Cybersecurity Maturity Model Certification

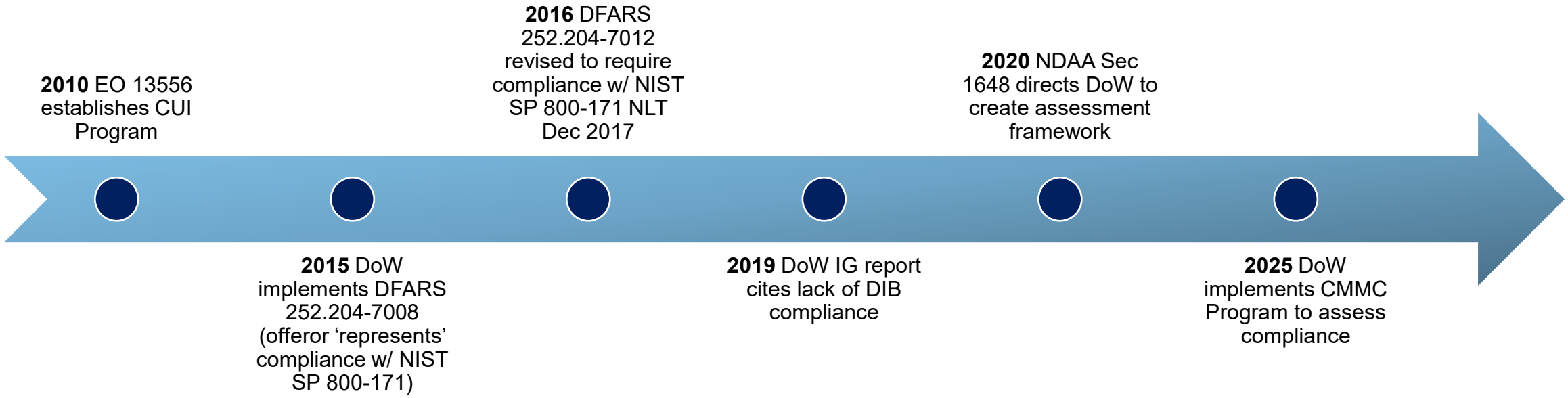
Overview

25-T-2910

Acronym Glossary included in slides 15-17

CMMC Program Overview and History

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

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

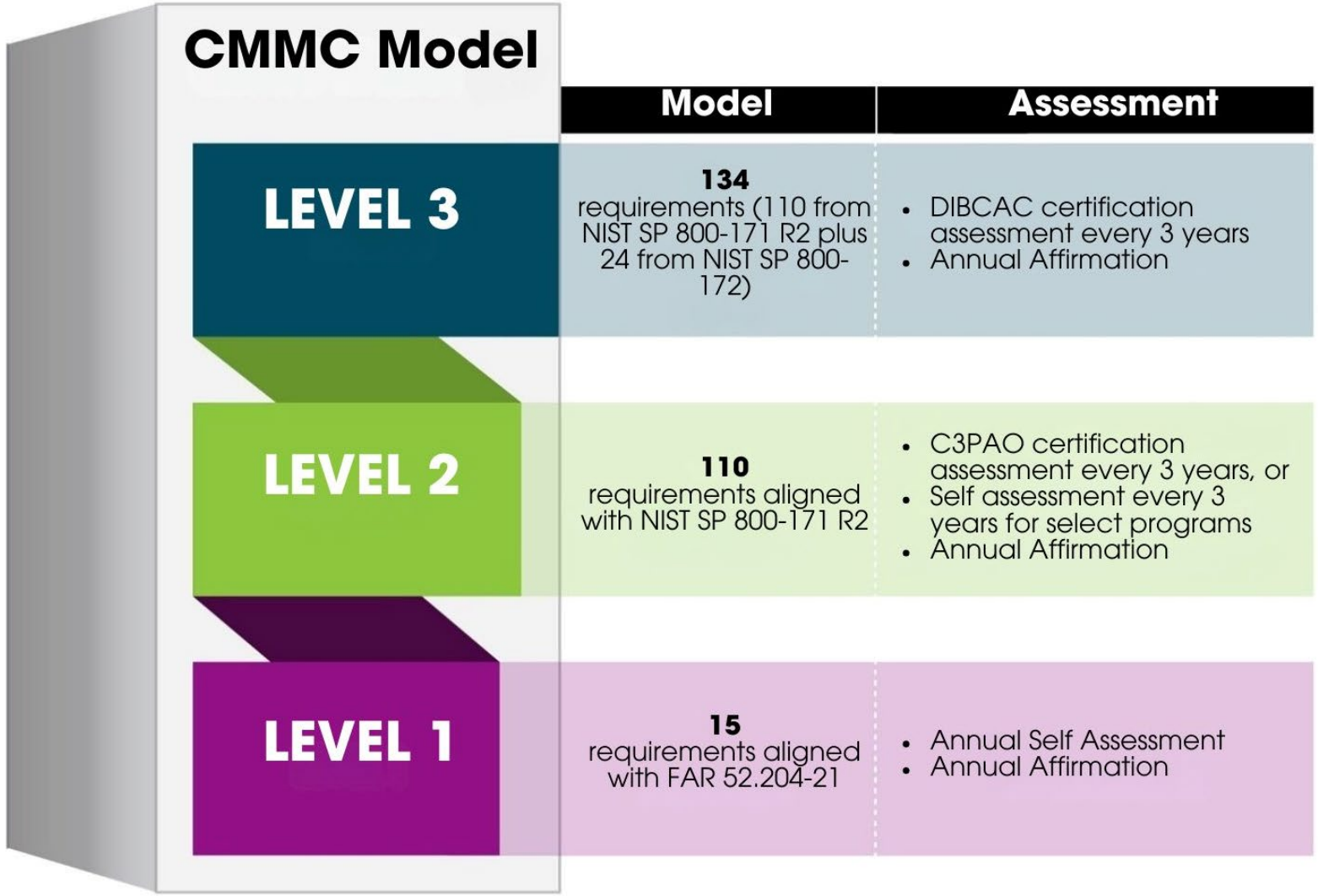
The CMMC Program does not alter separately applicable requirements to protect FCI or CUI

CMMC Implementation Through Contracts

- DFARS clause 252.204-7021
  - Relies on the requiring activity to identify the appropriate CMMC Status requirements based on the type of information to be processed, stored, or transmitted
  - Implements CMMC Program requirements codified in 32 CFR Part 170, which include:
    - Minimum passing score of 80% (88/110)
    - Restriction of items that can be identified on a POA&M
    - Maximum 180-day POA&M close-out date
    - Annual affirmation of continued compliance in SPRS
    - Flow-down of requirements to subcontractors

The Effective Date for the Final CMMC DFARS Clause is 10 Nov 2025

Revised CMMC Framework Requirements



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

CMMC Post-Assessment Remediation

❑ CMMC Program will allow limited use of POA&Ms

- POA&Ms are not allowed for CMMC Level 1.
- Refer to § 170.21 of the 32 CFR CMMC Program final rule for CMMC Level 2 and Level 3 POA&Ms requirements, including critical requirements not allowed in a POA&M.

❑ Closeout Assessment

- POA&M closeout self-assessment is conducted by the OSA.
- POA&M closeout Certification Assessment is conducted by a C3PAO or the DIBCAC.
- POA&Ms must be closed out within 180 days of when the CMMC Assessment results are finalized and submitted to SPRS or CMMC eMASS, as appropriate.

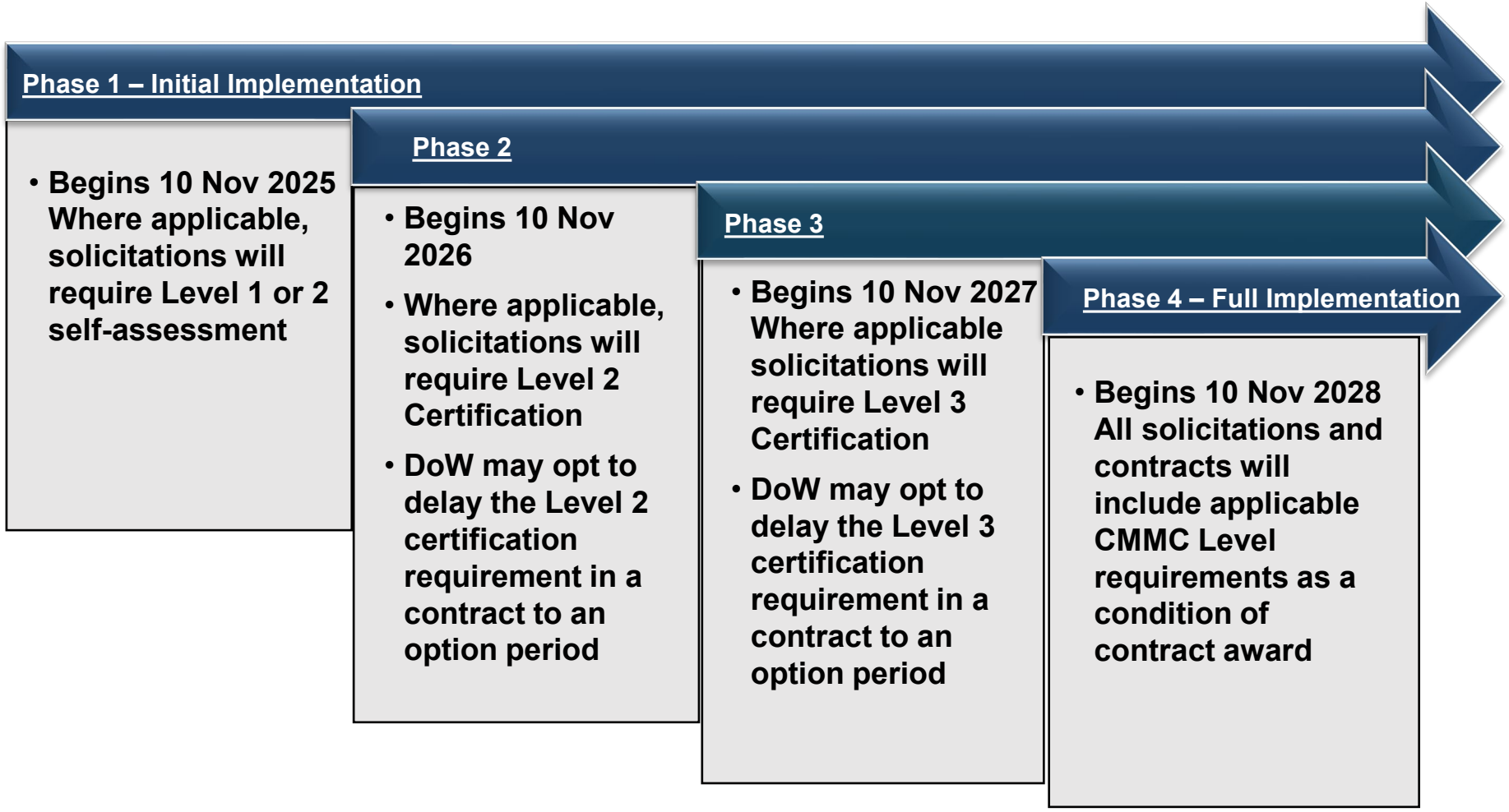
Failure to close POA&M within 180 days will result in an expired CMMC Status

Conditional and Final Status

- An Organization Seeking Assessment (OSA) may achieve a **Conditional CMMC Status** if the initial assessment (with passing score) resulted in allowable POA&M items.

- An Organization Seeking Certification (OSC) achieves a **Final CMMC Status** when assessment results in a passing score with no POA&M, or when the POA&M has been closed out within 180 days of achieving a Conditional CMMC Status.

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

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

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

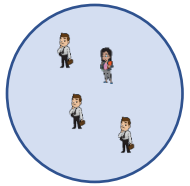
DoW Contract

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

Additional Resources

- The **DoW CIO CMMC website** houses a broad range of resources, including **CMMC scoping and assessment guides**: https://dodcio.defense.gov/cmmc/Resources-Documentation/

- To locate **certified CMMC assessors, trainers, and instructors that companies can engage now to prepare for CMMC implementation**, visit the CMMC Accreditation Body Marketplace: 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

Additional Resources Cont'd

- DoW **CUI Quick Reference Guide** includes information on the marking and handling of CUI: https://www.dodcui.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/
- Additional cybersecurity resources:
  - https://www.cisa.gov/shields-up
  - https://www.nist.gov/mep
  - https://www.apexaccelerators.us/#/

Acronym Glossary (1 of 3)

Acronym	Meaning
AB	Accreditation Body
CAICO	Cybersecurity Assessor and Instructor Certification Organization
CIO	Chief Information Officer (Department of War)
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

Acronym Glossary (2 of 3)

Acronym	Meaning
EO	Executive Order
FAR	Federal Acquisition Regulation
FAQ	Frequently Asked Question
FedRAMP	Federal Risk and Authorization Management Program
FCI	Federal Contract Information
FIPS	Federal Information Processing Standards
IAW	In Accordance With
IG	Inspector General
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
MFA	Multi-Factor Authentication
NDAA	National Defense Authorization Act

Acronym Glossary (3 of 3)

Acronym	Meaning
NIST	National Institute of Standards and Technology
NLT	No Later Than
POA&M	Plan of Action and Milestones
PMO	Program Management Office
Rev	Revision
RFI	Request for Information
RFP	Request for Proposal
SP	Special Publication
SPRS	Supplier Performance Risk System
QC	Quality Check