It’s Here!

Cybersecurity Maturity Model Certification (CMMC)

32 CFR Part 170

CMMC Solutions

forvis mazars

Forvis Mazars Among First *Authorized* CMMC Third-Party Assessor Organization (C3PAO)

Forvis Mazars is the sixth Authorized C3PAO and has performed multiple JVSA assessments for contractors of all size and industry. With an experienced CMMC Solutions team, our firm can provide support with the following:

- NIST 800-171 Joint Surveillance Voluntary Assessments
- CMMC Compliance Program Development
- Gap and Mock Assessments
- System Security Plan Development
- POAM Development and Remediation Advisory
- Technical Assessment and Penetration Testing

Agenda

1. Introductions
2. Overview of the CMMC Program
3. Highlights of the 32 CFR 170 FINAL Rule
4. Top Challenges and Cost Considerations
5. Walk Through the Assessment Process
6. What's Next?

Panelists

Tom Tollerton, CCA
Principal
Forvis Mazars

Stacy Bostjanick
DCIO(CS),
DIB CS Division Chief

Eric Crusius

Partner
Holland & Knight, LLP

Bill Walter

Managing Director
Forvis Mazars

OPENING COMMENTS

Cybersecurity Maturity Model Certification (CMMC Program)

Need

CMMC is the cybersecurity compliance framework currently applicable to organizations with contracts with the U.S. Department of Defense.

- Defense Industrial Base (DIB) estimated at **over 200,000** organizations
- Contractors are in a wide variety of industries

Scope

Scope of the framework is to protect Controlled Unclassified Information (CUI).

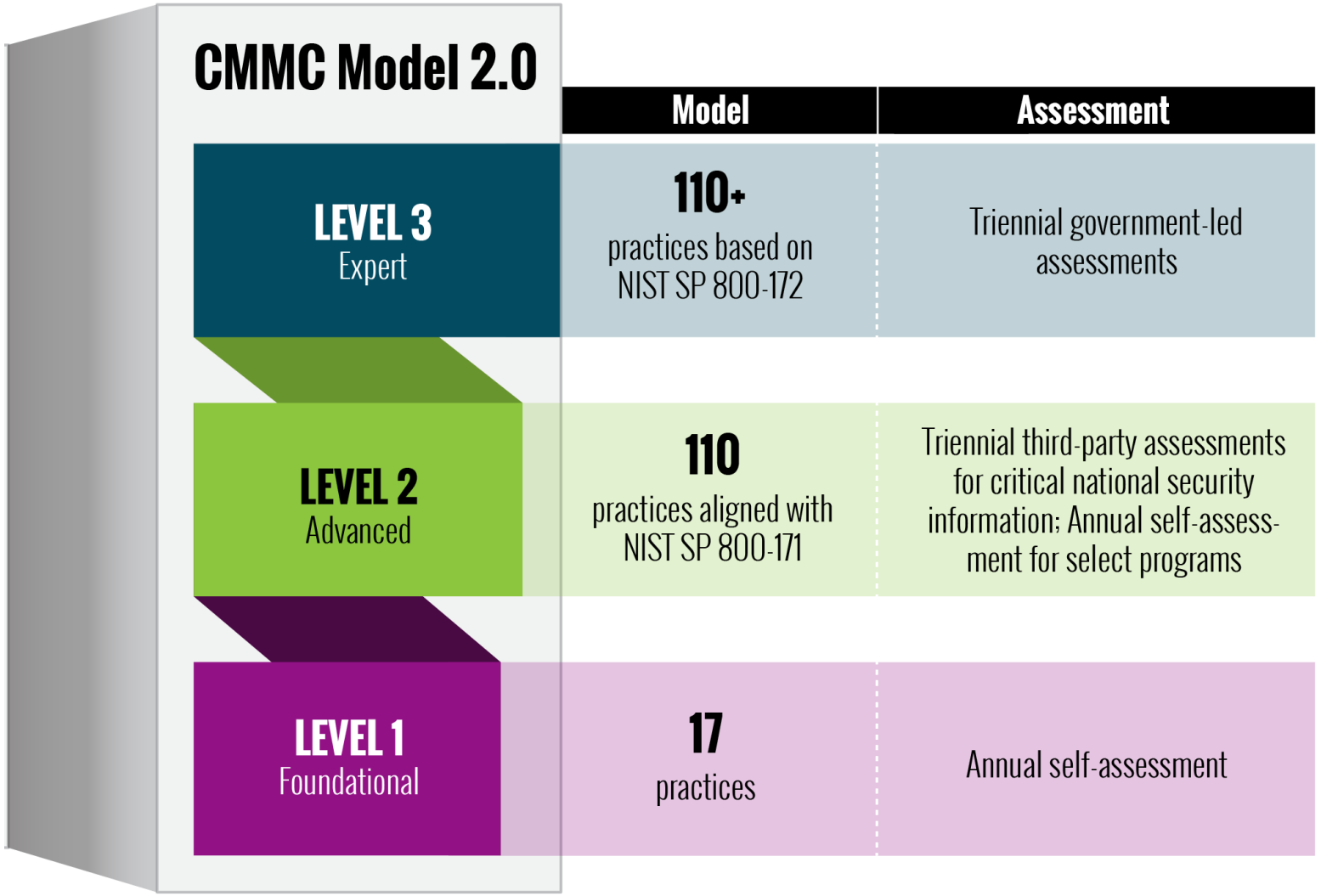
- Extremely broad categories of information. Information sensitive to DoD but doesn't rise to the level of "classified."
- Significant ambiguity about responsibilities for defining and marking CUI.

Ecosystem

The CMMC PMO within the Department of Defense manages the CMMC Program:

- Has assigned accreditation and credentialling of assessors and assessment organizations to the private sector Accreditation Body (Cyber AB).
- Assessments are performed by credentialed assessment companies called Certified 3rd Party Assessor Organizations
- Currently **60** Authorized C3PAOs, with over hundred in the queue for Authorization.

CMMC Program Levels



Level 1

- Contractors handling Federal Contract Information (FCI)
- Represents "Foundational" security practices

Level 2

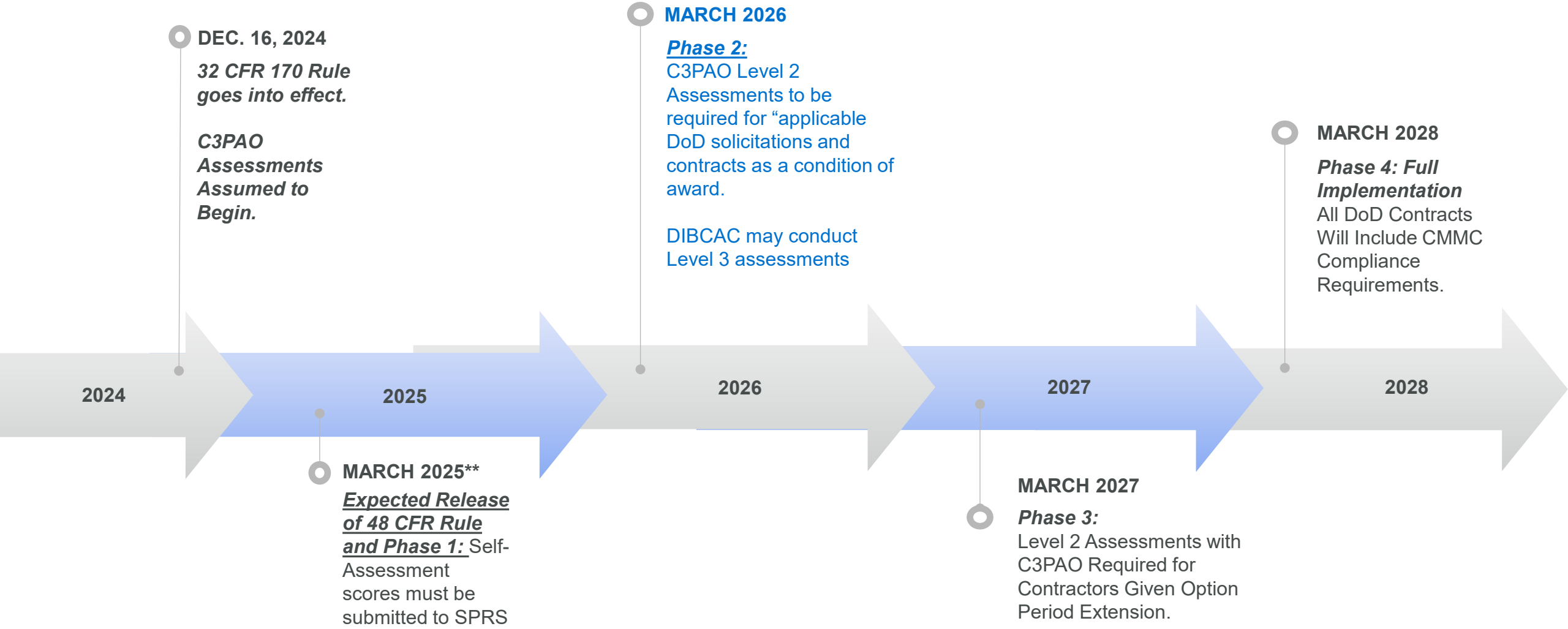
- Contractors processing, storing, or handling CUI as part of a DoD contract
- Represents "Advanced" security practices

Level 3

- Applicable to contractors processing, storing, or handling CUI associated with the most sensitive DoD programs

CMMC Rollout Timeline

The Final 32 CFR 170 and Proposed 48 CFR rules have laid out key milestones for the requirement of CMMC compliance.



DEC. 16, 2024

32 CFR 170 Rule goes into effect.

C3PAO Assessments Assumed to Begin.

MARCH 2025**

Expected Release of 48 CFR Rule and Phase 1: Self-Assessment scores must be submitted to SPRS

MARCH 2026

Phase 2:
C3PAO Level 2 Assessments to be required for "applicable DoD solicitations and contracts as a condition of award.

DIBCAC may conduct Level 3 assessments

MARCH 2027

Phase 3:
Level 2 Assessments with C3PAO Required for Contractors Given Option Period Extension.

MARCH 2028

Phase 4: Full Implementation
All DoD Contracts Will Include CMMC Compliance Requirements.

*****All dates assume March 2025 issuance of the 48 CFR rule.***

forvis mazars

Highlights of the 32 CFR Part 170 CMMC Rule

Joint Surveillance Voluntary Assessments (JSVAs) Convert to CMMC Level 2 Certifications. Assessments that were performed under the JSVA program with DCMA will convert to Level 2 certifications with a standard three year lifecycle, effective from the completion date of the assessment.

The JSVA program is now retired. DCMA has indicated that no more JSVAs will be scheduled through the rest of the year. Contractors needing a CMMC Level 2 certification will need to engage with a C3PAO directly in order to schedule and conduct the assessment. These are likely to begin at the end of 2024 or early 2025.

Revision 2 of NIST 800-171 Lives On…For Now. The aging version of the NIST 800-171 will continue to be used as the basis for CMMC assessments and certification at Level 2. Though revision 3 has been released, DoD has not incorporated the newer requirements into the CMMC program, but could in the future, using a class deviation from the rule.

CMMC Certifications Are Required Every Three Years. As expected CMMC certifications at Levels 1 and 2 carry a three year life cycle. For Level 2 certifications, the "off years" 2 and 3 will necessitate the contractor to "affirm" that they remain compliant will all requirements of their CMMC certification, including compliance with NIST 800-171 Rev. 2.

Highlights of the 32 CFR Part 170 CMMC Rule

Managed Service Providers (MSPs) may no longer be required to obtain a CMMC certification. Where MSPs have no direct access to CUI, a CMMC certification matching that of their customer will no longer be required. Instead, MSPs can provide a Shared Responsibility Matrix and be included in the scope of their customers CMMC assessment. External Service and Cloud Service Providers who do transmit, process or store CUI on behalf of a contractor will still be required to achieve the requisite certification level.

Endpoints Accessing Virtual Desktop Infrastructure (VDIs) From Outside the CUI Boundary May Not in Scope: Organizations using endpoints to access virtual desktops from outside environments where CUI is stored finally have clarity on the inclusion of those endpoints. The Final rule indicates that, if proper boundary segmentation requirements are met, those external endpoints are not in scope for the requirements of NIST 800-171.

DISCUSSION / QUESTIONS

Contact

Forvis Mazars

Tom Tollerton, CISSP, CMMC-CA
Principal
P: 704.367.7051
tom.tollerton@us.forvismazars.com