments
  - Fortalice will perform a pre-assessment, which includes:
    - Conducting interviews to gather information on current state
    - Reviewing existing documentation
      - SSP
      - POAM
    - Providing recommendations to achieve desired CMMC level

- Planned Action and Milestones (POAM) Review
  - Fortalice will identify tasks needing to be accomplished by detailing resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
- Roadmap for POAM completion
- Provide resources to remediate any findings and help execute the roadmap

About Fortalice

- Nationally Certified Woman-Owned Small Business
- DUNS #07938-3000
- Top Secret Facility Clearance (CAGE: 7431)
- GSA IT Schedule 70; Contract Holder #Contract Number: 47QTCA19D001C
- CISSP, OSCP, CEH, CCNA, and SANS Trained Cyber Experts
- Industry-leading Red Teaming Capability
- Proven success in Digital Forensics and Incident Response

- Locations:
  - Northern Virginia
  - Maryland
  - Washington, D.C.
  - Charlotte, NC
  - EMEA (based in United Kingdom)

SBA WOSB
Woman Owned Small Business
Certified WBENC Women's Business Enterprise
Certified

2020 CYBERCRIME MAGAZINE HOT 150 CYBERSECURITY COMPANIES

★ Commercial and Government Service Offerings

To date, Fortalice has successfully completed more than 300 commercial and government projects.

Offensive Cyber Ops	Network Defense	Incident Response	Cyber Risk	OSINT	Government
★ Objective-Based Ethical Hacking/Red Teaming	★ Defensive Security	★ Digital Forensics	★ Cyber Risk Posture Assessments	★ Attribution	★ Policies and Procedures
★ Collaborative Purple Teaming	★ Security Posture Review	★ Incident Runbook Development	★ Pre-Audit Compliance Assessments (PCI, SOC1/SOC2, HIPAA, HITRUST, CIS, CMMC Readiness)	★ Incident Support	★ Compliance Reviews
★ Penetration Testing	★ Threat Hunting	★ Incident Response Strategy	★ DoD and Federal Acquisition Reg. Assessments (NIST-171)	★ Personal Executive Protection	★ Strategic Communications, Outreach, & Engagement
★ IoT/Device Testing	★ Independent Product Evaluation	★ Tabletop Exercises (TTX)	★ M&A Advisory Services	★ Law Enforcement Interaction	★ White Glove Consulting and Strategic Counsel to Senior Leaders
★ Vulnerability Assessments	★ Security Lab		★ BCP/DR	★ Litigation Support	★ IR Support
	★ Public Key Infrastructure (PKI) services			★ Deep Web monitoring and analysis	★ Classified National Security System Engineering
	★ Fraud Detection/Insider Threat			★ Digital Forensics	★ Offensive Cyber Ops

References

- Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification

  https://www.acq.osd.mil/cmmc/faq.html
- C3PAOS (www.cmmcab.org)
- Cybersecurity Maturity Model Certification (CMMC) https://www.acq.osd.mil/cmmc/docs/cmmc-overview-brief-30aug19.pdf
- National Defense Information Sharing and Analysis Center (NDISAC) https://ndisac.org/
- The ND ISAC cyber assist website is https://ndisac.org/dibscc/cyberassist/ It was originally set up to share best practices across the DIB but covers compliance as well. There is now a CMMC subsection to the site.