SLIDES ONLY

NO SCRIPT PROVIDED

Cybersecurity Maturity Model Certification

Foreign Partner Integration into CMMC Ecosystem

Acronym Glossary included on slides 11-13

U.S. Federal CUI Safeguarding Requirements

The DoD follows a strict set of safeguarding requirements

The DoD adheres to the federal CUI safeguarding standard, as outlined in 32 CFR Part 2002, and implements NIST SP 800-171 requirements via DFARS 252.204-7012

- **The DoD follows the federal CUI safeguarding standard**
  - 32 CFR Part 2002 establishes federal policy for designating, handling, and decontrolling information that qualifies as CUI
    - § 2002.14: Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on nonfederal information systems
- **32 CFR Part 170 codifies DoD policy for verifying compliance with NIST SP 800-171 through CMMC assessment**
  - Compliance will be assessed in accordance with new contractual requirements, as proposed in 48 CFR
- **Countries may have their own national standards, creating a need to:**
  - Compare the foreign standard against NIST SP 800-171 to identify requirement gaps (“crosswalk”)
  - Meet NIST SP 800-171 requirement gaps for DoD procurements containing CUI safeguarding requirements

Compliance with DoD Cybersecurity Requirements

Foreign partners can integrate into the existing CMMC Program

Foreign partners can participate in the accreditation process, submit self-assessments, and comply with DoD cybersecurity requirements to participate in DoD procurements

- **DoD's CUI safeguarding requirements and associated compliance assessments apply uniformly to all contractors**
- **Accordingly, the DoD implements the following standards:**
  - FAR 52.204-21 is the USG's basic safeguarding requirement; CMMC Level 1 self-assessment will be required
  - DFARS clause 252.204-7012 is DoD's covered defense information safeguarding requirement; various assessments are required by DFARS clauses 252.204-7019, 7020, and 7021

Foreign partners must meet the same cybersecurity requirements as U.S. companies

Foreign companies will submit self-assessments, as required, and must comply with DoD cybersecurity requirements to participate in DoD procurements

- **CMMC assessment requirements are codified in 32 CFR Part 170 and provide for international compliance with and participation in the CMMC ecosystem**
  - Foreign companies will submit self-assessments, as required
  - The CMMC Program does not prohibit foreign citizens from becoming CCAs or foreign companies from becoming authorized/accredited as C3PAOs
  - Companies may employ assessment services from any authorized/accredited C3PAO or CCA

Participation in the CMMC Ecosystem

Foreign partners must meet specific requirements to participate in the CMMC ecosystem

Foreign assessors must complete a Tier 3 background investigation or equivalent, pass the CAICO-managed CMMC assessor certification exam, and comply with ISO/IEC 17011:2017, 17020:2012, and ISO/IEC 17024:2012 standards

- **Any organization that meets all requirements of 32 CFR § 170.9 can operate as a C3PAO**
- **Any individual that meets all requirements of 32 CFR § 170.11 or § 170.13 can act as a CCA or CCP, respectively**
  - Foreign assessors must complete a Tier 3 background investigation or equivalent
  - Foreign assessors must complete and pass the CAICO-managed CMMC assessor certification exam
  - Foreign assessors can take CAICO provided training, or foreign partners may obtain CAICO training materials and blueprints to develop their own training
  - Foreign Assessors may be employed by U.S.-based or foreign C3PAOs

The DoD recognizes a single CMMC Accreditation Body (CMMC AB)

- **The CMMC AB can accredit U.S.-based or foreign candidate C3PAOs (when all requirements are met)**
- **32 CFR Part 170 allows the CMMC AB to establish Mutual or Multilateral Recognition Arrangements with other accreditation, inspection, and personnel certification bodies, in accordance with ISO/IEC**

The CMMC Program is open to foreign participation

The CMMC Program does not prohibit foreign citizens from becoming CCAs or foreign companies from becoming authorized/accredited as C3PAOs

- **In accordance with 32 CFR Part 170, DCMA's DIBCAC performs all CMMC Level 3 and candidate C3PAO Level 2 assessments**
  - Foreign partners may participate jointly in DCMA DIBCAC on-site assessment activities

CMMC Ecosystem

DoD – DoD 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 DoD requirements of C3PAOs, CAICO, Assessors, and Instructors

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

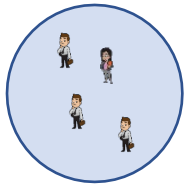
DoD Contract

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

Agreements

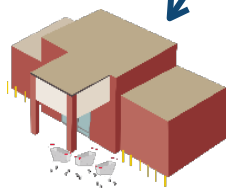


CMMC Certified Professionals, Assessors & Instructors – § 170.11, § 170.12 and § 170.13
- Certified by CAICO IAW ISO/IEC 17024

CAICO

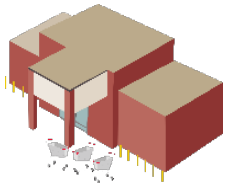
CMMC Assessor and Instructor Certification Organization - § 170.10

- ISO/IEC 17024
- Certifies CMMC Certified Professionals, Assessors, and Instructors
- Defines knowledge areas required for CCPs, CCAs, and CCIs with input from DoD
- QCs curriculum developed by ecosystem



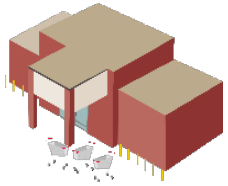
Approved Publisher Partners

- Develops Training Materials



Approved Training Providers

- Trains Certified Professionals
- Trains Assessors
- Trains Instructors
- In-person / Virtual / Hybrid



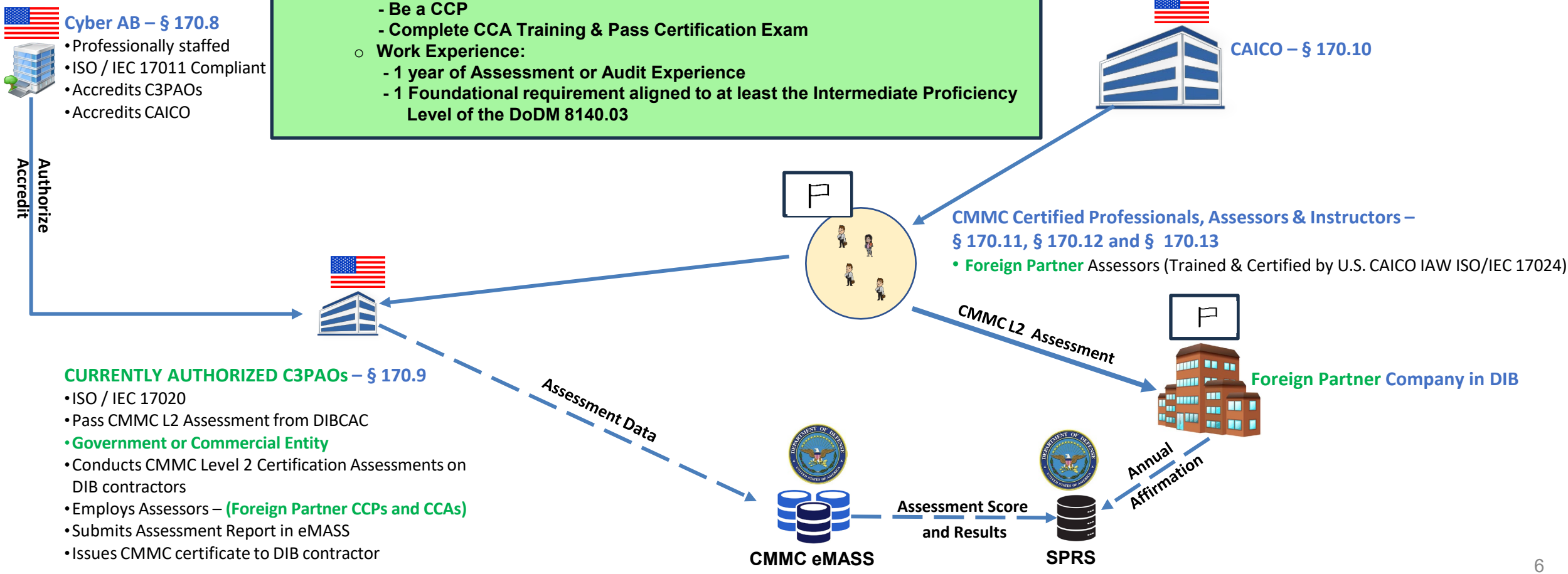
Approved CMMC Exam Org

- Develops and administers Assessor and Instructor Certification Exams

Foreign Partner Integration into CMMC – Course of Action 1 for CMMC L2

COA 1: Existing Authorized C3PAOs

- Use existing Accreditation Body – Cyber AB
- Use existing CAICO
- Add new Foreign Partner CCPs and CCAs
  - Favorable Tier 3 Background Investigation
  - CCP: Complete Training & Pass Certification Exam
  - CCA:
    - Be a CCP
    - Complete CCA Training & Pass Certification Exam
  - Work Experience:
    - 1 year of Assessment or Audit Experience
    - 1 Foundational requirement aligned to at least the Intermediate Proficiency Level of the DoDM 8140.03



Foreign Partner Integration into CMMC – Course of Action 2 for CMMC L2

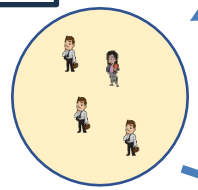
COA 2: New Authorized Foreign Partner C3PAOs

- Use existing Accreditation Body – Cyber AB
- Use existing U.S. CAICO
- Add new Foreign Partner CCPs and CCAs
  - Favorable Tier 3 Background Investigation
  - CCP: Complete Training & Pass Certification Exam
  - CCA:
    - Be a CCP
    - Complete CCA Training & Pass Certification Exam
  - Work Experience:
    - 1 year of Assessment or Audit Experience
    - 1 Foundational requirement aligned to at least the Intermediate Proficiency Level of the DoDM 8140.03

Cyber AB – § 170.8
- Professionally staffed
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO

Authorize
Accredit

CAICO – § 170.10



CMMC Certified Professionals, Assessors & Instructors – § 170.11, § 170.12 and § 170.13
- Foreign Partner Assessors (Trained and Certified by U.S. CAICO IAW ISO/IEC 17024)

NEW Int'l Partner AUTHORIZED C3PAOs – § 170.9
- ISO / IEC 17020
- Pass CMMC L2 Assessment from DIBCAC
- Government or Commercial Entity
- Conducts CMMC Level 2 Certification Assessments on DIB contractors
- Employs Assessors – (Foreign Partner CCPs and CCAs)
- Submits Assessment Report in eMASS through CMMC PMO
- Issues CMMC certificate to DIB contractor

Assessment Data (Through CMMC PMO)

CMMC L2 Assessment

Foreign Partner Company in DIB

CMMC eMASS

Assessment Score and Results

SPRS

Annual Affirmation

Foreign Partner Integration into CMMC – Course of Action 3 for CMMC L2

COA 3: New Foreign Partner CMMC Ecosystem

- Create new Foreign Partner Accreditation Body IAW ISO 17011
- Mutual Recognition Agreement between Existing Cyber AB and new Foreign Partner CMMC AB
- Create new Foreign Partner C3PAO accredited by Foreign Partner CMMC AB
- Use existing U.S. CAICO
- Use Foreign Partner CCPs and CCAs Trained by U.S. CAICO approved ATP
  - Favorable Tier 3 Background Investigation
  - CCP: Complete Training & Pass Certification Exam
  - CCA:
    - Be a CCP
    - Complete CCA Training & Pass Certification Exam
  - Work Experience:
    - 1 year of Assessment or Audit Experience
    - 1 Foundational requirement aligned to at least the Intermediate Proficiency Level of the DoDM 8140.03

Cyber AB – § 170.8
- Professionally staffed
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO

MRA

Foreign Partner CMMC AB – § 170.8
- Professionally staffed
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO

Authorize
Accredit

CAICO – §170.10

CMMC Certified Professionals, Assessors & Instructors – § 170.11, § 170.12 and 170.13
- Foreign Partner Assessors (Trained and Certified by U.S. CAICO IAW ISO/IEC 17024)

NEW Foreign Partner AUTHORIZED C3PAOs – § 170.9
- ISO / IEC 17020
- Pass CMMC L2 Assessment from DIBCAC
- Government or Commercial Entity
- Conducts CMMC Level 2 Certification Assessments on DIB contractors
- Employs Assessors – (Foreign Partner CCPs and CCAs)
- Submits Assessment Report in eMASS through CMMC PMO
- Issues CMMC certificate to DIB contractor

Assessment Data (Through CMMC PMO)

CMMC L2 Assessment

Foreign Partner Company in DIB

Annual Affirmation

CMMC eMASS

Assessment Score and Results

SPRS

Backups

Acronym Glossary

Acronym	Meaning
AB	Accreditation Body
CAICO	Cybersecurity Assessor and Instructor Certification Organization
CIO	Chief Information Officer (DoD)
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
DoD	Department of Defense
eMASS	Enterprise Mission Assurance Support Service

Acronym Glossary Cont'd

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 Final

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

CMMC

What:

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

Why:

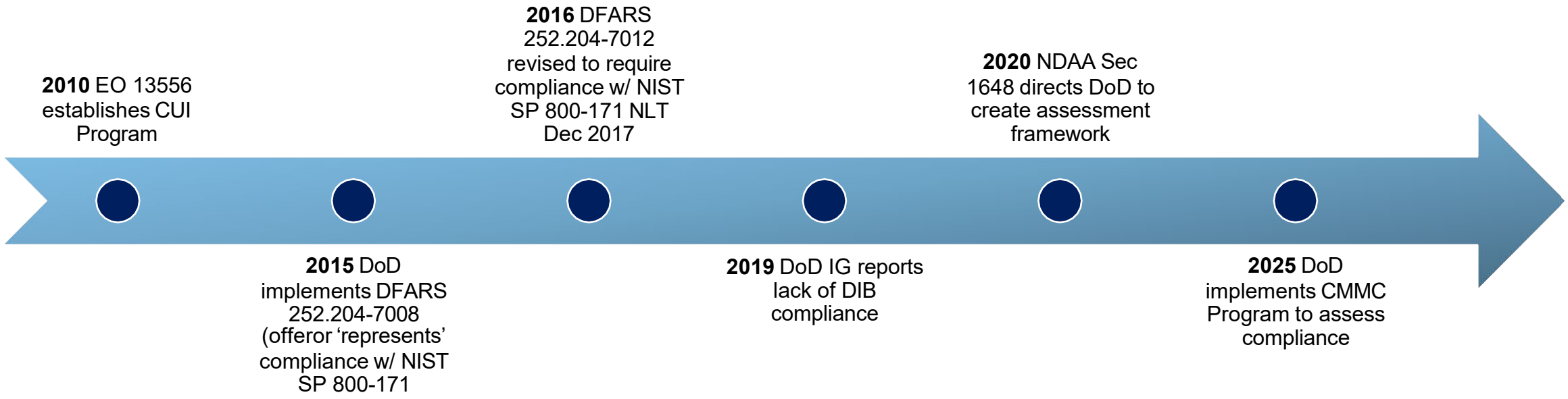
To increase the cybersecurity posture of the DIB and better protect sensitive unclassified information.

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).

CMMC Program Overview and History

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



Safeguarding FCI and CUI

Safeguarding Requirements for Nonfederal Information Systems

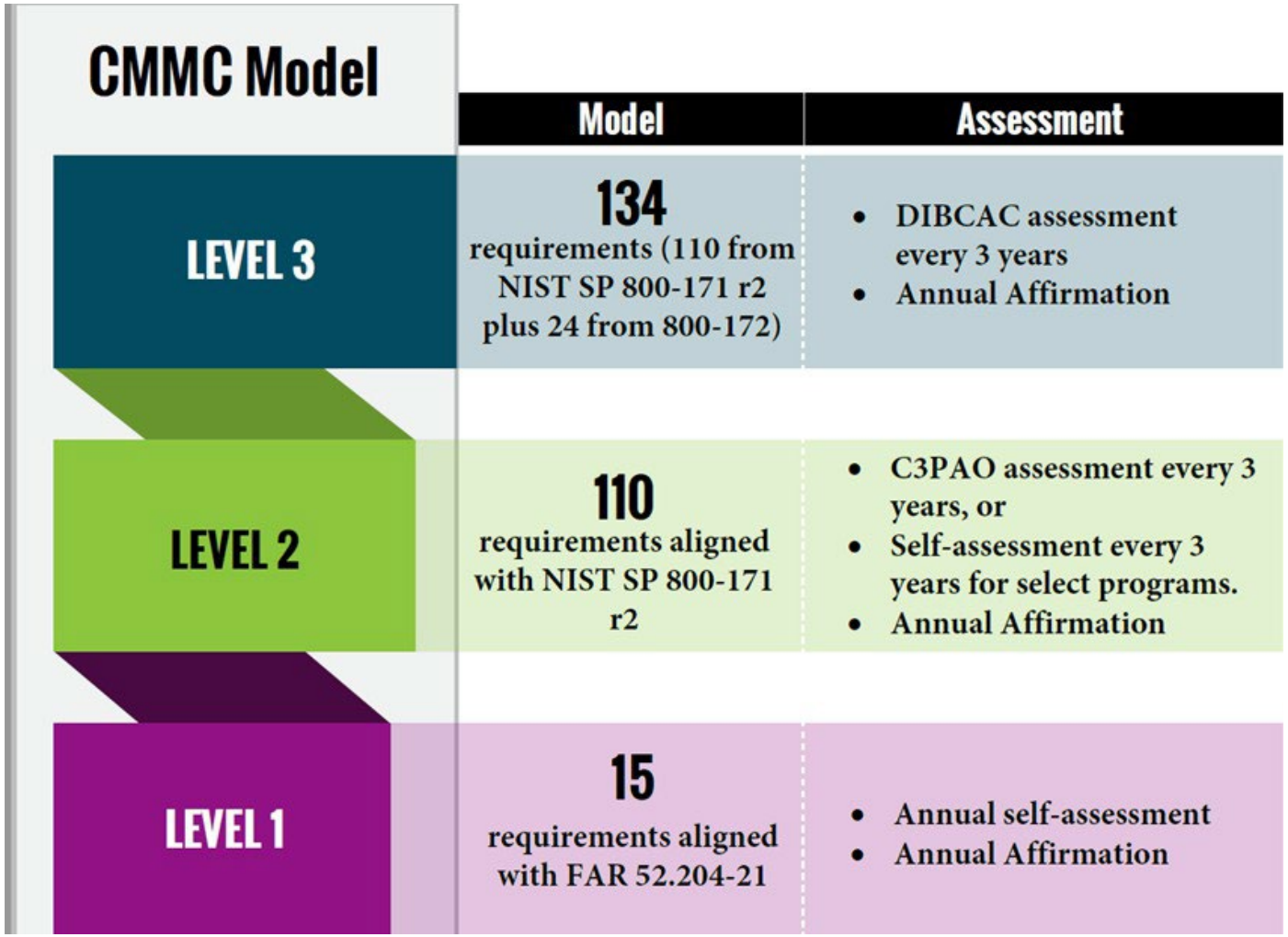
FCI

- Information that is not marked as public or for public release and is not designated as CUI
- Defined in FAR 52.204-21
- Minimum safeguarding requirement: 48 CFR 52.204-21

CUI

- Information that is marked or identified as requiring safeguarding in the DoD CUI Program
- Defined in 32 CFR Part 2002
- Minimum safeguarding requirement: NIST SP 800-171

Revised CMMC Framework Requirements



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

CMMC Alignment to NIST SP 800-171 Revisions

- DoD followed federal rulemaking guidelines when aligning CMMC assessment requirements to NIST SP 800-171 **Rev 2.**

- Defense contractors can implement NIST SP 800-171 Rev 3, but must comply with **Rev 2 requirements not covered in Rev 3** to meet CMMC assessment requirements.

- DoD will incorporate Rev 3 with future rulemaking.

Existing DoD Cybersecurity Requirements

- DFARS clause 252.204-7012 – **Effective Oct 2016 (to be implemented NLT Dec 2017)**
  - Safeguard DoD 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 DoD 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 DoD contractor has implemented these standards

The CMMC Clause

- 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
  - Requires the contractor/subcontractor 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

DoD is updating Title 48 CFR (the DFARS) to include revised CMMC Requirements

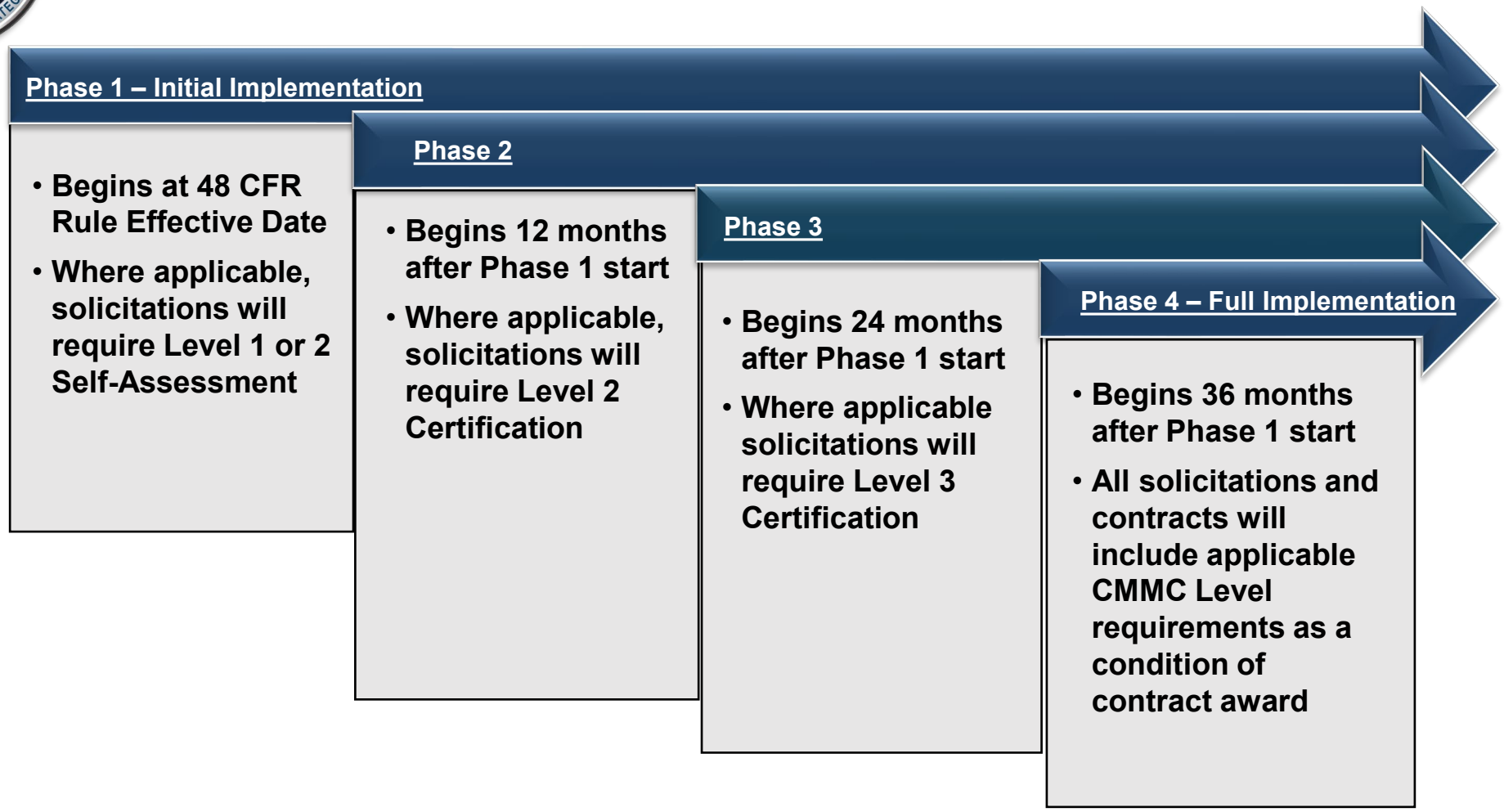
Existing DoD Cybersecurity & Assessment Requirements

Compliance with DoD cybersecurity requirements is mandatory

Contractors must comply with DFARS clauses 252.204-7012, 252.204-7019, 252.204-7020, and 252.204-7021 to participate in DoD procurements containing CUI safeguarding requirements.

- DFARS clause 252.204-7012 – **Effective Oct 2016**
  - Provide *adequate security* on covered contractor information systems (i.e., implement NIST SP 800-171 "as soon as practical, but NLT Dec 31, 2017" on systems that process, store, or transmit covered defense information)
  - Report cyber incidents that affect covered contractor information systems or covered defense information residing therein, or that affects ability to perform operationally critical support requirements identified in the contract
- DFARS Provision 252.204-7019 – **Effective Nov 2020**
  - Advises offerors subject to NIST SP 800-171 requirements to have a current NIST SP 800-171 DoD Assessment on record (in SPRS) to be considered for award
  - Current is defined as not more than three (3) years old unless a lesser time is specified in the solicitation
- DFARS clause 252.204-7020 – **Effective Nov 2020**
  - Provide access to facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment (if necessary)
  - Include requirements of the clause in all applicable subcontracts and ensure applicable subcontractors have the results of a current assessment posted in SPRS prior to awarding a subcontract
- DFARS clause 252.204-7021 (Proposed CMMC clause) – **Published for public comment Aug 2024, Effective TBD**
  - Provides for the assessment of contractor implementation of the above applicable security requirements

Phased Implementation of CMMC Requirements



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