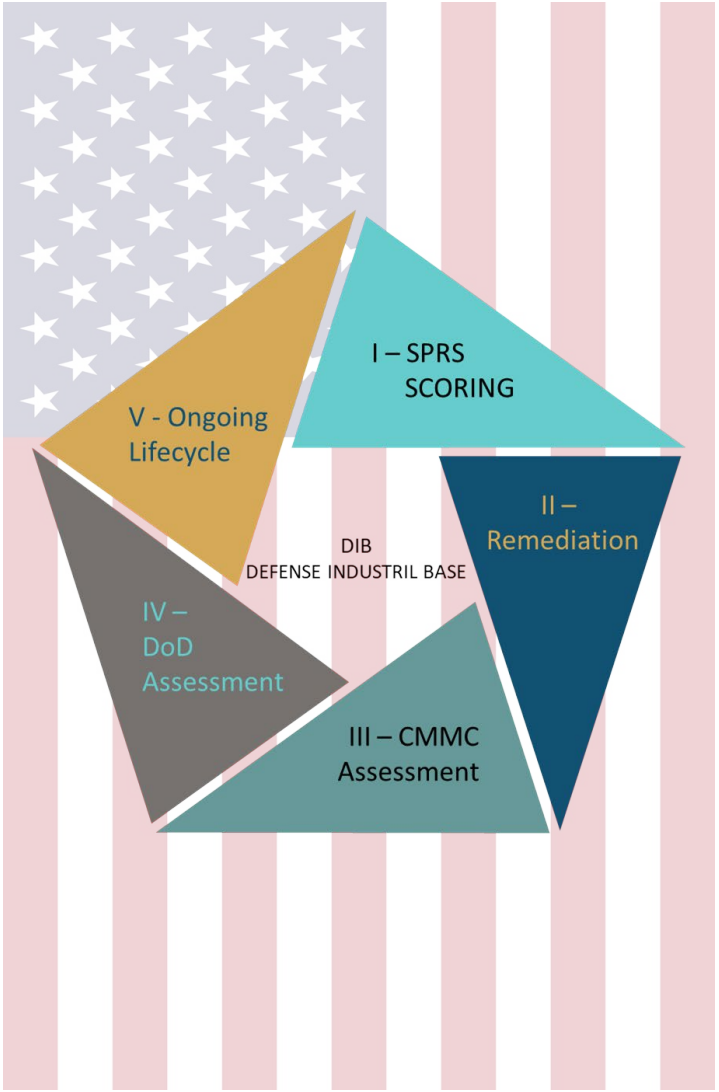
POSEIDON
TRIDENT OF INNOVATION

Cybersecurity Maturity Model Certification CMMC 2.0

July 7, 2021

Agenda

- History
- Ecosystem Roles
- CMMC 1.0 vs CMMC 2.0
- CMMC 2.0 Framework
- Accountability
- Changes
- Domains
- Existing Compliance
- CMMC 2.0 Lifecycle
- Phases
- Readiness Baseline
- Cyber Compliance Time/Costs
- Recommendations
- Questions



History

U.S. Department *of* Defense

Department of Defense (DoD):

In 2019, sought a means to protect information from threat actors

- Commissioned a new cyber compliance framework, the Cybersecurity Maturity Model Certification (CMMC)
- Expanded beyond Defense Industrial Base (DIB) to the entire Defense Supply Chain (DSC)

In 2021, revised the framework

- Split program into Levels 1-3 with Level 2 bifurcation
- Level 1, 2A requires self-assessment with Supplier Performance Risk System (SPRS) score submission and C-suite+ level signature affirmation
- Level 2B requires CMMC assessment (audit) to obtain certification
- Level 3 requires DoD assessment (audit) to obtain certification

By 2026, will be phased into all contracts

Ecosystem Roles

CMMC – Accreditation Body (AB) defines the structure surrounding the ecosystem, develops and maintains the framework in cooperation with the DoD, maintains a marketplace of providers, and (currently) accredits assessors to audit Defense contractors, subcontractors, and suppliers.

Organizations Seeking Certification (OSC) are the organizations that are contractually required to undergo an assessment in order to obtain the required certification for conducting business within the DSC.

Registered Provider Organizations (RPO) are organizations that can assist OSC's in the preparation of their processes and documentation in order to submit a package to an assessor for review.

Registered Practitioner (RP) is a trained, tested, designated individual working under an RPO or Certified Third-Party Assessor Organization (C3PAO) as a contractor or employee to advise during the preparation process and provide understanding of the standard. The RP can work for either type of organization (with some stipulations) but will generally refer to pre-audit advisory work.

C3PAO are organizations that provide Level 2B assessment services to OSC's and ensure that assessments are being conducted in the same manner by all their assessors.

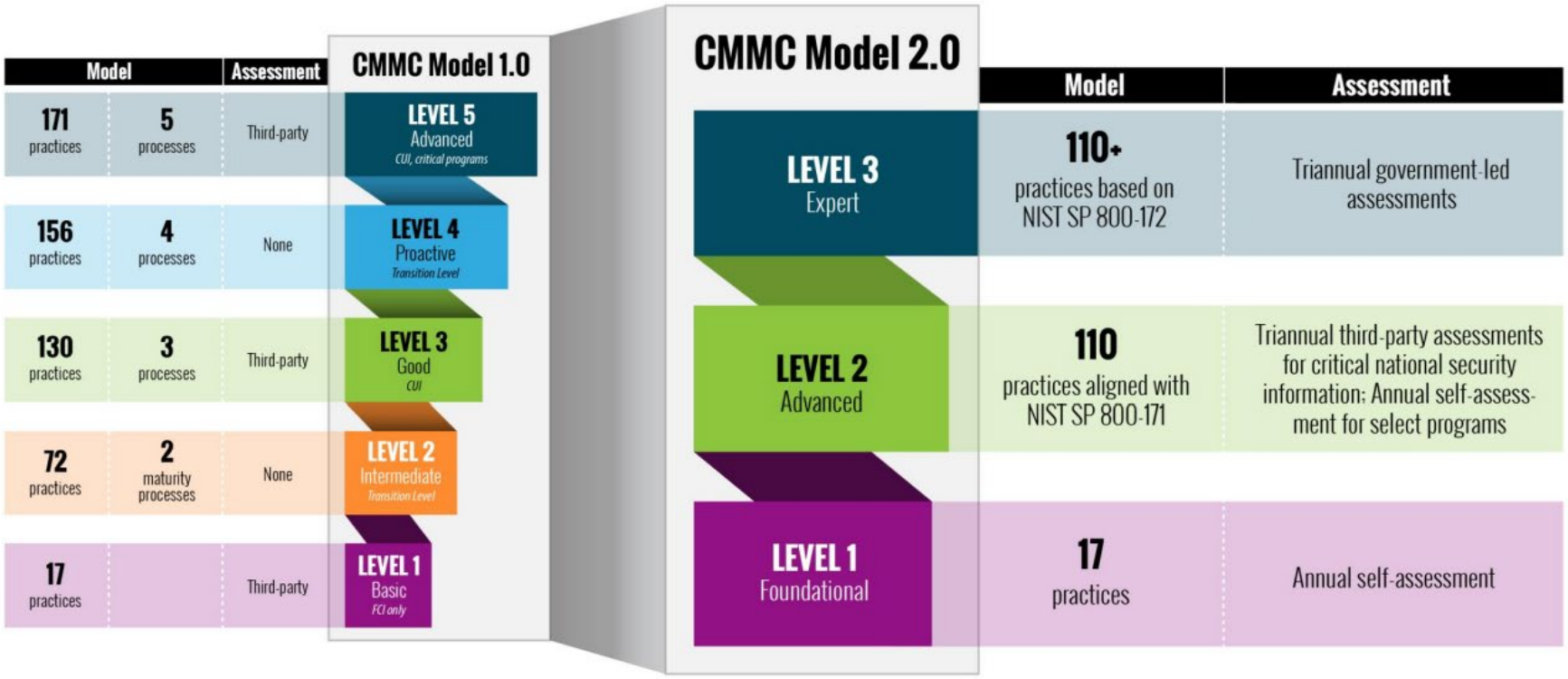
Certified CMMC Assessor (CCA) is a trained, certified individual working under the C3PAO who reviews the submitted assessment package and its evidence, conducts interviews, and makes a recommendation for certification or denial of.

Provisional Assessor (PA) is a trained, certified individual working under the C3PAO who has similar responsibilities as the CCA. The PA is the interim certification while the CCA training is still being developed.

Certified CMMC Professional (CCP) is a certified individual that serves on an assessment team assisting the assessor under a C3PAO.

Department of Defense (DoD) provides steering to the CMMC-AB and directly handles assessments for Level 3.

CMMC 1.0 vs CMMC 2.0



Rulemaking process can take 9-24 months (expected release Sept 2022 to Nov 2023)

CMMC 2.0 will become a contract requirement once rulemaking is completed

CMMC 2.0 Framework

General:

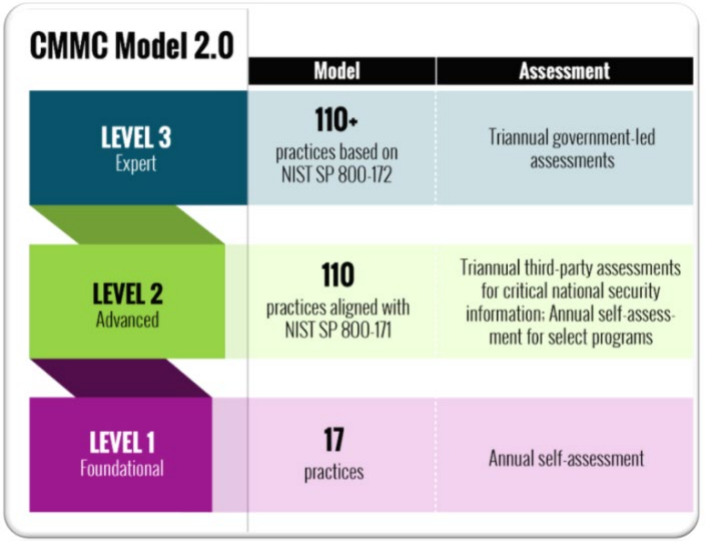
- Aligns with NIST 800-171 Controls
- Removes CMMC-specific (20) practices
- Maturity processes eliminated; practices only

Reduced from 5 Maturity Levels to 3 Levels:

- Level 1 Foundational: 17 Practices; same as previous ML-1. Protects Federal Contract Information (FCI).
- Level 2 Advanced: 110 Practices of NIST 800-171. Protects FCI and Controlled Unclassified Information (CUI).
- Level 3 Expert: Above and subset of NIST 800-172 Practices

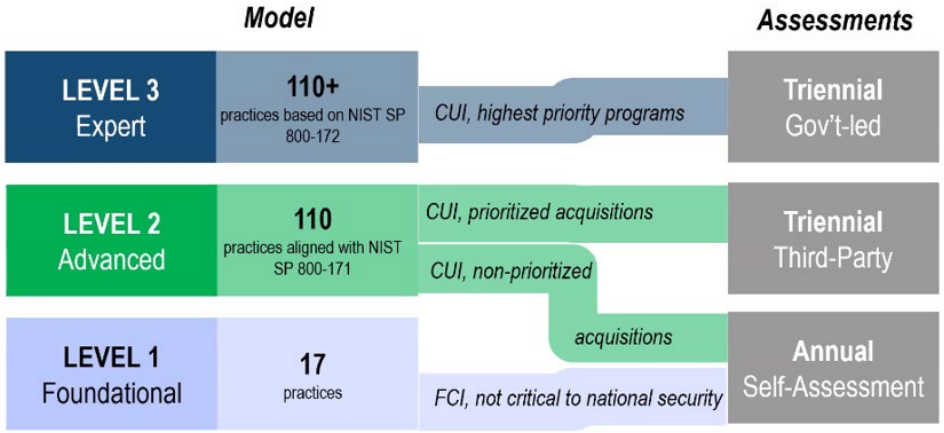
Standards In Development:

- NIST 800-171 Assessment Criteria and FedRAMP Moderate On-Premise Equivalency



CMMC 2.0 Maturity Model

Accountability



Level 1 Foundational

- Annual Self-Assessment with System Security Plan (SSP) and POAMs maintained
- Affirmation provided by C-suite or higher executive, Self-Assessment, and Score submitted SPRS

Level 2 Advanced

- Bifurcation of level non-critical to national security information and critical to national security subsets
- Self-attestation, SPRS score with C-suite + signature for non-critical subset
- Triennial CMMC Assessment for critical security subset performed by a CMMC Certified Assessor (CCA) under a Certified Third-Party Assessor Organization (C3PAO)

Level 3 Expert

- Government-led DoD Assessment for critical defense programs

Changes

POAMs

- Limited Plan of Action and Milestones (POAMs) will be permitted for certain practice types with time-bound restrictions
- Highest weighted items cannot include a POAM
- Must meet minimum score requirement overall
- POAM will be required to be addressed within 180 days

Waivers

- CMMC waivers will be permitted under specific approval
- Applies to CMMC requirement in entirety, not individual practices
- Permitted on a very limited basis on select mission-critical instances
- Requires senior leadership approval
- DoD program office must submit a justification package including a risk mitigation plan and specified timeline.
- Timelines imposed on a case-by-case basis to achieve CMMC compliance

Domains

Domains for Evaluation

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

Previous:

- Asset Management (V 1.0)
- Audit and Accountability (V 1.0)
- Security Assessment (V 1.0)
- Recovery (V 1.0)
- Risk Management (V 1.0)
- Situational Awareness (V 1.0)

Existing Compliance

Existing Federal Contract Information (FCI) Compliance

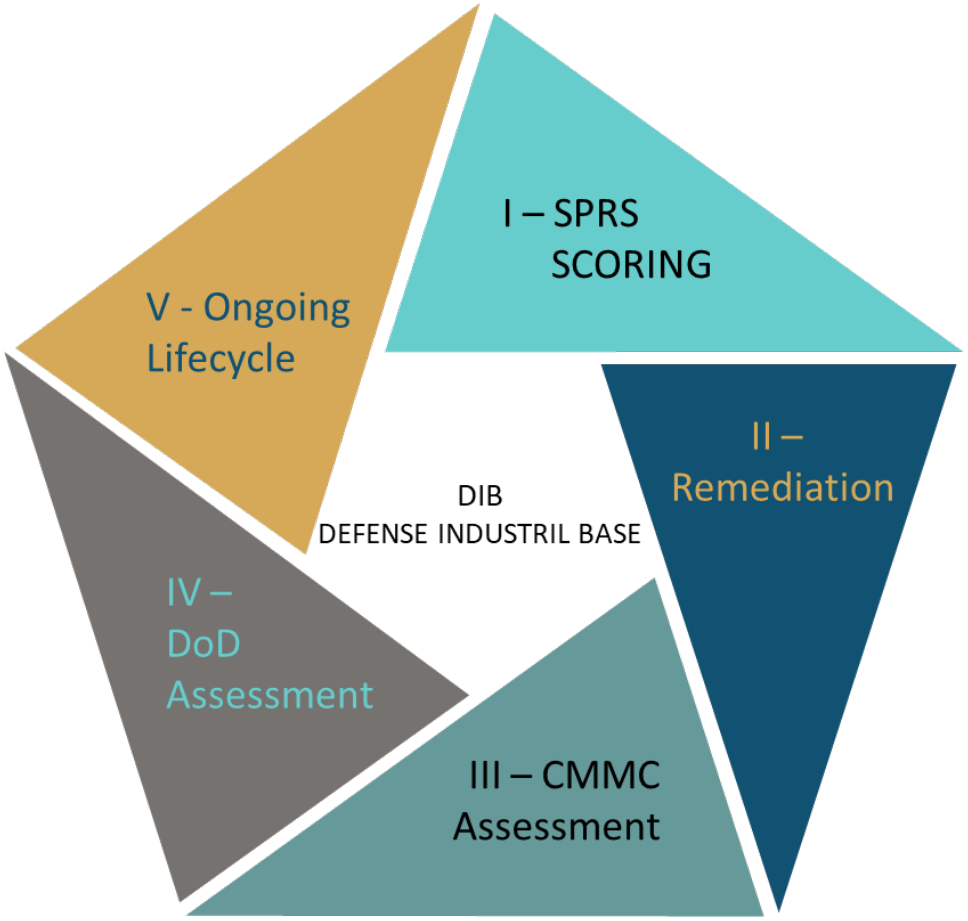
- 48 CFR 52.204-21 “Basic Safeguarding of Covered Contractor Information Systems”

Existing Controlled Unclassified Information (CUI) Compliance

- EO 13556 “Controlled Unclassified Information”
- DoDI 5200.48 Defines CUI Requirements
- DFARS 252.204-7012 Cyber Incident Reporting, NIST Requirement by 12/31/2017
- NIST SP 800-171 “Protecting CUI in Nonfederal Systems and Organizations”
- DFARS 7019/7020 Submit to SPRS, Flow Down to Subs
- NIST SP 800-172 “Enhanced Security Requirements for Protecting CUI”

(ii)(A) The Contractor shall implement NIST SP 800–171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at *osd.dibcsia@mail.mil*, within 30 days of contract award, of any security requirements specified by NIST SP 800–171 not implemented at the time of contract award.

CMMC 2.0 Lifecycle



Phase I SPRS Scoring

Supplier Performance Risk System (SPRS) process - Annual

- Gap Analysis
- Series of Interviews/Process Reviews
- Create Readiness Baseline
- POA&M Writing/Submission (SPRS and some CMMC only)
- SSP Writing (Includes Architectural Diagrams, Hardware, Firmware, Software Lists)
- Generate Self-Assessment with Score
- Develop Self-Affirmation of Score with C-Suite or high-level Signature
- Enter score into SPRS system with accompanying documentation

Organization Seeking Certification (OSC) with Third-Party IT or Consultants

Readiness Baseline

Critical Questions

- Has the organization already determined all the relevant compliance frameworks or certifications, cross-walked the controls, and implemented each? Examples: FedRAMP Moderate or High, Controlled Unclassified Information (CUI), Controlled Defense Information (CDI), International Traffic in Arms Regulations (ITAR), Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, National Institute of Standards and Technology (NIST) SP 800-53/171, etc.
- What Maturity Level is required for the DSC contracts the organization has or will attempt to acquire? Will contract work require the creation of, storage of, or transmission of Federal Contract Information (FCI), Controlled Unclassified Information (CUI)?

Microsoft Azure Selection

Microsoft 365 Government (DoD)

	Commercial	M365 "GCC"	M365 "GCC High"	M365 "DoD"
Customer Eligibility	Any customer	Federal, SLG, Tribes, DIB	Federal, DIB	**DoD only**
Datacenter Locations	US & OCONUS	CONUS Only	CONUS Only	**CONUS Only**
FedRAMP *	High	High	High	**High**
DFARS 252.204-7012	No	Yes	Yes	**Yes**
FCI + CMMC L1-2	Yes	Yes	Yes	**Yes**
CUI / CDI + CMMC L3-5	No	Yes^	Yes	**Yes**
ITAR / EAR	No	No	Yes	**Yes**
DoD CC SRG Level **	N/A	IL2	IL4	**IL5**
NIST SP 800-53 / 171 ***	Yes	Yes	Yes	**Yes**
CJIS Agreement	No	State	Federal	**No**
NERC / FERC	No	Yes^	Yes	**Yes**
Customer Support	Worldwide / Commercial Personnel		US-Based / Restricted Personnel	
Directory / Network	Azure Commercial		Azure Government	

US Sovereign Cloud

* *Equivalency,* Supports accreditation at noted impact level

** *Equivalency,* PA issued for DoD only

*** Organizational Defined Values (ODV's) will vary

^ CUI Specified (*e.g. ITAR, Nuclear, etc.*) not suitable REQS US Sovereignty

Readiness Baseline II

Critical Questions II

- Has the organization inventoried all of its processes that contain Federal Contract Information (FCI), Controlled Unclassified Information (CUI), or Controlled Defense Information (CDI), marked the data where applicable, and mapped the workflows throughout the networks, platforms, devices, systems, applications, databases, physical locations, manual processes, etc.? Does the inventory include a Shared Responsibility Matrix or Responsible Accountable Consulted Informed (RACI) Matrix?
- Does the organization's architecture utilize a Cloud Service Provider (CSP) platform with a Federal Risk and Authorization Management Program (FedRAMP) Moderate (CMMC ML 1-2) or FedRAMP High (CMMC L3-5) Authorization with security configurations or have all the NIST SP 800-53/171 and, if applicable 800-172 controls, been implemented within the organization's on-premise architecture? Similarly, are all of the organization's products from vendors authorized in the FedRAMP Marketplace or otherwise substantiated its security controls?
- Has the organization reviewed all the controls and implemented into policies and plans including, but not limited to: Configuration Management, Continuous Monitoring, and Incident Response?

Phase II Remediation

Remediation - Annual

- Gap Analysis
- FCI/CUI Process Inventory
- Risk Assessment
- Executive Policies
- Architecture Builds, Development
- Technical Policies
- Manual Processes
- Plan and Program Documentation
  - Configuration Management
  - Continuous Monitoring
  - Incident Response
- Responsibilities Matrix – SRM, RACI
- Funding
- Update SSP
- Testing
- Maintaining
- Evidence Collection if Level 2B, 3

Level 1, 2A: Update SPRS with Annual Self-Assessment; Advance to Phase V
Level 2B: Prepare/Gather/Review Evidence; Submit package to C3PAO; Advance to Phase III
Level 3: Prepare/Gather/Review Evidence; Submit package to DoD; Advance to Phase IV

Organization Seeking Certification (OSC) with Third-Party IT or Consultants and RP/RPO/C3PAO

Phase III-A, B CMMC Assessment

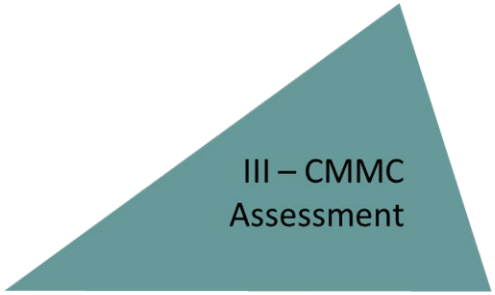
Phase III-A CMMC Assessment

Assessor

- Reviews Package with Objective Evidence from OSC
- Interviews OSC without RP
- Requests Additional Evidence
- Makes Pass/Fail Recommendation to C3PAO Board

C3PAO

- Reviews Package and Assessor Recommendation
- Submits to CMMC-AB for Review and Certification



Phase III-B CMMC Certification

CMMC-AB

- Reviews Package from C3PAO
- Passes or Fails the Assessment
- Grants/Declines CMMC Certification
- Reserves the right of Continuous Monitoring of Organization
- Reserves the right to Audit the organization within 36 months of certification

Organization Seeking Certification (OSC) with CCA/C3PAO/CMMC-AB

Phase IV DoD Assessment

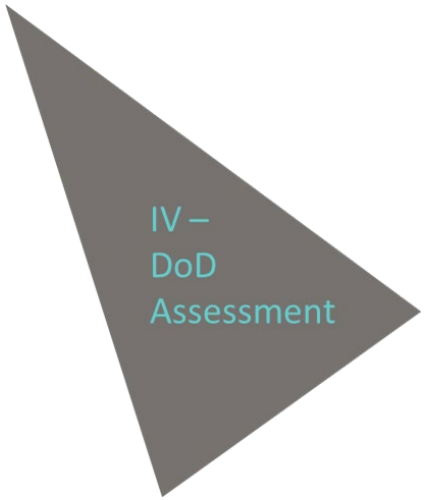
DoD Assessment

Assessor

- Reviews Package with Objective Evidence from OSC
- Interviews OSC without RP
- Requests Additional Evidence
- Makes Pass/Fail Recommendation to DoD Board

DoD

- Reviews Package and Assessor Recommendation
- Grants/Declines the DoD Certification



Organization Seeking Certification (OSC) with DoD

Phase V Ongoing Lifecycle

Ongoing

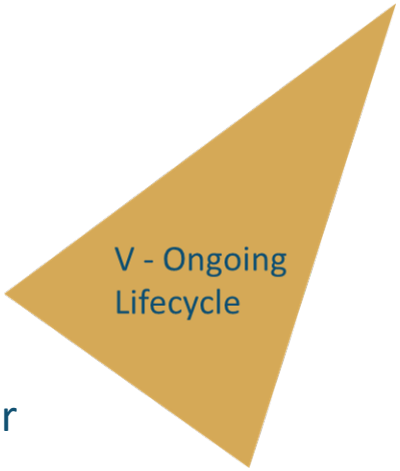
- Conduct Ongoing Review of Policies, Practices, Processes (Monthly/Quarterly/Annually)
- Review Delta Changes from CMMC/NIST
- Progressive Configuration Management, Continuous Monitoring, Incident Response
- Add-On vCISO Trusted Advisor Services

Implement Changes

- Re-execute plans annually
- Add-On Cybersecurity Maturity-as-a-Service (CMaaS) Services

Maintain Resources for three years

- Remain in Audit-Ready Posture, Resourced for Three Years
- Plan for next assessment or certification at least 6 months prior



Organization Seeking Certification (OSC) with Third-Party IT or Consultants and RP/RPO/C3PAO

Cyber Compliance Time/Costs

Effort Estimates:

- Ready before award
- Time: 6-24 months depending on baseline readiness, size (locations, product offerings) and complexity of organization, internal vs. external resource utilization, environment, hardware/software/application, physical controls
- Cost: SMB $300-500,000 initial
- Soft Costs: Education/Training, Procedural Changes, Tool Functionality Changes
- Ongoing and incremental costs; increased vigilance

Recommendations

Assessment (Audit) Preparation & Remediation:

- Begin Early
- Enclaves
- Primes Can Allow Subs into Enclaves
- Cybersecurity-Maturity-as-a-Service (CMaaS) subscription from a Registered Practitioner (RP)

QUESTIONS

Contact:

James Quilty – james.quilty@poseiodn-us.com

Jessica Paull – Jessica.paull@poseidon-us.com