CMMC 2.0 Overview & Rollout

Briefers: Jesse Watkins, SID
Bethanie Healey, CMO
Neil Dsouza, ITD

DARPA

DISTRIBUTION A: Approved for public release; distribution unlimited.

CMMC 2.0 Program BLUF

Purpose: Safeguard CUI & FCI

Effective Date: 16 December 2024

DFARS Clause: Final Rule Published 10 September 2025; Enforcement date: **10 November 2025**

Applicability (only when prime or sub will process; store; transmit CUI/FCI

- New DoW solicitations
- New procurement contracts (task & delivery orders)
- When exercising an option period
- Subcontractors flow-down requirements

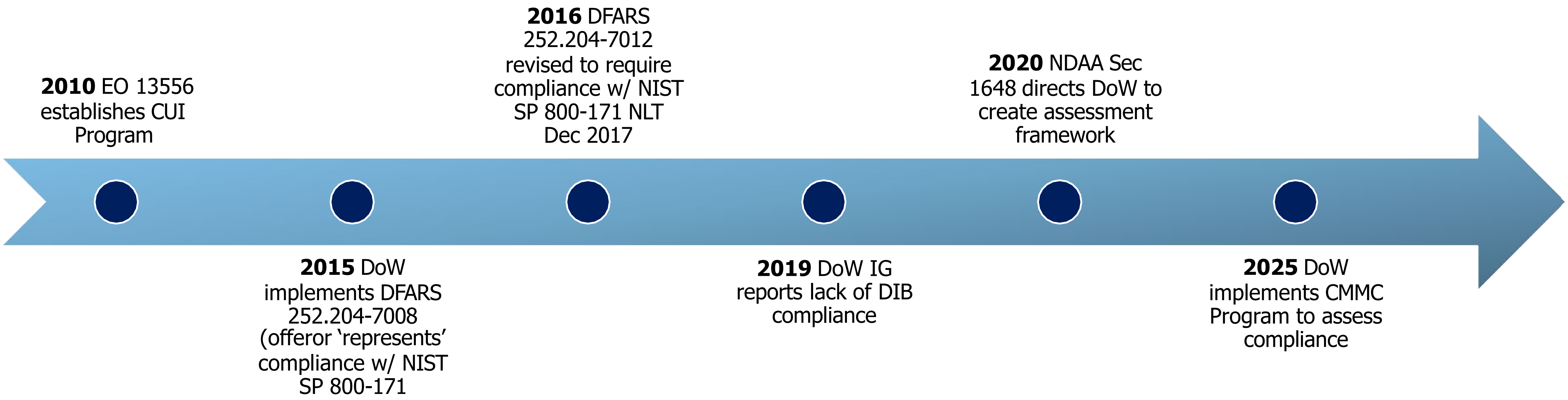
What you need to know (your role)

- Ensure proper level in contract
- Track compliance & certification

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

CMMC Program History

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



2010 EO 13556 establishes CUI Program

2015 DoW implements DFARS 252.204-7008 (offeror ‘represents’ compliance w/ NIST SP 800-171

2016 DFARS 252.204-7012 revised to require compliance w/ NIST SP 800-171 NLT Dec 2017

2019 DoW IG reports lack of DIB compliance

2020 NDAA Sec 1648 directs DoW to create assessment framework

2025 DoW implements CMMC Program to assess compliance

About Cybersecurity Maturity Model Certification (CMMC) Program

Cybersecurity is a top priority for the Department of War (DoW). The Defense Industrial Base (DIB) faces increasingly frequent, and complex cyberattacks. To strengthen DIB cybersecurity and better safeguard DoW information, the department developed the Cybersecurity Maturity Model Certification (CMMC) Program to assess existing DoW cybersecurity requirements

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).

DISTRIBUTION A: Approved for public release; distribution unlimited.

Protected Information

The CMMC model is designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) shared with defense contractors and subcontractors during contract performance.

- **Federal Contract Information (FCI)**: As defined in section 4.1901 of the Federal Acquisition Regulation (FAR), FCI is “information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, excluding information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments.”

- **Controlled Unclassified Information (CUI)**: As outlined in Title 32 CFR 2002.4(h), CUI is “information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.” For more information regarding specific CUI categories and subcategories, see the DoW CUI Registry website.

CMMC 2.0 Applicability

- CMMC Program requirements will apply to <u>all DoW solicitations and contracts</u> 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 (Currently does not apply to Grants, Cooperative Agreements, and OTs)
  - Exercising an option period
  - Subcontractors are subject to flow-down requirements

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

Existing DoW Cybersecurity Requirements

- DFARS clause 252.204-7012 – **Effective Oct 2016, Implement 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
- DFARS Provision 252.204-7019 – **Effective Nov 2020**
  - Implement DFARS clause 252.204-7012 and have at least a Basic NIST SP 800-171 DoW Assessment that is current (i.e., not more than three (3) years old unless a lesser time is specified in the solicitation) posted in SPRS
- 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 performer has implemented these standards

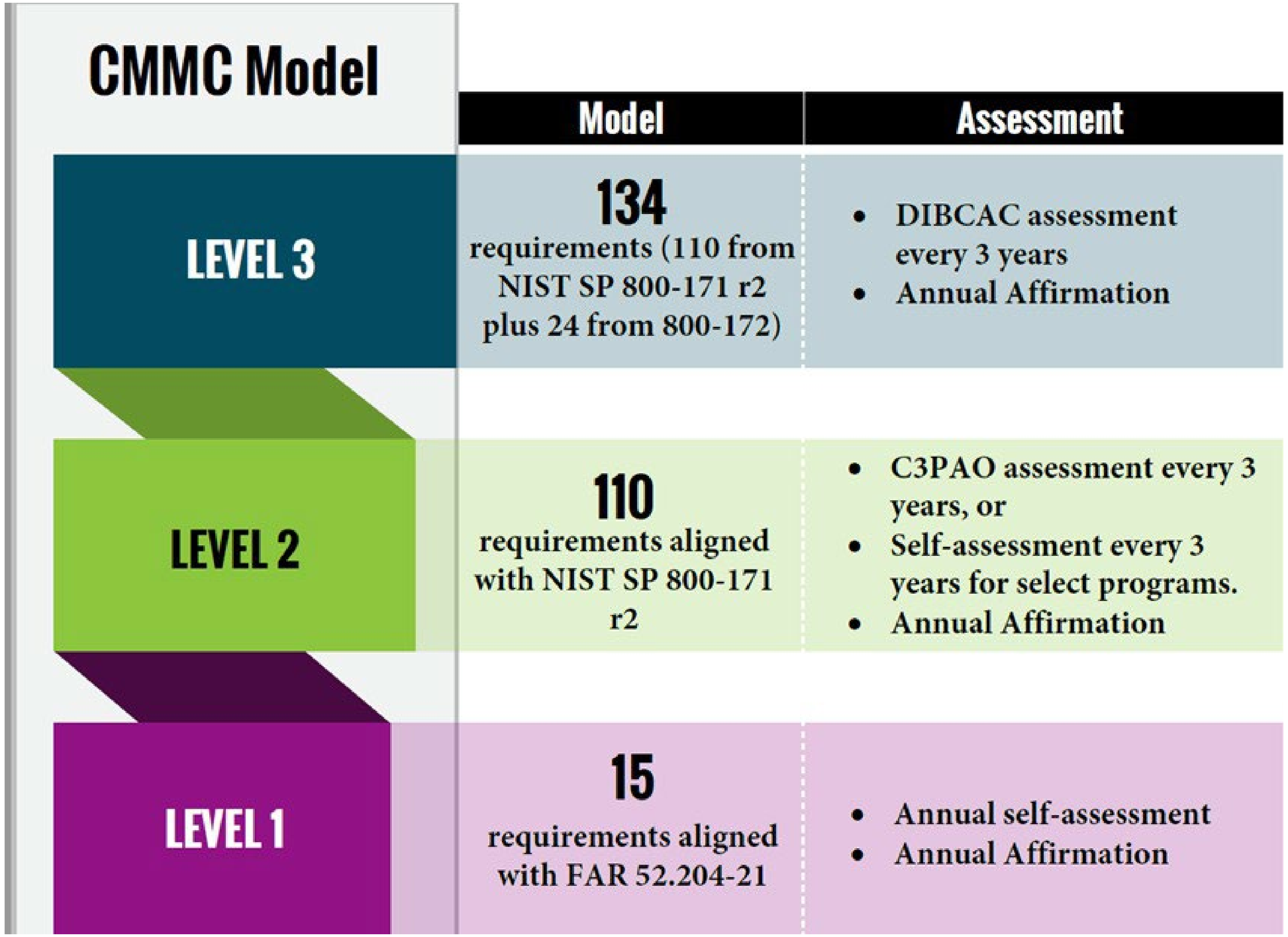
CMMC DFARS Clause

- DFARS clause 252.204-7021 – Effective **10 Nov 2025**
  - Relies on the requirements owner to identify the appropriate CMMC Status requirements based on the type of information to be processed, stored, or transmitted

  - Requires the performer/sub to:
    - Develop and update Artifacts and Deliverables per RFI/RFP
    - Conduct Self-Assessment or request a C3PAO or DIBCAC to perform a CMMC Certification Assessment, depending on the sensitivity of the data on the contractor’s or subcontractor’s information system
    - Complete annual affirmation of continued compliance in SPRS
    - Flow-down the DFARS clause 252.204-7021 to subcontractors

CMMC Final Rule Published 10 Sep 2025, Enforcement begins 10 Nov 2025

Revised CMMC Framework Requirements



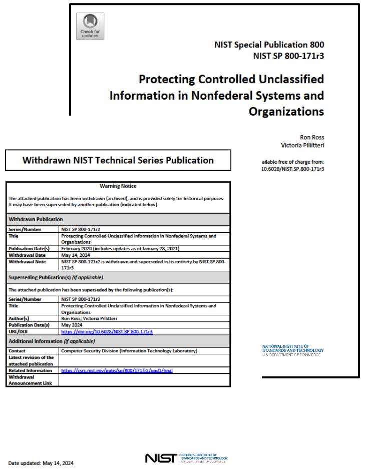
CMMC Model

	Model	Assessment
LEVEL 3	**134** requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	• DIBCAC assessment every 3 years • Annual Affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171 r2	• C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs. • Annual Affirmation
LEVEL 1	**15** requirements aligned with FAR 52.204-21	• Annual self-assessment • Annual Affirmation

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

Information Technology (IT) Cybersecurity Requirements

- **NIST SP 800-171, Rev 2** (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)
    - Rev 3 not currently implemented for CMMC requirements.
  - Compliance required for protection of USG CUI data and information
  - 800-171 security requirements represent a subset of the controls that are necessary to protect the confidentiality of CUI
  - Government Organizational-Defined Parameters
    - Provide both the flexibility and specificity needed by organizations to clearly define their CUI security requirements, given the diverse nature of their missions, business functions, operational environments, and <u>risk tolerance</u>
    - Support consistent security assessments in determining whether specified security requirements have been satisfied



Check for updates

NIST Special Publication 800
NIST SP 800-171r3

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Ron Ross
Victoria Pillitteri

ailable free of charge from:
10.6028/NIST.SP.800-171r3

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Withdrawn NIST Technical Series Publication

Warning Notice

The attached publication has been withdrawn (archived), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

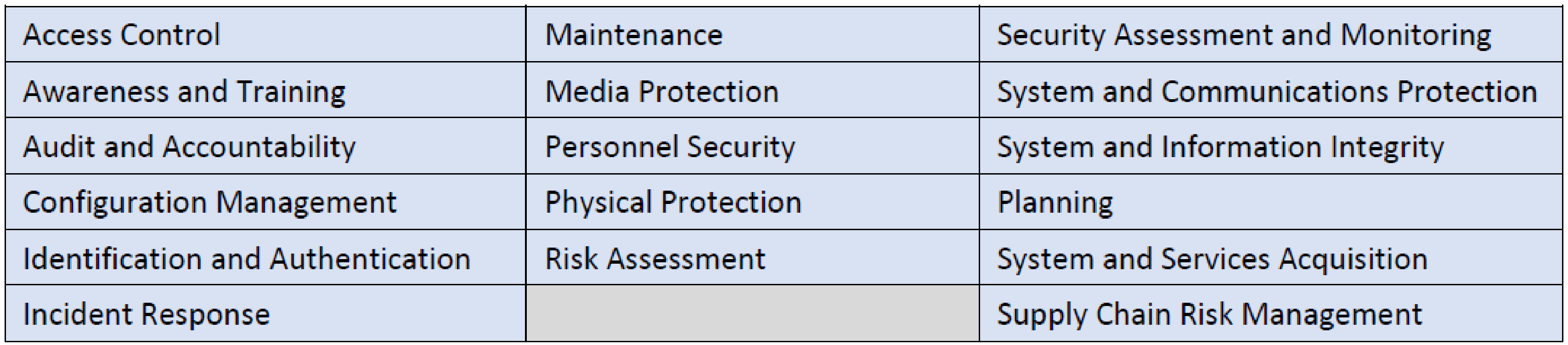
Withdrawn Publication	
Series/Number	NIST SP 800-171r2
Title	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Publication Date(s)	February 2020 (includes updates as of January 28, 2021)
Withdrawal Date	May 14, 2024
Withdrawal Note	NIST SP 800-171r2 is withdrawn and superseded in its entirety by NIST SP 800-171r3
Superseding Publication(s) *(if applicable)*	
The attached publication has been superseded by the following publication(s):	
Series/Number	NIST SP 800-171r3
Title	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Author(s)	Ron Ross; Victoria Pillitteri
Publication Date(s)	May 2024
URL/DOI	https://doi.org/10.6028/NIST.SP.800-171r3
Additional Information *(if applicable)*	
Contact	Computer Security Division (Information Technology Laboratory)
Latest revision of the attached publication	
Related Information	https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
Withdrawal Announcement Link	

Date updated: May 14, 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NIST SP 800-171, R2 &R3

Table 1. Security Requirement Families



Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response		Supply Chain Risk Management

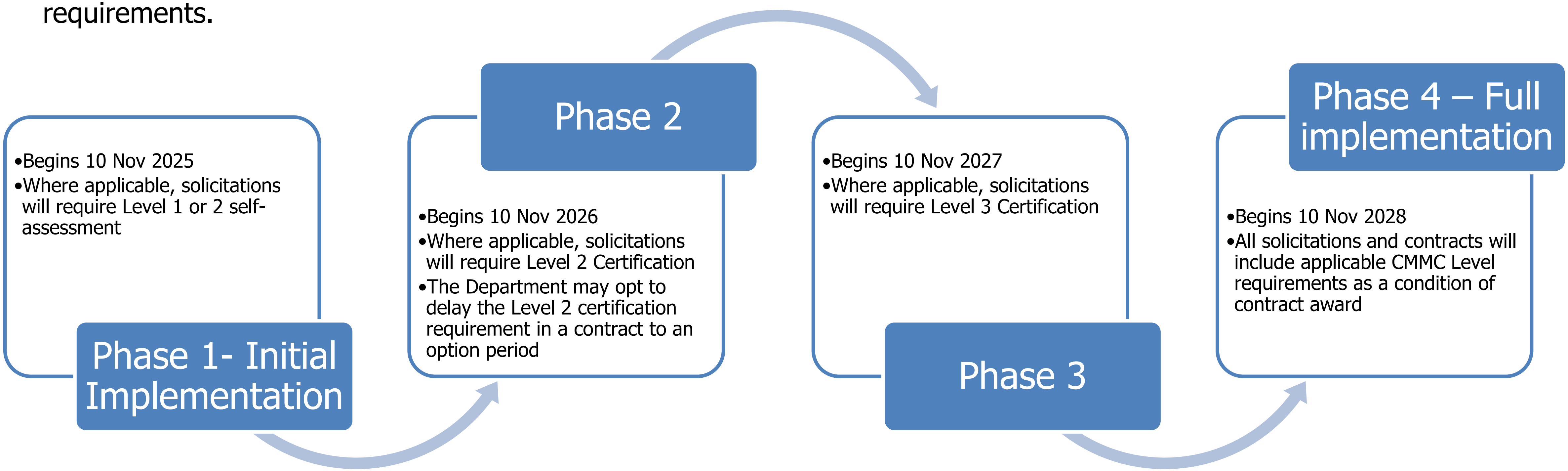
Microsoft Excel Worksheet

NIST SP 800-171A, R3

- **NIST SP 800-171A, Rev 2** (Assessing Security Requirements for Controlled Unclassified Information)
  - Assessment of institution IT network/system needs accomplished to identify areas of non-compliance

Phased Implementation of CMMC Requirements

The first phase of CMMC implementation will begin **November 10, 2025**. CMMC assessment requirements will be implemented using a four-phase plan over three years. The phases add CMMC Level requirements incrementally, starting with self-assessments in Phase 1, and ending with full implementation of program requirements in Phase 4. This phased approach allows time to train assessors and for companies to understand and implement CMMC assessment requirements.



Phase 1- Initial Implementation

- Begins 10 Nov 2025
- Where applicable, solicitations will require Level 1 or 2 self-assessment

Phase 2

- Begins 10 Nov 2026
- Where applicable, solicitations will require Level 2 Certification
- The Department may opt to delay the Level 2 certification requirement in a contract to an option period

Phase 3

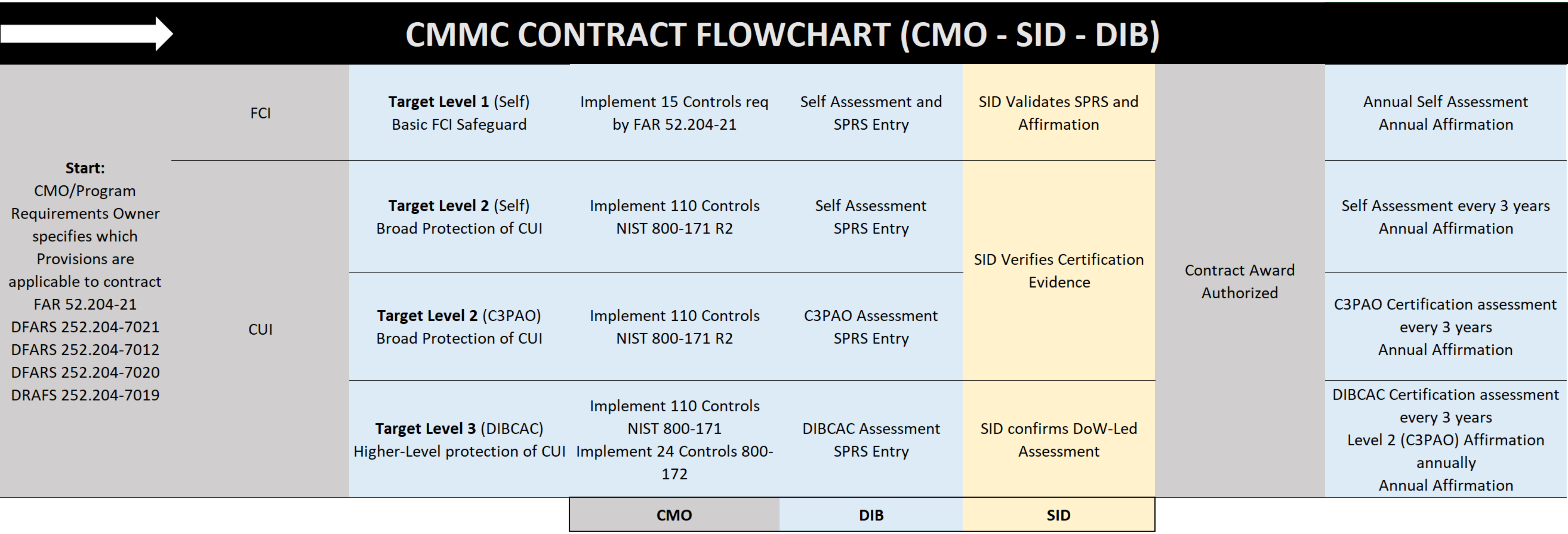
- Begins 10 Nov 2027
- Where applicable, solicitations will require Level 3 Certification

Phase 4 – Full implementation

- Begins 10 Nov 2028
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

In some procurements, DoW may implement CMMC requirements in advance of the planned phase

CMMC Contract Flowchart (CMO-DIB-SID)



CMMC CONTRACT FLOWCHART (CMO - SID - DIB)

Start: CMO/Program Requirements Owner specifies which Provisions are applicable to contract FAR 52.204-21 DFARS 252.204-7021 DFARS 252.204-7012 DFARS 252.204-7020 DRAFS 252.204-7019	FCI	**Target Level 1** (Self) Basic FCI Safeguard	Implement 15 Controls req by FAR 52.204-21	Self Assessment and SPRS Entry	SID Validates SPRS and Affirmation	Contract Award Authorized	Annual Self Assessment Annual Affirmation
	CUI	**Target Level 2** (Self) Broad Protection of CUI	Implement 110 Controls NIST 800-171 R2	Self Assessment SPRS Entry	SID Verifies Certification Evidence		Self Assessment every 3 years Annual Affirmation
		Target Level 2 (C3PAO) Broad Protection of CUI	Implement 110 Controls NIST 800-171 R2	C3PAO Assessment SPRS Entry			C3PAO Certification assessment every 3 years Annual Affirmation
		Target Level 3 (DIBCAC) Higher-Level protection of CUI	Implement 110 Controls NIST 800-171 Implement 24 Controls 800-172	DIBCAC Assessment SPRS Entry	SID confirms DoW-Led Assessment		DIBCAC Certification assessment every 3 years Level 2 (C3PAO) Affirmation annually Annual Affirmation

CMO	DIB	SID

NIST Recommended Solutions to Challenges

- **Targeted cybersecurity resources**
  - Developed resources that are specific to particular fields of research and could emphasize the risks, impacts, and importance of applying cybersecurity within the research context.
- **Collaborative engagements**
  - Collaborating with existing research communities and the need for more collaboration with Federal Government entities. (e.g. EDUCASE HEISC, NSF RRCoP, Trusted CI, RENH-ISAC, National Laboratories)
- **Training**
  - Training 431 resources designed for researchers and their teams could raise awareness about the importance of cybersecurity, particularly cybersecurity's value in preserving data integrity.
- **Guidance for frameworks**
  - Tailoring certain frameworks to support research environments could help ease the integration of cybersecurity while simplifying the process and minimizing operational overhead.
- **Grant guidance for security compliance**
  - Effective grant writing guidance that considers security, compliance, and research environments hosted at higher education institutions.
- **Shared services support**
  - Increasing awareness of available shared service opportunities and developing trusted cybersecurity services can help mitigate limited cybersecurity budgets for many institutions

CMMC 2.0

Please send all questions to CMMC@darpa.mil

CMMC 2.0

Resources

- The DoW CIO CMMC website houses a broad range of resources, including CMMC scoping and assessment guides: https://DoWcio.defense.gov/cmmc/ResourcesDocumentation/
- To locate certified CMMC assessors, trainers, and instructors that companies can engage now to prepare for CMMC implementation, visit the CMMC Accreditation Body Marketplace: https://www.cyberab.org/marketplace
- The Defense Acquisition University offers free online CMMC training: https://www.dau.edu/courses/cyb-1010 & https://www.dau.edu/courses/cyb-1030
- The Department's CUI Quick Reference Guide includes information on the marking and handling of CUI: https://www.DoWcui.mil/
- The DoW CMMC eMASS Systems of Record https://cmmc.emass.apps.mil/
- To find a FedRAMP Moderate Authorized Service Provider, please visit: https://marketplace.fedramp.gov/assessors
- DoW's Office of Small Business Programs has compiled a list of resources on their website that are aimed at helping small- and medium-sized businesses understand security requirements and reach compliance: https://business.defense.gov/Resources/FAQs/

Resources

- **32 CFR Part 170:** Cybersecurity Maturity Model Certification (CMMC) Program
- **48 CFR Parts 204, 212, 217, and 252:** Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)
- **CMMC 101 Brief:** CMMC 101 Brief
- **CMMC Overview Briefing (Audio):** CMMC Overview Briefing (Audio)
- **CMMC Model Overview:** CMMC Program Model Overview
- **CMMC Level 1 Scoping Guidance:** CMMC Level 1 Scoping Guidance
- **CMMC Level 1 Self-Assessment Guide:** CMMC Level 1 Self-Assessment Guide
- **CMMC Level 2 Scoping Guidance:** CMMC Level 2 Scoping Guidance
- **CMMC Level 2 Assessment Guide:** CMMC Level 2 Assessment Guide
- **CMMC Level 3 Scoping Guidance:** CMMC Level 3 Scoping Guidance
- **CMMC Level 3 Assessment Guide:** CMMC Level 3 Assessment Guide
- **CMMC Hashing Guide:** CMMC Hashing Guide
- **CMMC Briefing:** CMMC Alignment to NIST Standards (Feb 2025)
- **CMMC Briefing:** DoW SPRS (Feb 2025)
- **CMMC Briefing:** CMMC eMASS (Feb 2025)
- **CMMC Briefing:** FedRAMP Authorization and Equivalency (Feb 2025)
- **CMMC Briefing:** Levels Determination (Feb 2025)
- **CMMC Briefing:** Technical Implementation of CMMC Requirements (Feb 2025)
- **DoW Memo:** Organization-Defined Parameters for NIST SP 800-171 Rev3 (Feb 2025)

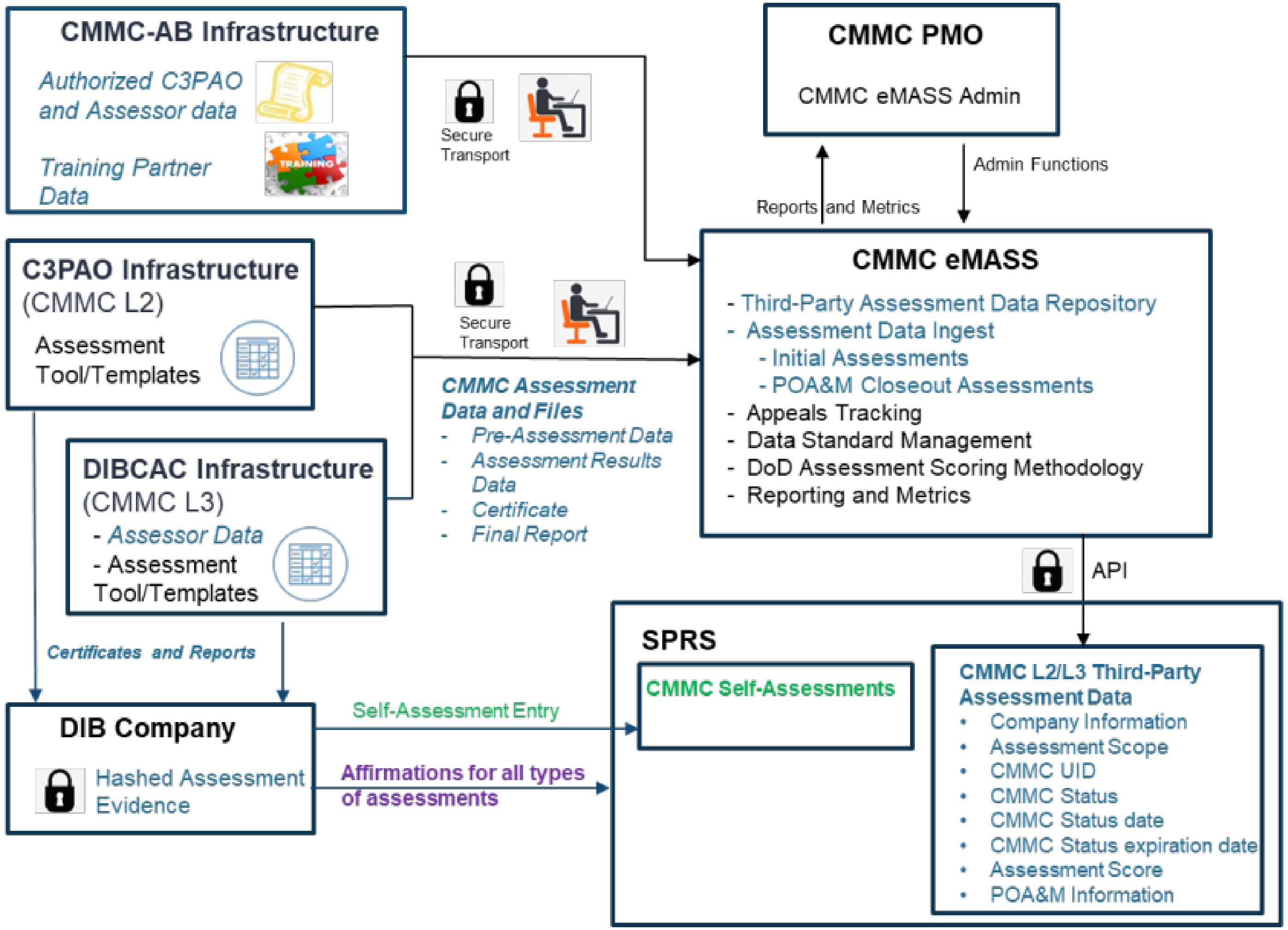
Acronym Glossary

Acronym	Meaning
AB	Accreditation Body
CAICO	Cybersecurity Assessor and Instructor Certification Organization
CIO	Chief Information Officer (DoW)
CFR	Code of Federal Regulations
CMMC	Cybersecurity Maturity Model Certification
CCPs/CCAs/CCIs	CMMC Certified Professionals/Assessors/Instructors
C3PAO	Certified Third-Party Assessment Organization
CUI	Controlled Unclassified Information
DCMA	Defense Contract Management Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DoW	Department of War
eMASS	Enterprise Mission Assurance Support Service
EO	Executive Order
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FCI	Federal Contract Information
FIPS	Federal Information Processing Standards
IAW	In Accordance With
IG	Inspector General

Acronym	Meaning
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
MFA	Multi-Factor Authentication
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NLT	No Later Than
POA&M	Plan of Action and Milestones
Rev	Revision
RFI	Request for Information
RFP	Request for Proposal
SP	Special Publication
SPRS	Supplier Performance Risk System
QC	Quality Check

CMMC eMASS (Enterprise Mission Assurance Support Service) Overview

- The Cybersecurity Maturity Model Certification (CMMC) eMASS is a tailored version of DoW's eMASS that is used to store, track, and report on CMMC Level 2 and Level 3 assessment data
- CMMC eMASS is the data repository for CMMC assessment and supporting data. It does not contain proprietary data (e.g., assessment evidence)
- CMMC eMASS is also the engine for tracking assessments, Plans of Actions and Milestones (POA&Ms), and appeals actions, and is a mechanism used for reporting/tracking CMMC metrics



CMMC-AB Infrastructure
Authorized C3PAO and Assessor data
Training Partner Data

Secure Transport

CMMC PMO
CMMC eMASS Admin

Reports and Metrics

Admin Functions

C3PAO Infrastructure (CMMC L2)
Assessment Tool/Templates

Secure Transport

CMMC eMASS
- Third-Party Assessment Data Repository
- Assessment Data Ingest
  - Initial Assessments
  - POA&M Closeout Assessments
- Appeals Tracking
- Data Standard Management
- DoD Assessment Scoring Methodology
- Reporting and Metrics

DIBCAC Infrastructure (CMMC L3)
- *Assessor Data*
- Assessment Tool/Templates

CMMC Assessment Data and Files
- *Pre-Assessment Data*
- *Assessment Results Data*
- *Certificate*
- *Final Report*

API

Certificates and Reports

DIB Company
Hashed Assessment Evidence

Self-Assessment Entry

Affirmations for all types of assessments

SPRS

CMMC Self-Assessments

CMMC L2/L3 Third-Party Assessment Data
- Company Information
- Assessment Scope
- CMMC UID
- CMMC Status
- CMMC Status date
- CMMC Status expiration date
- Assessment Score
- POA&M Information

https://cmmc.emass.apps.mil/

Cybersecurity Maturity Model Certification (CMMC)

- CMMC provides the DoW with increased assurance that contractors and subcontractors are meeting the cybersecurity requirements for nonfederal systems processing controlled unclassified information.

- Tiered System
  - Level 3 (Higher-Level Protection of CUI Against Persistent Threats, Extra Sensitive CUI (e.g. NUC, UCNI, NNPI, etc.)
    - 134 requirements [110 from NIST SP 800-171, 24 from NIST SP 800-172] (DFAR clause 252.204-7012)
    - Level 2 Certification pre-requisite
    - DIBCAC Certification Assessment every 3 years
    - Annual Affirmation

  - Level 2 (Broad Protection of CUI) – **Current DARPA Minimum Standard for Industry Performers**
    - 110 requirements (DFAR clause 252.204-7012)
    - C3PAO Certification Assessment every 3 years, or
    - Self Assessment every 3 years, certain programs
    - Annual Affirmation

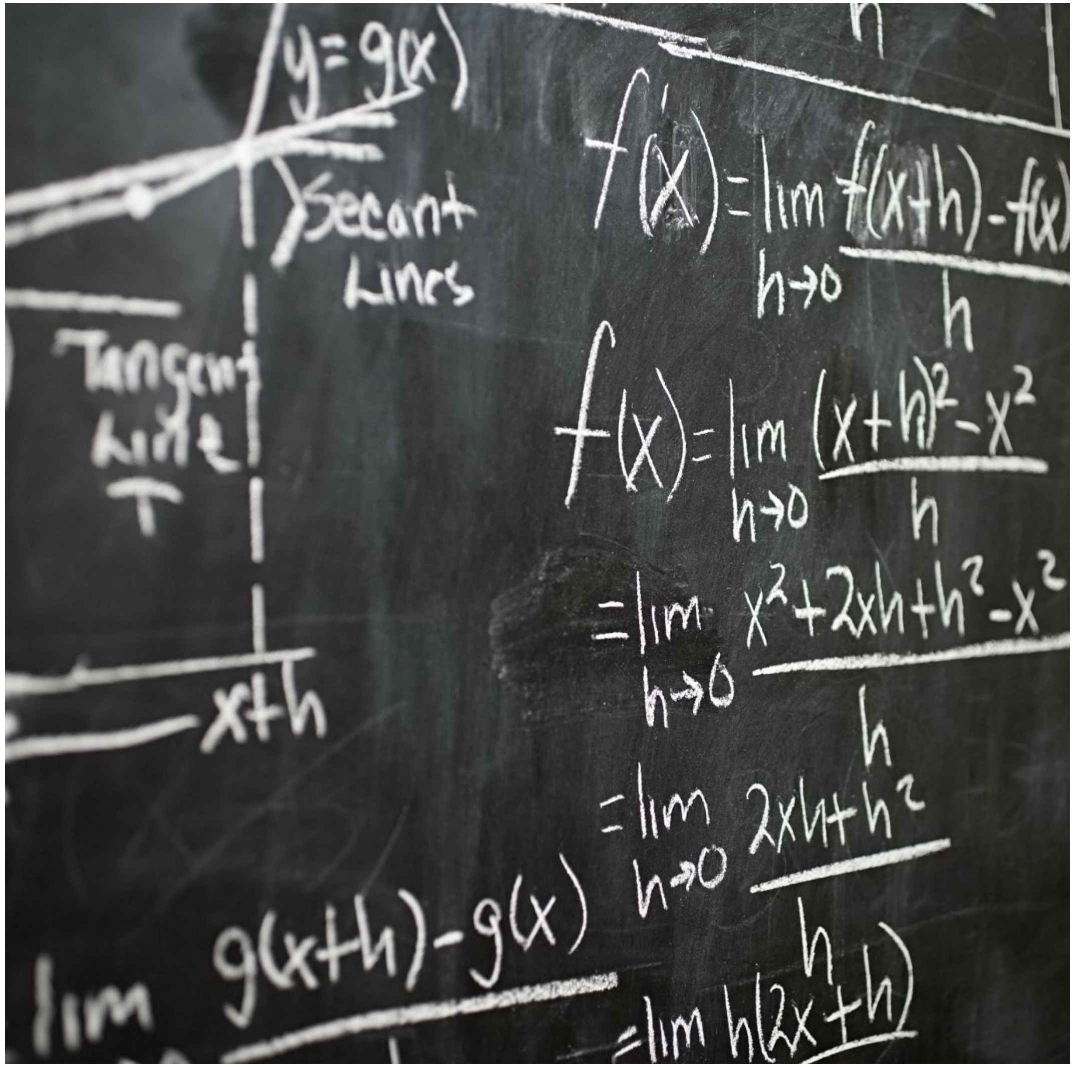
  - Level 1 (Basic Safeguarding of Unclassified Government Information)
    - 15 requirements (FAR clause 52.204-21)
    - Annual Self Assessment
    - Annual Self Affirmation

CMMC Scoring Methodology (§ 170.24)

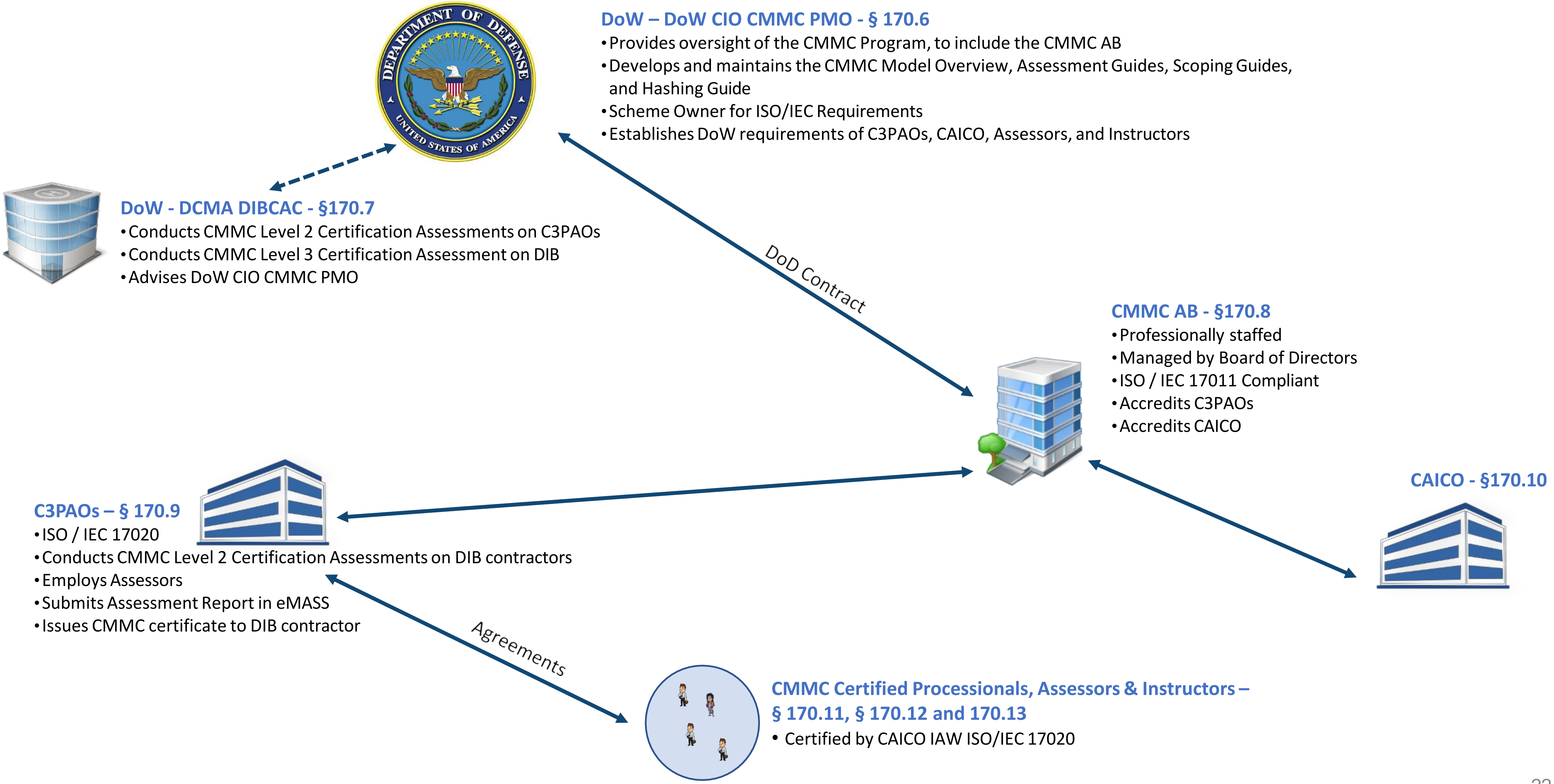
- Level 1: Score not required; either **MET** or **NOT MET**
- Level 2: Security requirements are valued 1, 3, or 5 points with a range of -203 to 110, with a minimum passing score of 88.

  Partial credit is allowed for 2 requirements:

  - MFA: 5 points deducted from overall score of 110 if MFA is not implemented or implemented only for general users and not remote and privileged users;
  - MFA: 3 points deducted if MFA is implemented for remote and privileged users but not implemented for general users;
  - FIPS: 5 points deducted from overall score of 110 if no cryptography is employed;
  - FIPS: 3 points deducted if cryptography is employed, but not FIPS validated.
- Level 3: All Level 3 security requirements are valued 1 point with a maximum score of 24. Requires a prerequisite Level 2 score of 110.
- Results for all Levels are posted in SPRS and reviewed by contracting officers and requiring activities.



CMMC Ecosystem



DoW – 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

CMMC AB - §170.8

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

CAICO - §170.10

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

CMMC Certified Processionals, Assessors & Instructors – § 170.11, § 170.12 and 170.13

- Certified by CAICO IAW ISO/IEC 17020

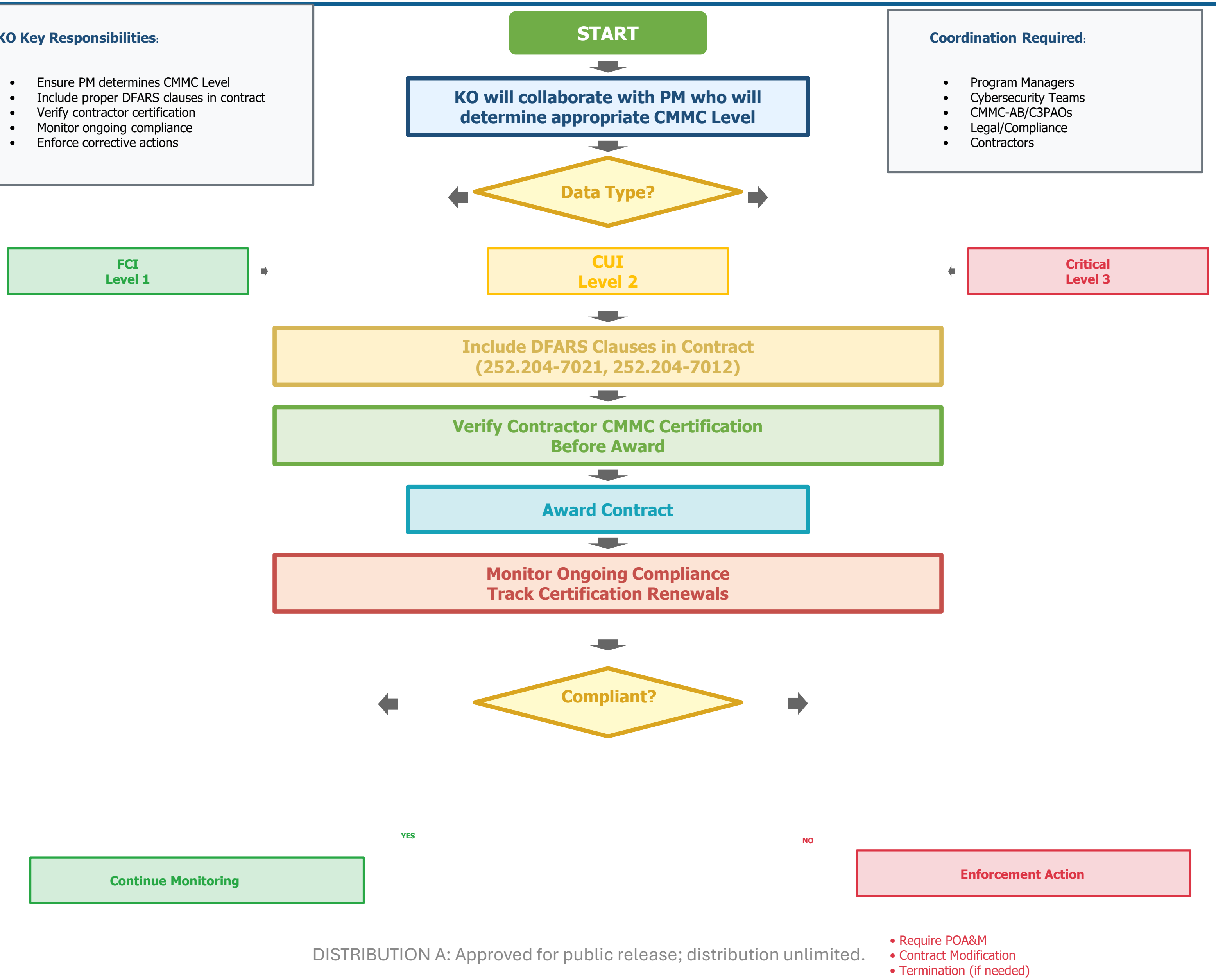
Contracting Officer/PM CMMC Responsibilities – Process Flow

KO Key Responsibilities:

- Ensure PM determines CMMC Level
- Include proper DFARS clauses in contract
- Verify contractor certification
- Monitor ongoing compliance
- Enforce corrective actions

Coordination Required:

- Program Managers
- Cybersecurity Teams
- CMMC-AB/C3PAOs
- Legal/Compliance
- Contractors



START

KO will collaborate with PM who will determine appropriate CMMC Level

Data Type?

FCI Level 1

CUI Level 2

Critical Level 3

Include DFARS Clauses in Contract (252.204-7021, 252.204-7012)

Verify Contractor CMMC Certification Before Award

Award Contract

Monitor Ongoing Compliance
Track Certification Renewals

Compliant?

YES

Continue Monitoring

NO

Enforcement Action

- Require POA&M
- Contract Modification
- Termination (if needed)

Additional Resources

- Please refer to the **official DoW CMMC Program website**, including the FAQ page, for more information about CMMC: https://DoWcio.defense.gov/CMMC/
- **DoW no-cost cybersecurity compliance resources** can be found at dibnet.DoW.mil under *DoW DIB Cybersecurity-As-A Service (CSaaS) Services and Support*.
- **Additional cybersecurity resources** can be found at:
  - https://www.cisa.gov/shields-up
  - https://www.nist.gov/mep
  - https://www.apexaccelerators.us/#/
- To **locate a C3PAO**, visit the CMMC Accreditation Body Marketplace at cyberab.org.
- To **obtain additional information on CMMC Assessments, Scoping, and Hashing**, visit: https://DoWcio.defense.gov/ cmmc/Resources-Documentation/
- The Department's **CUI Quick Reference Guide** includes information on the marking and handling of CUI: https:// www.DoWcui.mil/
- To find a **FedRAMP Moderate Authorized Service Provider**, please visit: https://marketplace.fedramp.gov/assessors