We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

What You Need to Know About New CMMC Requirements

March 12, 2025

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Objectives

Key changes in the CMMC framework.

How these changes impact your organization.

The expected implementation timeline.

Strategies to prepare your team and infrastructure for the new standards.

What's Happening?

After a nearly 3-year delay in rulemaking, Defense Industrial Base contractors will need to comply with new data protection requirements in order to do business with the Department of Defense (DoD)

You may begin to see contractual requirements rolled out as soon as the next two quarters, but a phased roll out could take up to three years

It's important to begin preparation NOW as it could take up to a year to comply with the requirements

Helping understand the business risk will help with priority

What is CMMC?

- DoD Cybersecurity Maturity Model Certification (CMMC) is a DoD program built to protect the defense industrial base (DIB), DoD Contractors, Federal Contract Information (FCI), and Controlled Unclassified Information (CUI)
- The CMMC Ecosystem is administered by Cyber-AB (Accreditation Body), a non-profit appointed by DoD
- Final Rule final rule for the CMMC was published to the Federal Register, with the effective date of December 16, 2024.

Understanding: FCI and CUI

What is Federal Contract Information (FCI)?	• Information not intended for public release
What is Controlled Unclassified Information (CUI)?	• Information that must be protected

Understanding: CUI

Executive Order 13556 (2010) required Executive Agencies to establish **safeguarding** and **dissemination** controls.

National Archives and Records Administration is the Executive Agent overseeing the CUI program.

50+ categories of CUI defined.

Dissemination controls dictates compliance.

Department of Defense has a separate CUI registry for DoD specific guidance.

Polling Question

How prepared is your organization for CMMC Level 2 compliance?

- 100%
- 75%
- 50%
- Less than 50%

Understanding: DFARS

Defense Federal Acquisition Regulation Supplement

Defines federal contracting requirements

- Compliance with NIST 800-171 for DoD contractors began in 2017
- Clauses are invoked as a prerequisite to bid / contract
- Flow-down provisions are required for all subcontractors
- Must register in the Supplier Performance Risk System (SPRS)
- Supplier Performance Risk System (disa.mil)

CUI – Related DFARS

- 252.204-7000 Disclosure of Information. (osd.mil)

DFARS Clauses – Final Rulemaking

DFARS 7012

- Safeguarding Covered Defense Information and Cyber Incident Reporting. Requires NIST SP 800-171. Includes flow-downs.

DFARS 7019

- Notice of NIST SP 800-171 DoD Assessment Requirements.

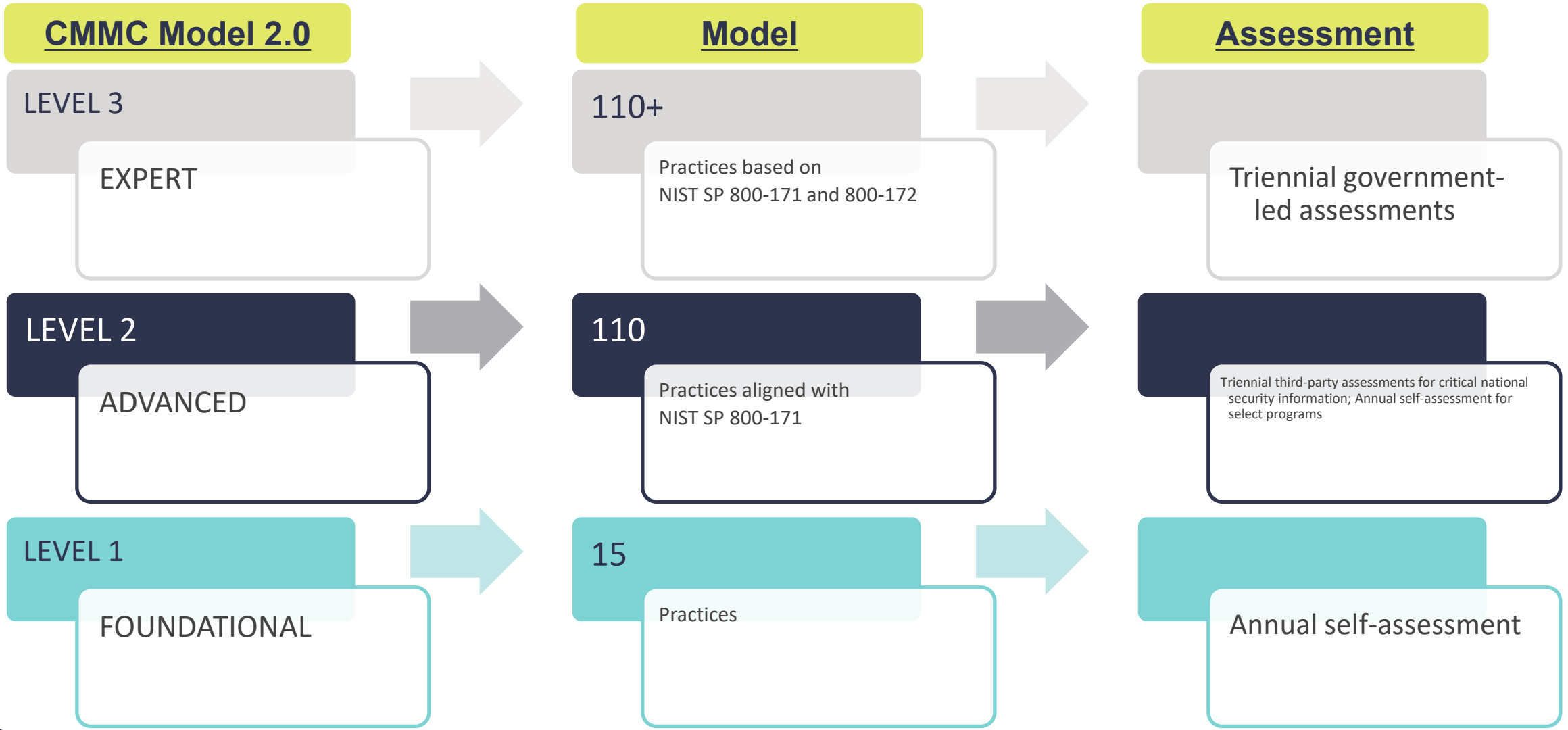
DFARS 7020

- NIST SP 800-171 DoD Assessment Requirements.

DFARS 7021

- Cybersecurity Maturity Model Certification Requirement. Flow-downs.

CMMC Levels



Point of Emphasis: NIST SP800-171

110 required controls, Over 300 sub-control attributes

Requirements are derived from NIST SP800-53 controls

Focus of an organization’s compliance can be:

- Enterprise-wide
- Application Focused
- General Support System (network)
- Carve-out / Enclave
- External Service Provider

CMMC Roles

- Organizations Seeking Certification (OSCs), also referenced as Organizations Seeking Assessment (OSAs)
- Registered Practitioner Organizations (RPOs)
- Certified Third Party Assessment Organizations (C3PAOs)
  - Organizations consulting with an OSC regarding the implementation cannot also perform the assessment for the same organization
- Licensed Training Professionals (LTP)
- Licensed Publishing Partner (LPP)

The Cyber-AB Ecosystem

- 63 C3PAO's and 337 RPO's in the Marketplace as of March 3rd, 2025

- Cyber-AB CMMC Resources
  - Marketplace
  - Monthly townhalls
  - OSC, RPO, and C3PAO Registration

- DoD CIO CMMC resources
  - https://dodcio.defense.gov/CMMC/Resources-Documentation/

How to Prepare

Understand fundamental aspects

Prioritize how to implement “significant controls”

Derive a Self-Assessment Score against the 110 requirements which will be documented in the Supplier Performance Risk System (SPRS)

Organizations Seeking Certification (OSCs) must have a documented System Security Plan

Develop and update Plan of Action and Milestones (POAM)

Implementation Requirements

Understand your Requirements

- Bid requirements if direct
- Register in SPRS
- Flow-downs from customers and sub-contractors

Data Governance / Discovery

- Where is CUI and how does it flow?

Determine scope of system(s)

Are systems capable of conforming without redesign?

Scoping

Controlling the flow of CUI and FCI is paramount

CMMC level 1, 2, and 3 scoping guides released by the DoD CIO in September of 2024

Understanding of Asset Categories

- CUI Assets
- Security Protection Assets
- Contractor Risk Managed Assets
- Specialized Assets
- Out of Scope Assets – prepare justification

Preparing for Assessment

Conduct Basic Self-Assessment against 110 Requirements

Be prepared to produce the following:

- SP 800-171 Assessment Score
- System Security Plan
- Plans of Action and Milestones
  - 180 Day period for remediation
  - Justification for areas of non-conformance
  - Mitigating controls

Examples are available on the NIST SP 800-171 Rev. 2 Site

Assessment

- CMMC level 1, 2, and 3 Assessment guides released by the DoD CIO in September of 2024

- Control vs Objective
  - Example: AC.L2-3.1.1 – Authorized Access Control includes six specific assessment objectives from NIST SP 800-171A

- Your assessment may include multiple points of assessment

What's Next?

Key Events	Timeline
CMMC Final Rule	December 16, 2024
SPRS Self Assessment for Level 2 available	February 28, 2025
Publication of CMMC acquisition rule	Expected mid-2025, implementation 60 days after publication
Phase 1 – Initial Implementation	If required, solicitations will require level 1 or 2 Self-Assessment
Phase 2 – 12 months after phase 1 start	If required, solicitations will require level 2 Certification
Phase 3 – 24 months after phase 1 start	If required, solicitations will require level 3 Certification
Phase 4 – 36 months after phase 1 start	All solicitations will require the applicable level of CMMC requirements

Source: https://dodcio.defense.gov/

Certification Process – High Level

Scoping/Building Secure IT Environment

What DoD contracts do we have currently?

Do we receive FCI or CUI?

Must have CMMC compliant environment and document a System Security Plan

Supplier Performance Risk System

Conduct self assessment for CMMC at appropriate level and enter SPRS score

Apply for Assessment

Register in Cyber-AB locate an C3PAO

Assessment

Must pass C3PAO assessment with Plan of action and milestones address with 180 days

Maintain Certification

- Annual self assessment
- Triannual re-assessment

Thank you!

David Scaffido
Principal
david.scaffido@CLAconnect.com

David Nowacki
Controls Consultant Manager
david.nowacki@CLAconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS