“CMMC F-35s & $320B Annual DoW Contracts – O-My”

Brian Schultz

CISM, CISA, CISSP, ISSMP, ISSAP, and NSA IAM

Married 35 years

Father of 4 Eagle Scouts

Avid white-water kayaker

THE VIGILANT

FORUM

OF NATIONAL & CYBER SECURITY

Scouting America™

Disclaimer

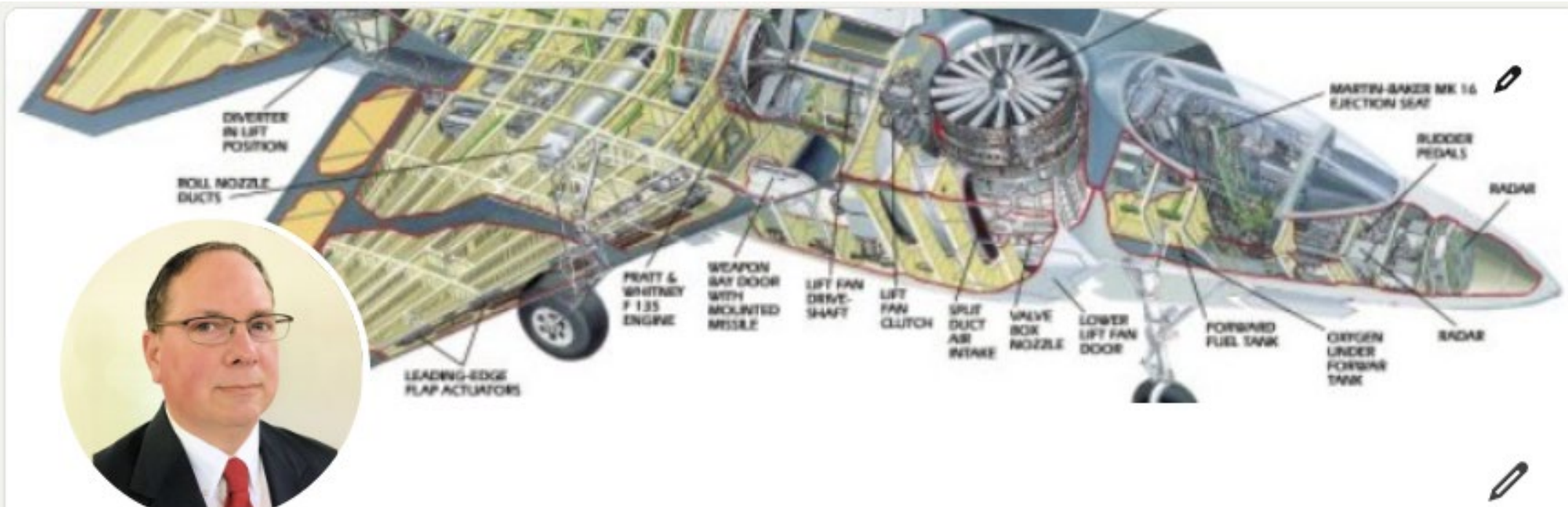
- Not a lawyer – “don’t play one on TV”
- My opinions are my own – Not my employer’s
- My opinions are my own – Not Vigilant Forum’s
- Use my observations at your own risk

CMMC Talk - Intro

- October 1, 2025 – “shields up” to protect the IP in a four year–four phased program to fully execute the CMMC program. Prior DoD regulation enforcement efforts failed miserably with no means to regulate 78,000 entities. However, this time US DoW is driving resiliency through the “power of the purse” with over $320B in annual contracts. Contractors with NO CMMC Level 2 Certification – NO contracts – means NO revenue. DoW contractors, referred to as the Defense Industrial Base (DIB)s are rapidly moving to become CMMC Level 2 C3PAO Certified. Like a version of the “hunger games” where the contractors compete for an ever increasingly short supply of CMMC readiness consultants; and C3PAOs and Certified Assessors that can assess and certify them. C3PAOs are scrambling to recruit and retain the short supply of ISACA certified LCCAs, CCAs and CCPs needed to perform the DIB certifications. Additionally, prime contractors like Lockheed Martin, Northop Grumman, Boeing and L3 are demanding that its subcontractors become CMMC Level 2 Certified NOW to ensure that their contract teams are prepared to win new contracts and contract renewals. CMMC also solves the TPRM challenge. No longer will prime contractors need to validate the cybersecurity resiliency of its tier 1, 2, 3, 4 suppliers to ensure that they won’t be ransomware’d and then not provide a key component of a weapon system.

Brian’s Perspective – Driven by Experiences

- **Speaker Bios:**
  Brian Schultz is a Department of War (DoW) Cyber Maturity Model Certification (CMMC) expert with 20+ yrs protecting $1.4T of DoW Defense Industrial Base (DIB), Department of Defense (DoD), Department of Homeland Security (DHS), FBI, Fed CIV, and Fortune 500 assets from Advanced Persistent Threats (APTs). While serving as. Currently serving as a Senior Dir, Supply Chain Cybersecurity, at Gartner and serving over 250 large Global 1,000 clients, firsthand heard the dire need for a CMMC like ecosystem that would secure corporate IP whilst also building a robust Third Party Risk Management (TPRM) programssessor with C3PAO NSF to determine DIB contractor’s compliance with NIST 800-171 R2. Co-Host & Facilitator of The Vigilant Forum – leading and facilitating weekly gathering of senior level executives, visionaries, thought leaders, strategists, experts, speakers, authors, and influencers. Highly rated speaker RSA, Gartner, AFCEA, FISSEA, FIAC, ISC2, ISSA, and API cyber conferences. Author of Gartner, SC Magazine, FISSEA articles and INFOSEC Mgt Handbook. Board Member, Technology Advancement Center (TAC); Former ISSA International Board Member, Former ISC2 Advisory Board Member, ISSA Distinguished Fellow, and Past President of the ISSA-NOVA Chapter. Holds a MBA from George Washington University, BBA from James Madison University, and industry certifications: CISM, CISA, CISSP, ISSMP, ISSAP, and NSA IAM.



Brian R. Schultz

CMMC Lead Mock Assessor | MBA | CISSP | CISM | CISA | ISSMP | ISSAP | TAC Advisory Board Member | Co-Host Vigilant Forum| ISSA Distinguished Fellow

Greater Richmond Region · Contact info

2,533 followers · 500+ connections

NSF

The George Washington University

TPRM – Supply Chain

- Car manufacture example
- Cyber Surveys
- Return Surveys
- Lack consistent frameworks, standards, and nomenclature
- Tracking survey results – where, how?
- Communicating risk to C-suite
- Process to update C-Suite risk profile
- Process to update 1,000s & multiple tiers of supplier's cyber resiliency
- Would it be great…..

CMMC

Cybersecurity Maturity Model Certification

What is CUI? Why should I care?

- DoW R&D Annual Budget - $148B FY 2026
- DoW will award $320B+ CMMC Level 2 contracts - annually
- Who will steal it?
- What will they do with CUI?

CMMC

What:

A consistent pre-award assessment methodology to determine whether a prospective contractor has implemented cybersecurity protections necessary to adequately safeguard DoW information.

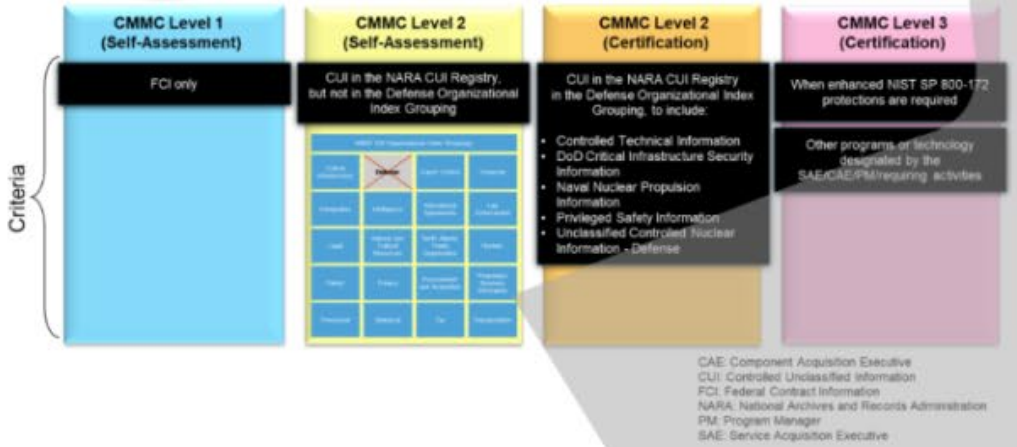
Why:

To increase the cybersecurity posture of the DIB and better protect Federal Contract Information and Controlled Unclassified Information.

How:

All defense contractors and subcontractors will show compliance with applicable security requirements through self-assessment or independent assessment, prior to contract award (excluding Commercial-Off-The-Shelf procurements).

Criteria for CMMC Levels



CMMC Level 2 (Self-Assessment)

CUI in the NARA CUI Registry, but not in the Defense Organizational Index Grouping

NARA CUI Organizational Index Groupings			
Critical Infrastructure	~~Defense~~	Export Control	Financial
Immigration	Intelligence	International Agreements	Law Enforcement
Legal	Natural and Cultural Resources	North Atlantic Treaty Organization	Nuclear
Patent	Privacy	Procurement and Acquisition	Proprietary Business Information
Provisional	Statistical	Tax	Transportation

CMMC Level 2 (Certification)

CUI in the NARA CUI Registry in the Defense Organizational Index Grouping, to include:

- Controlled Technical Information
- DoD Critical Infrastructure Security Information
- Naval Nuclear Propulsion Information
- Privileged Safety Information
- Unclassified Controlled Nuclear Information - Defense

CAE: Component Acquisition Executive
CUI: Controlled Unclassified Information
FCI: Federal Contract Information
NARA: National Archives and Records Administration
PM: Program Manager
SAE: Service Acquisition Executive

Information that meet these criteria may require a higher CMMC level. CUI meeting multiple criteria will align to the highest applicable CMMC level.

CMMC Overview

What is CMMC?

- A DoD framework ensuring protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

Why Align to NIST Standards?

- Leveraging existing federal requirements, efficiency, and risk mitigation.

Existing DoW Cybersecurity Requirements

- DFARS clause 252.204-7012 – **Effective Oct 2016 (to be implemented NLT Dec 2017)**
  - Safeguard DoW CUI that resides on or is transiting through a contractor/subcontractor internal information system or network by implementing NIST SP 800-171 at a minimum
  - Report cyber incidents that affect contractor/subcontractor ability to perform requirements designated as operationally critical
  - Does not required a specific POA&M close-out date or a compliance assessment
- DFARS Provision 252.204-7019 – **Effective Nov 2020**
  - Implement DFARS clause 252.204-7012 and have at least a NIST SP 800-171 self-assessment (Basic) that is current posted in SPRS (i.e., not more than three (3) years old unless a lesser time is specified in the solicitation)
  - Does not require a minimum passing score
- DFARS clause 252.204-7020 – **Effective Nov 2020**
  - Provide Government access when necessary to conduct or renew a higher-level Assessment
  - Include requirements of the clause in all applicable subcontracts and ensure applicable subcontractors can conduct and submit an Assessment

CMMC assesses whether a prospective DoW contractor has implemented these standards

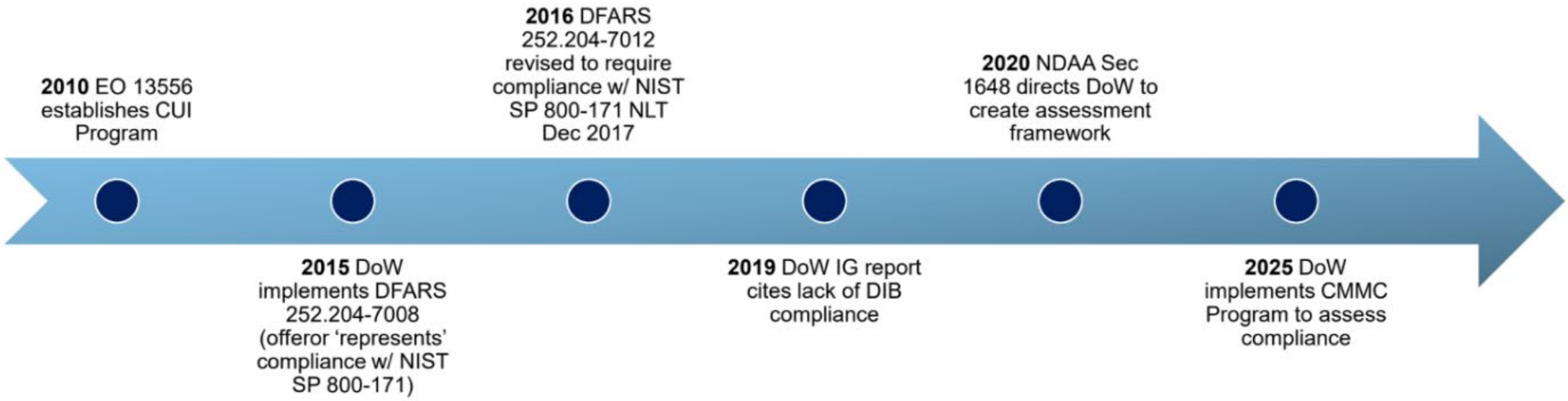
CMMC Applicability

- CMMC Program requirements will apply to all DoW solicitations and contracts for which a defense contractor or subcontractor will process, store, or transmit FCI or CUI on its unclassified contractor information systems
  - New DoW solicitations
  - New DoW procurement instruments, including contracts, task orders, delivery orders and their associated option periods
  - As a condition to exercise an option period
  - Subcontractors are subject to flow-down requirements
- CMMC implementation will occur through new contracts awarded after **10 Nov 2025**
- Incorporation in older contracts would require bilateral modification

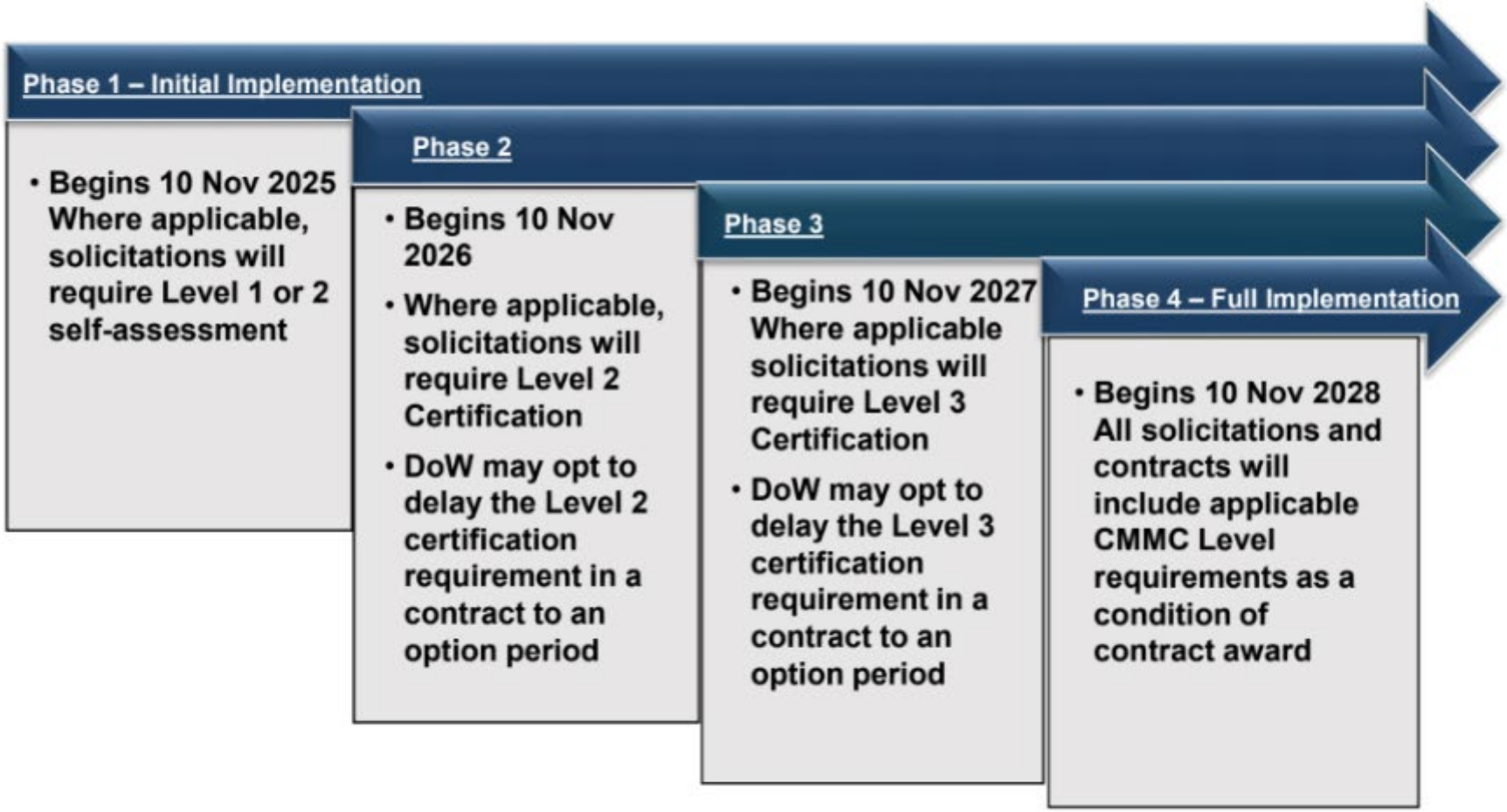
The CMMC Program does not alter separately applicable requirements to protect FCI or CUI

CMMC Program Overview and History

The CMMC Program helps ensure that DoW contractors and subcontractors comply with DoW requirements to safeguard FCI and CUI.



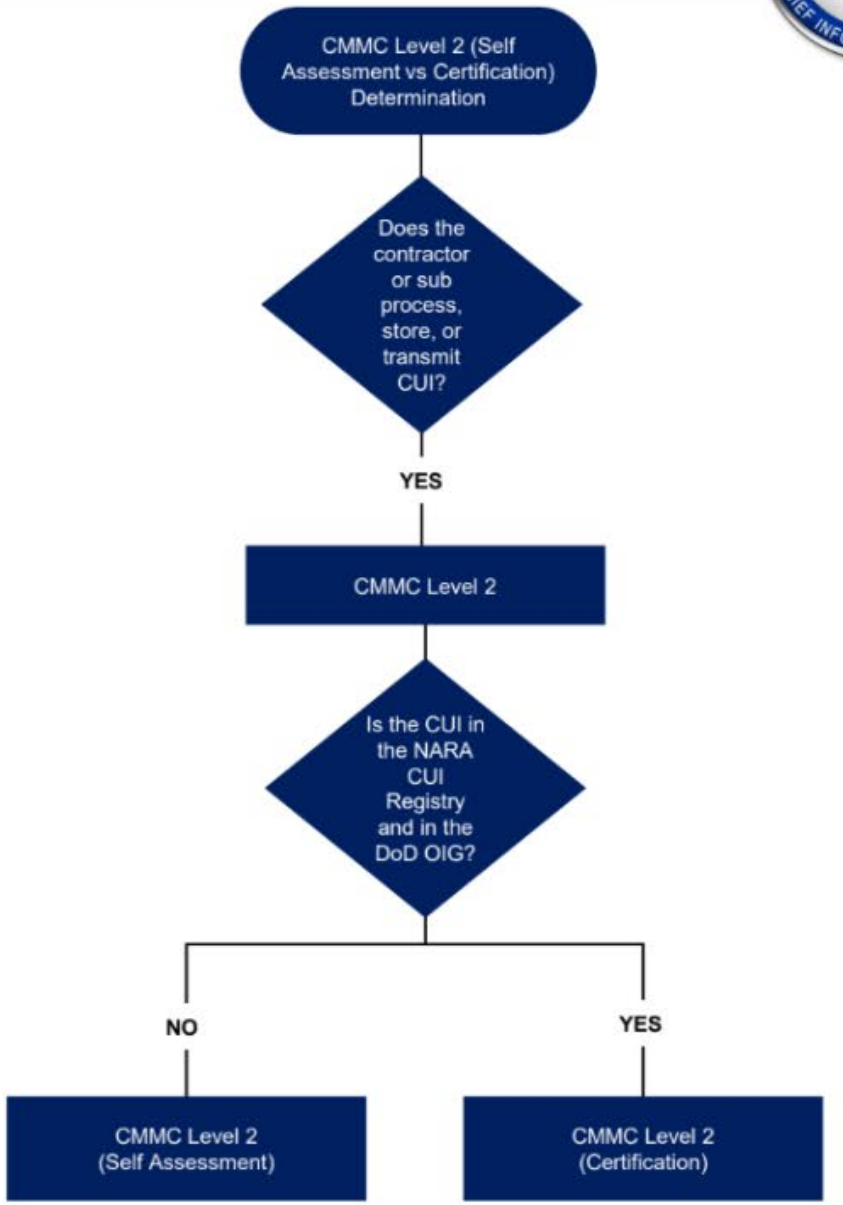
Phased Implementation of CMMC Requirements



DoW may implement CMMC Level 2 (C3PAO) requirements in some Phase 1 procurements or Level 3 requirements in some Phase 2 procurements, which may limit competitors or drive cost

Selecting CMMC Level 2 Requirements

- Contractors or subcontractors who process, store, or transmit controlled unclassified information (CUI) on their information systems must meet CMMC Level 2 requirements, at a minimum:
  - Level 2 (Self-Assessment) is the minimum assessment requirement for contractors handling CUI that is in the National Archives and Records Administration (NARA) CUI Registry, but not in the Defense Organizational Index Grouping (OIG).
  - Level 2 (Certification) is the minimum assessment requirement for contractors handling CUI in the NARA CUI Registry's Defense OIG.

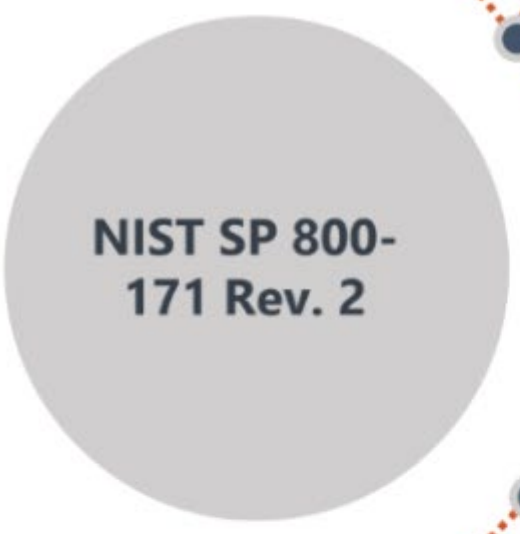


CMMC Overview (2 of 2)

CMMC currently aligns to NIST SP 800-171 R2, NIST SP 800-171A Jun2018, NIST SP 800-172 Feb2021, and NIST SP 800-172A Mar2022

CMMC Level	Applicability	Security Requirements	Assessment Type	Assessment Frequency	Affirmation of Compliance
Level 1	**Federal Contract Information (FCI) [~140,000 DIB companies]**	FAR 52.204-21 (15 security requirements)	Self-assessment	Annual	Annual
Level 2	**Controlled Unclassified Information (CUI) [~75,000 DIB companies]**	DFARS 252.204-7012 requires NIST SP 800-171 R2 (110 security requirements)	Self-assessment or CMMC Third-Party Assessment Organization (C3PAO) assessment *(as specified in contract based on type of CUI)*	Every 3 years	Annual
Level 3	**CUI** deemed critical or high-value CUI by DoD program manager (PM) **[~1,500 DIB companies]**	NIST SP 800-171 R2 (C3PAO assessment) plus 24 NIST SP 800-172 Feb2021 (134 security requirements)	DIBCAC assessment *(conducted after Level 2 C3PAO assessment)*	Every 3 years	Annual

Alignment to NIST SP 800-171 Rev. 2



Core of CMMC Level 2

- Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 requires NIST SP 800-171 Rev. 2.
- 110 Security Requirements across 14 families.

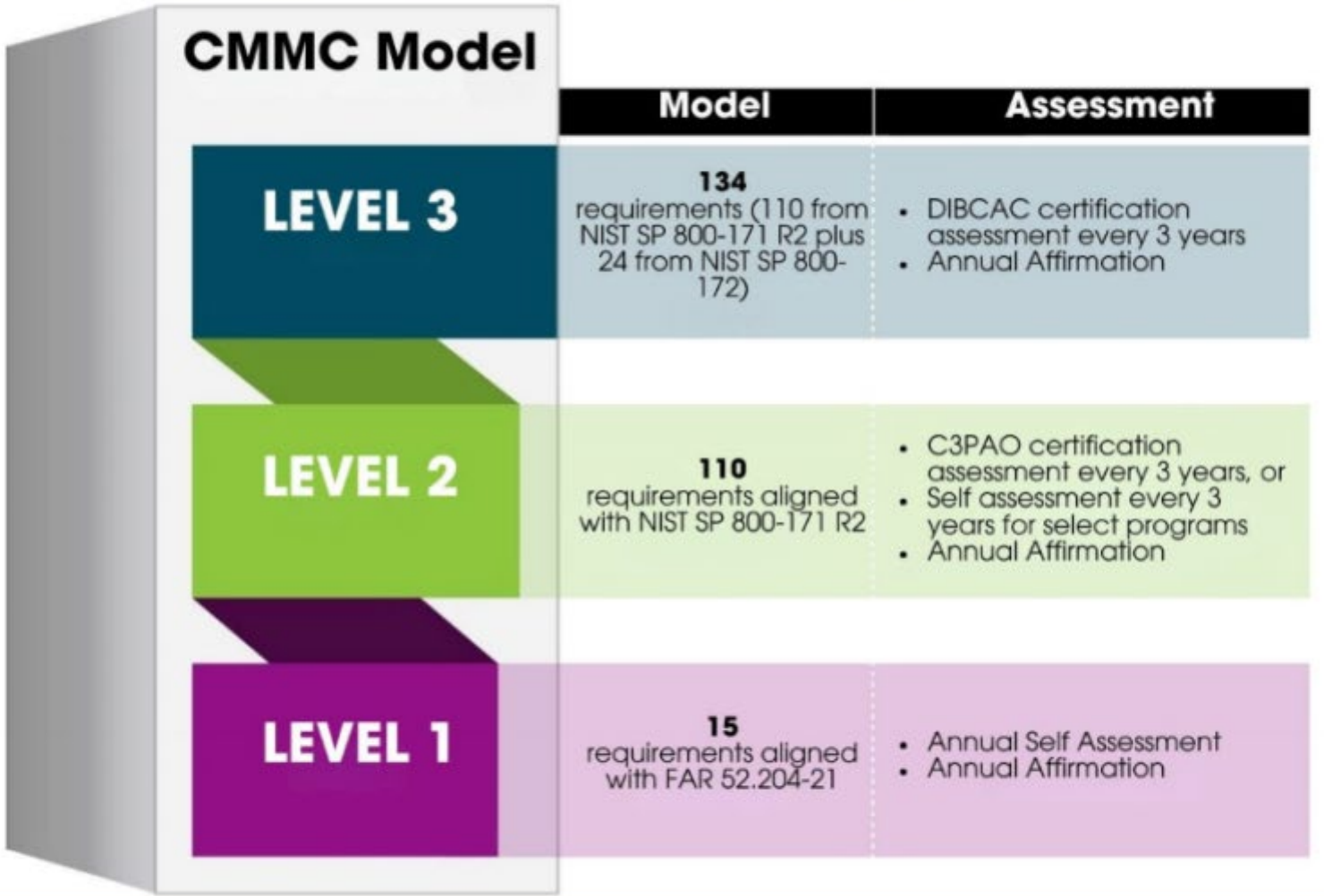
Assessment and Affirmation

- Ensures consistent baseline implementation of safeguards for protecting CUI.
- Self-assessments and third-party assessments (C3PAOs) validate compliance.

Key Requirements

- System Security Plan (SSP): How security requirements are met.
- Plan of Action & Milestones (POA&M): Addressing gaps (conditional compliance).

Revised CMMC Framework Requirements



When specified in a solicitation, all CMMC requirements must be met prior to award

CMMC Process - OSA Perspective

Government determines CMMC Status Requirements

CMMC Status visible to DoW in SPRS.

Contractor/Sub perform self-assessment

OR

Contractor/Sub completes Annual Affirmation

Contractor/Sub undergo C3PAO or DIBCAC assessment

Assessment results entered into SPRS or eMASS, depending upon assessment type

SPRS User Roles – PIEE single sign-on

- ***Government (KOs, PMs, LOGgies, etc.)***
  - ***SPRS ACQUISITION PROFESSIONAL***
    - *Gives access to all scores/reports*

https://piee.eb.mil

PIEE Procurement Integrated Enterprise Environment

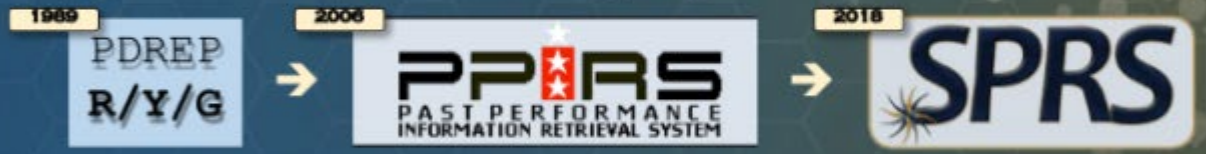
SPRS

- ***Contractor/Vendor***
  - ***SPRS CONTRACTOR/VENDOR (SUPPORT ROLE)***
    - *View your company's scores/reports*
    - *View-only access to CS assessments*
    - *CAGE hierarchy*
  - ***SPRS CYBER VENDOR USER*** ← Add New CMMC Level 2 Self-Assessment
    - *Add/edit/delete/affirm CS assessments*
    - *CAGE hierarchy*

What is SPRS? (1 of 2)

Supplier Performance Risk System

- *"... the authoritative source to retrieve supplier and product PI [performance information]" (DoDI 5000.79)*



- *Vendor Performance*
  - *Quality Classifications & On-time Delivery scores by FSC/PSC/NAICS*
  - *Supplier Risk – Ranked risk of vendor performance – 79K+ CAGEs*
  - *Price Risk – Average Price, Expected Range, over/underprice alerts – 1.6M+ items*
  - *Item Risk – Suspected Counterfeit, CSI/CAI, DMSMS, etc. – 135K+ items*

- *Vendor Compliance*
  - *Debarments/exclusions, § 889, FASCA, ~~representations/certifications~~ (from SAM)*
  - *Cyber Security Assessments: NIST SP 800-171, CMMC*
  - *NSS Restricted List (formerly § 806 "Do Not Buy List")*
  - *Vendor Threat Mitigation (§ 841 NCWtE)*

- *Supply Chain Illumination, contract history & analysis, corporate CAGE hierarchies*

CMMC Ecosystem

DoW CIO CMMC PMO - § 170.6
- Provides oversight of the CMMC Program, to include the CMMC AB
- Develops and maintains the CMMC Model Overview, Assessment Guides, Scoping Guides, and Hashing Guide
- Scheme Owner for ISO/IEC Requirements
- Establishes DoW requirements of C3PAOs, CAICO, Assessors, and Instructors

DoW - DCMA DIBCAC - §170.7
- Conducts CMMC Level 2 Certification Assessments on C3PAOs
- Conducts CMMC Level 3 Certification Assessment on DIB
- Advises DoW CIO CMMC PMO

DoW Contract

CMMC AB - §170.8
- Professionally staffed
- Managed by Board of Directors
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO

C3PAOs – § 170.9
- ISO / IEC 17020
- Conducts CMMC Level 2 Certification Assessments on DIB contractors
- Employs Assessors
- Submits Assessment Report in eMASS
- Issues CMMC certificate to DIB contractor

Agreements

CAICO - §170.10
- ISO/IEC 17024
- Certifies CMMC Certified Professionals, Assessors, and Instructors
- Defines knowledge areas required for CCPs, CCA,s and CCIs with input from DoW
- QCs curriculum developed by ecosystem

CMMC Certified Processionals, Assessors & Instructors – § 170.11, § 170.12 and 170.13
- Certified by CAICO IAW ISO/IEC 17024

Evaluation Criteria

- Requirements vs Status
- Building a team
- How do I get on a team
- Primes building teams
- Capabilities matrix
- Evaluation criteria
- Contracting officers award processes
- Protest proof

My CMMC Journey

- CCP
- CCA
- LCCA
- T3 – been 13 months

CMMC Future

- Where are we with primes?
- Where are we with solicitations?
- Will CMMC get canceled?
- Does Fortune 500 want it?

Questions?