CMMC Preparations from a C3PAO: What to do NOW

Cybersecurity Maturity Model Certification (CMMC)

32 CFR Part 170

2025 Cyber Symposium

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?

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).

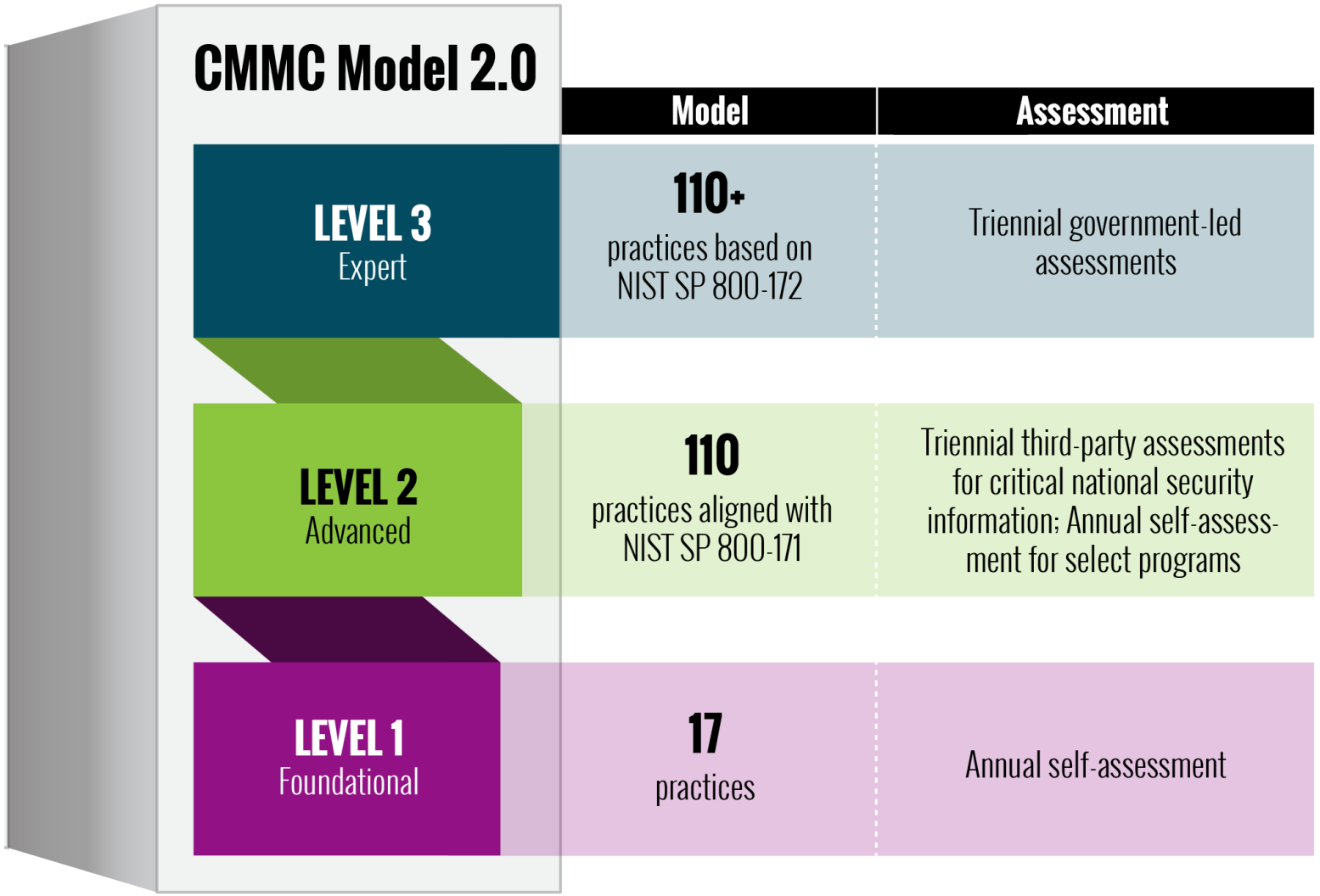
- Extremely broad categories of information. Information sensitive to DoD but doesn't rise to the level of "classified."
- Significant ambiguity about responsibilities for defining and marking CUI.

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 **81** 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

forvis mazars

Applicability Estimates (32 CFR Section 170.3(b))

Level	Small	Other Than Small	Total
1 Self-Assessment	103,010	36,191	139,201
2 Self-Assessment	2,961	1,039	4,000
2 C3PAO Assessment	**56,689**	**19,909**	**76,598**
3 DIBCAC Assessment	1,327	160	1,487
Total	163,987	57,299	221,286

Applicable to small businesses

Applicable to commercial products

Exclusions for COTS products and some room for staffing firms (depending upon nature of CUI handling).

Certifications last 3 years.

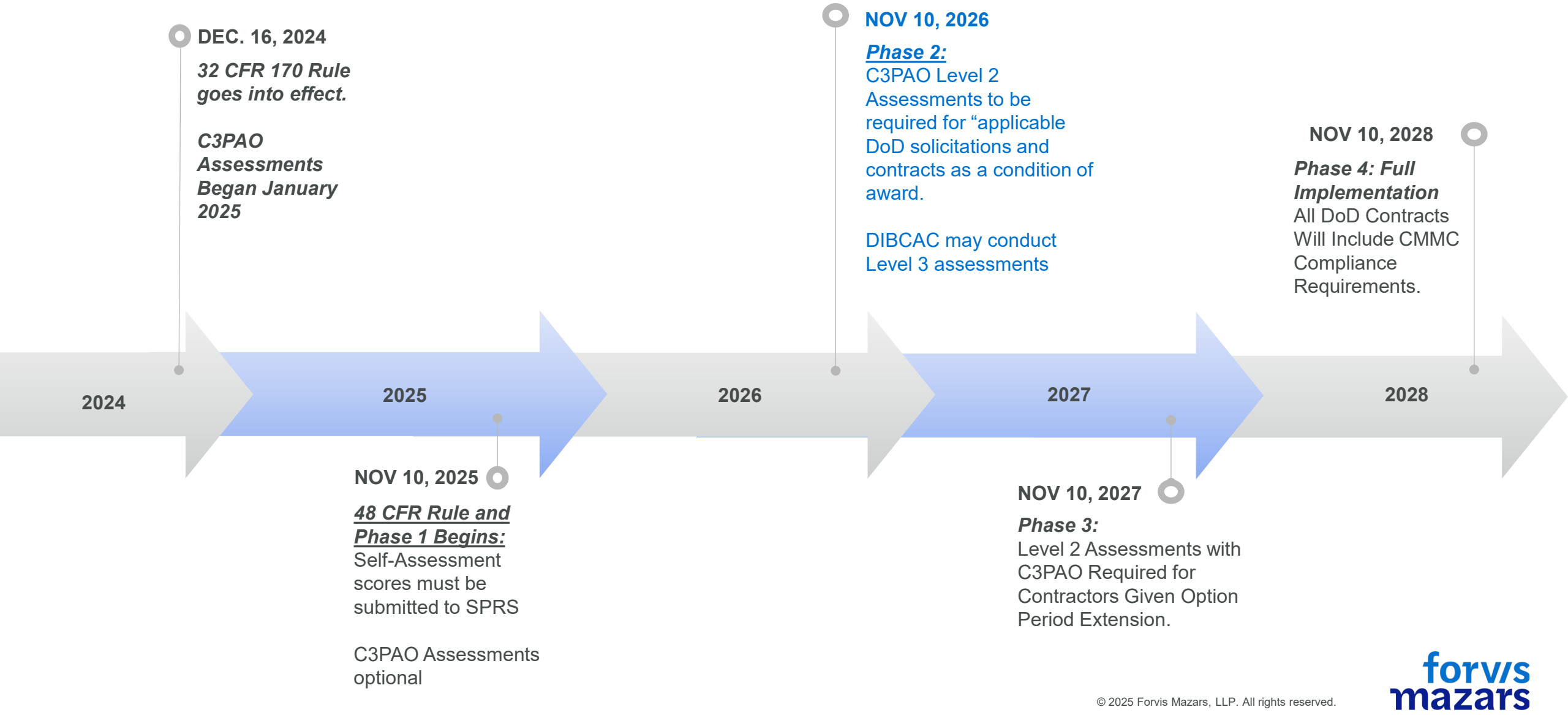
CMMC Assessment Logistics

What is the industry seeing?

- Some agencies already starting to reference CMMC in their solicitations.
- Large primes are pushing down requirements on their supply chains.
- Anticipated C3PAO (and individual assessor) bottleneck is real.
- CMMC Level 2 Certificate Template is Now Approved by DoD.
  - Cyber AB going to provide to C3PAOs to fill out and complete the Certificates and upload into eMASS
- Early assessments are likely successful – due to a focus on readiness - what about next year?

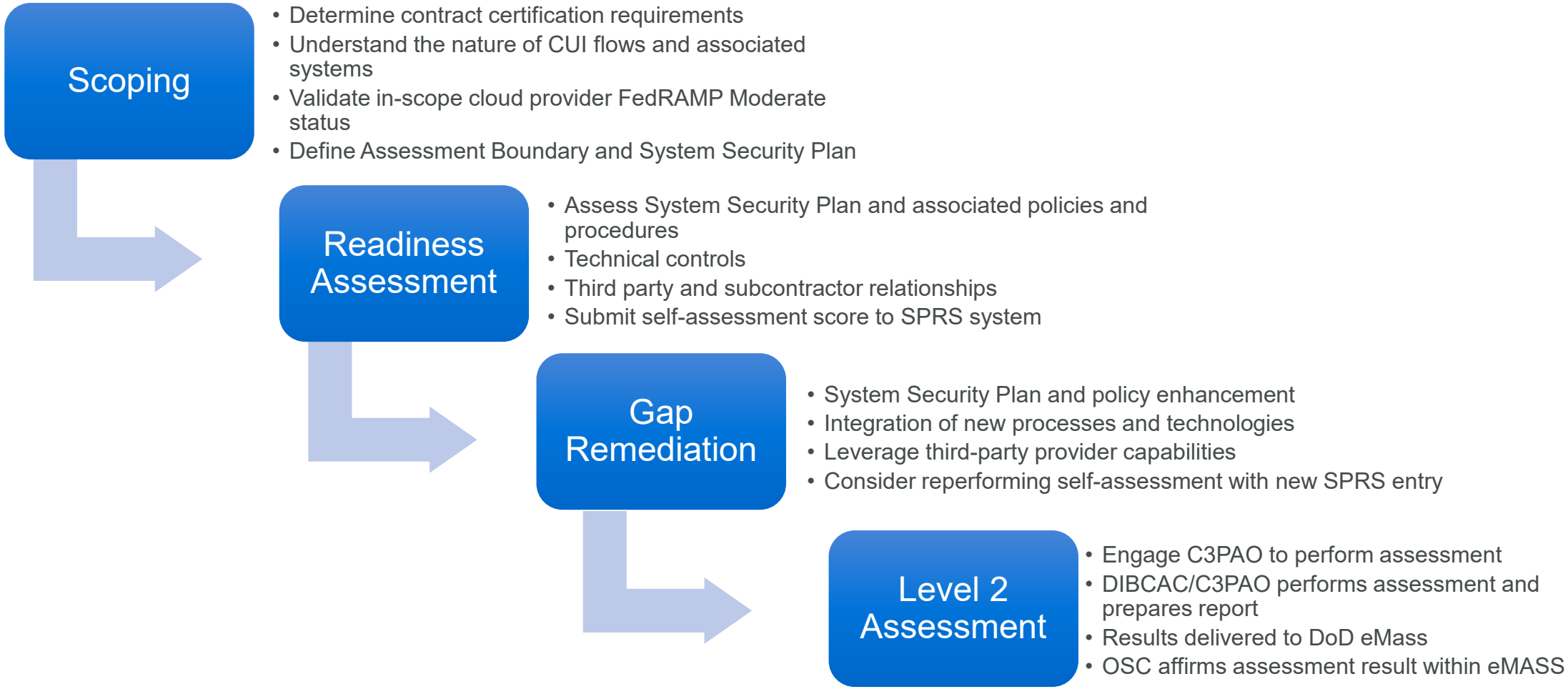
Updated CMMC Rollout Timeline

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



What to do NOW

What's Next: How to Prepare



CMMC L2 Scoping – Asset Categories

Asset Category	Asset Description	Contractor Requirements	CMMC Assessment Requirements
Assets that are in the CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	•Assets that process, store, or transmit CUI	•Document in the asset inventory •Document in the System Security Plan (SSP) •Document in the network diagram of the CMMC Assessment Scope •Prepare to be assessed against CMMC practices	•Assess against CMMC Practices, including SPAs
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		
Contractor Risk Managed Assets	•Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place •Assets are not required to be physically or logically separated from CUI assets	•Document in the asset inventory •Document in the SSP •Show these assets are managed using the contractor's risk-based security policies, procedures, and practices •Document in the network diagram of the CMMC Assessment Scope	•Review the SSP in accordance with practice CA.L2-3.12.4 •If appropriately documented, do not assess against other CMMC practices •If contractor's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited spot check to identify risks •The limited spot check(s) shall not materially increase the assessment duration nor the assessment cost •The limited spot check(s) will be within the defined assessment scope
Specialized Assets	•Assets that may or may not process, store, or transmit CUI •Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment		•Review the SSP in accordance with practice CA.L2-3.12.4 •Do not assess against other CMMC practices

forvis mazars

How to Craft and Effective SSP

- Identify control status
- Identify implementation responsibility and/or inheritance
- Identify additional documentation
- Provide clear description of how control is implemented
- Use NIST 800-171A to double-check SSP

3.1.3 Control the flow of CUI in accordance with approved authorizations.

Summary of NIST 800-171 Control & CMMC Practice Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: Firm Technology Services
Process Operator: Firm Technology Services
Occurrence: Ongoing
Location of Additional Documentation
Technology in Use:
Description of Control Implementation:

Effective SSP Ctd.

3.5.2 (IA.1.077) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Summary of NIST 800-171 Control & CMMC Practice Implementation
Implementation Status (check all that apply): ☒ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: Firm Technology Services
Process Operator: Firm Technology Services
Occurrence: Ongoing
Location of Additional Documentation: 61110 Identify & Access Management Policy, 65270 Network and Firewall Management
Technology in Use: Active Directory, CISCO ISE, Intune (Conditional Access)
Description of Control Implementation: **Users/Processes -** All users are required to authenticate using Active Directory credentials for both remote and wireless access (Cisco ISE with 802.1x + AD Auth). Access to the CUI virtual desktop enclave requires users to be on a managed device and belong to the dedicated "XYZ" or "ABC" Active Directory groups. **Devices -** All devices are authorized through domain enrollment and the use of a network access control solution (Cisco ISE). Devices are authenticated based upon machine certificates by a radius server prior to gaining access. Additionally, for remote VPN access. device certificates are examined by the VPN client for authorization prior to a remote connection being established. Specifically, for the CMMC enclave, conditional access policies further verify that the machine is a domain enrolled device prior to granting access.

3.5.2 (IA.1.077) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Summary of NIST 800-171 Control & CMMC Practice Implementation
Implementation Status (check all that apply): ☒ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Description of Control Implementation: Authentication is performed via active directory. All users are authenticated during system logon prior to gaining access to organizational systems.

Documentation – Helpful Tips

- All documentation should be version-controlled and reviewed/approved at least annually. This is most critical for the SSP and organizational policies.
- If enclave approach is utilized, leverage enterprise policies as much as possible.
- Policies should be communicated to relevant users annually. Consider implementing annual acknowledgement process.
- Answer assessors' questions for them. Use NIST 800-171A.
- Special attention on “defined” assessment objectives derived from NIST 800-171A

The Assessment Process

CMMC Assessment Logistics

Who are the Assessors?

Assessment Teams:

- TWO Lead CMMC Certified Assessors (CCAs)
- At least one CCA must be qualify and serve as a Lead CCA
- One additional CCA for Quality Assurance and Dispute Resolution
- CMMC Certified Professionals (CCPs) may support assessments by assessing CMMC Level 1 requirements

Cyber AB manages and maintains the CMMC ecosystem

Assessment Methods

NIST 800-171A (Assessment Guide) outlines three methods by which assessors can validate the implementation and operation of the control

Examine

- The process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities).

Interview

- The process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence.

Test

The process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior.

Interviewees – Helpful Tips

- Interviewees should be aware of the assessment purpose and scope.
- Familiarize POCs with control requirements prior to assessment.
- Familiarize POCs with specified documentation referenced in Security plan.
- Familiarize POCs with System Security Plan assessors will use to frame questions.
- Interviewees are typically managers or SMEs of their areas.

CMMC Assessment Logistics

The Scoring Methodology

32 CFR Part 170.24 defines how assessments are scored

- Each of the NIST 800-171 requirements is assigned a score of 1, 3, or 5
- Perfect score is 110
- Three outcomes are possible:
    1. Perfect 110: Final Level 2 Certificate of Compliance
    2. Score of 88 or above out of 110: Conditional Level 2 Certificate (POAMs, as permitted)
    3. Failed Assessment: No certificate is issued; final results still delivered to DoD.

CMMC Level 2 Assessment Discussion

We're done with a 110! What do we get?!

Basic Summary of Close-out Process Described in the CAP

- Initial assessment week close-out meeting held, informing OSC contacts of successful assessment and that all NIST 800-171 requirements are trending "MET."
- Lead CCA prepares finalized assessment results documentation and submits to QA CCA for review within the C3PAO.
- Final Out-brief meeting scheduled with the OSC to deliver Final results
- OSC provides C3PAO with artifact hashes
- C3PAO / Lead CCA prepares final assessment package for upload into eMASS.

CMMC L2 Certificate Achieved – Now What?

Potential Ways to Trip up After Certification is Achieved.

- **Failure to Monitor Changes to the Environment**
  - Major changes require new or re- assessment
- **Failure to Flow-Down / Integrate into Supply Chain Management**
- **Failure to Maintain Business as Usual (BAU) Operations**
  - CUI ingestion mechanisms / marking / placement
  - Ongoing training, vulnerability management controls
- **Failure to Conduct Accurate Annual Affirmation by Internal Leadership**
- **Failure to Start Considering NIST 800-171 Rev 3 Requirements – *They're Coming!***

DISCUSSION / QUESTIONS

Contact

Forvis Mazars

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

Alex Imani, CISSP, CMMC-CA
Senior Manager
alex.imani@us.forvismazars.com