

CLEARED  
For Open Publication

Oct 15, 2024

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

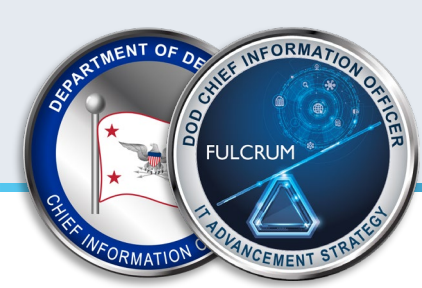


# Cybersecurity Maturity Model Certification

Overview

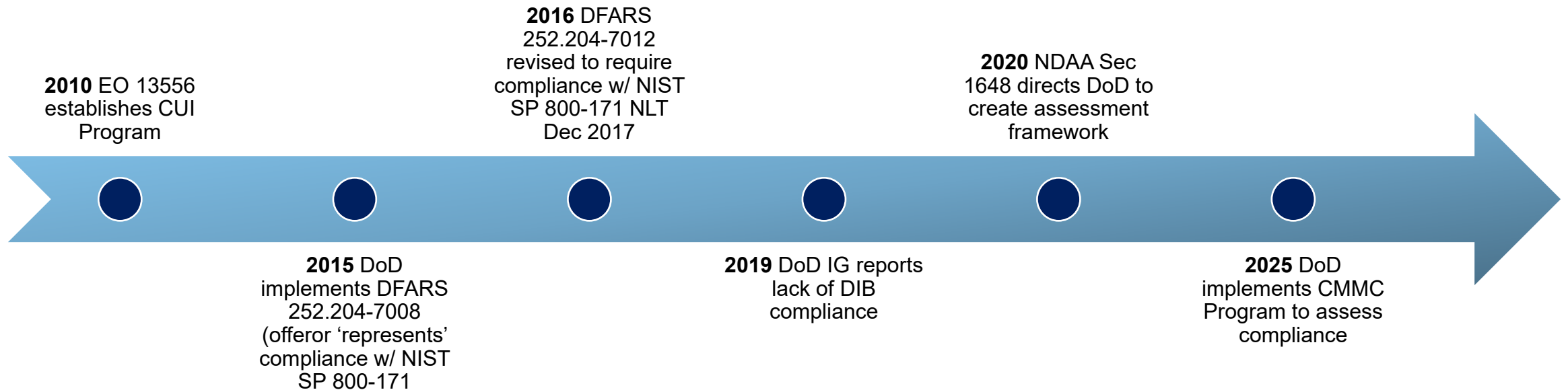
October 2024

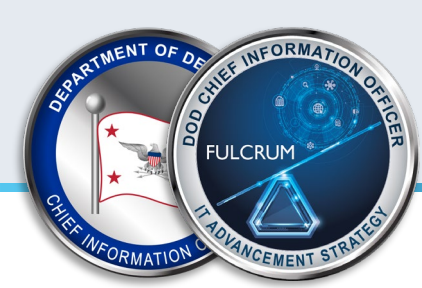
Acronym Glossary included in slides 20-21



# CMMC Program Overview and History

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





# CMMC



## **What:**

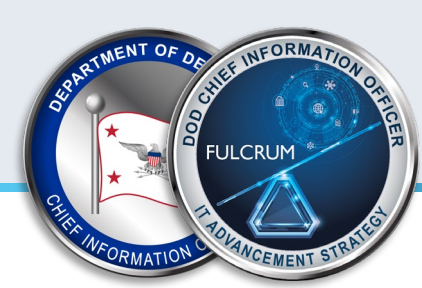
A consistent pre-award assessment methodology to determine whether a prospective contractor has implemented cybersecurity protections necessary to adequately safeguard DoD information.

## **Why:**

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

## **How:**

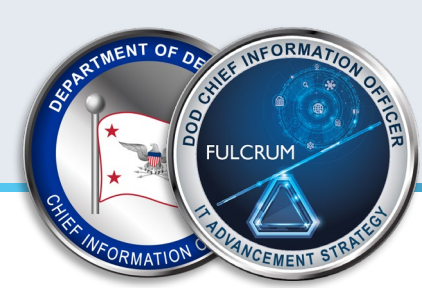
All defense contractors and subcontractors will show compliance with applicable security requirements through self-assessment or independent assessment, prior to contract award (excluding Commercial-Off-The-Shelf procurements).



# CMMC Applicability

- CMMC Program requirements will apply to all DoD 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 DoD solicitations
  - New DoD procurement instruments including contracts, task orders, delivery orders
  - As a condition to exercise an option period
  - Subcontractors are subject to flow-down requirements

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



# Safeguarding FCI and CUI

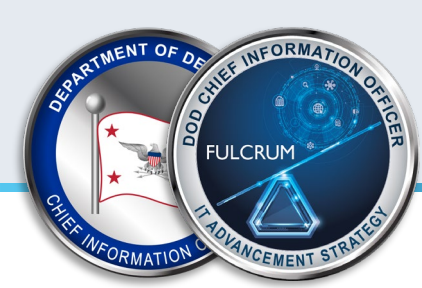
## Safeguarding Requirements for Nonfederal Information Systems

### 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

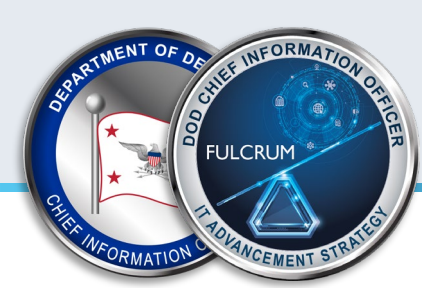
- Information that is marked or identified as requiring safeguarding in the DoD CUI Program
- Defined in 32 CFR Part 2002
- Minimum safeguarding requirement: NIST SP 800-171



# Existing DoD Cybersecurity Requirements

- **DFARS clause 252.204-7012 – Effective 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

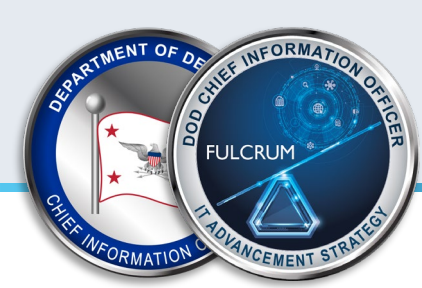
CMMC assesses whether a prospective DoD contractor has implemented these standards



# 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

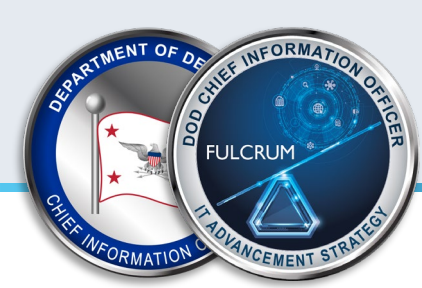


# Revised CMMC Framework Requirements

CMMC Model	Model	Assessment
<p><b>LEVEL 3</b></p>	<p><b>134</b> requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)</p>	<ul style="list-style-type: none"> <li>• DIBCAC assessment every 3 years</li> <li>• Annual Affirmation</li> </ul>
<p><b>LEVEL 2</b></p>	<p><b>110</b> requirements aligned with NIST SP 800-171 r2</p>	<ul style="list-style-type: none"> <li>• C3PAO assessment every 3 years, or</li> <li>• Self-assessment every 3 years for select programs.</li> <li>• Annual Affirmation</li> </ul>
<p><b>LEVEL 1</b></p>	<p><b>15</b> requirements aligned with FAR 52.204-21</p>	<ul style="list-style-type: none"> <li>• Annual self-assessment</li> <li>• Annual Affirmation</li> </ul>

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

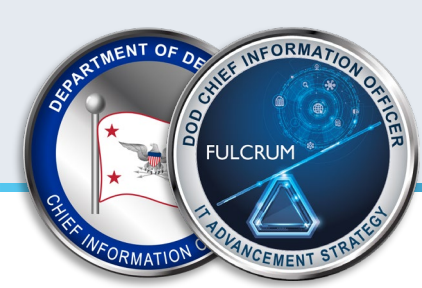




# CMMC Alignment to NIST SP 800-171 Revisions

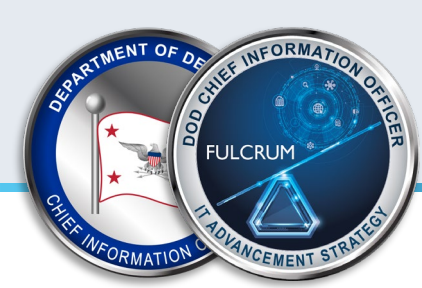
- DoD followed federal rulemaking guidelines when aligning CMMC assessment requirements to NIST SP 800-171 **Rev 2**.
- Defense contractors can implement NIST SP 800-171 Rev 3, but must comply with **Rev 2 requirements not covered in Rev 3** to meet CMMC assessment requirements.
- DoD will incorporate Rev 3 with future rulemaking.





# Conditional and Final Status

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



# CMMC Post-Assessment Remediation

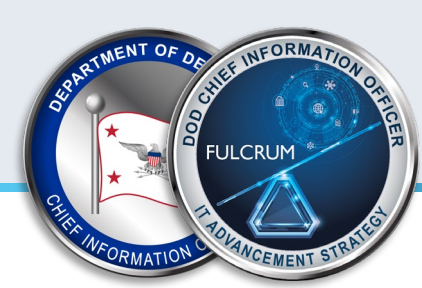
## ❑ CMMC Program will allow limited use of POA&Ms

- 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

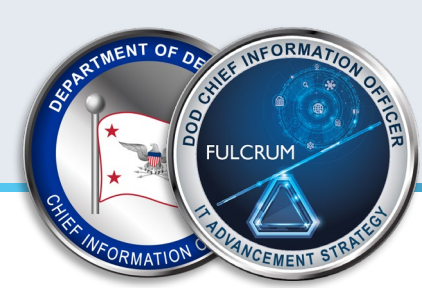
- POA&M closeout Self-Assessment is conducted by the OSA.
- POA&M closeout Certification Assessment is conducted by a C3PAO or the DIBCAC.
- POA&Ms must be closed out within 180 days of when the CMMC Assessment results are finalized and submitted to SPRS or CMMC eMASS, as appropriate.

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



# CMMC Scoring Methodology (§ 170.24)

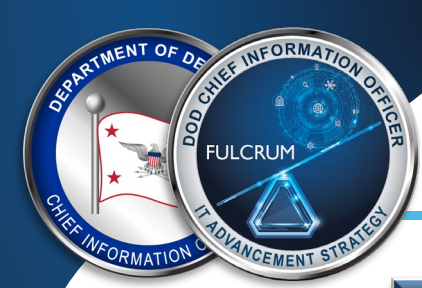
- Level 1: Score not required; either **MET** or **NOT MET**
- Level 2: Security requirements are valued 1, 3, or 5 points with a range of -203 to 110, with a minimum passing score of 88. Partial credit is allowed for 2 requirements:
  - MFA: 5 points deducted from overall score of 110 if MFA is not 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.



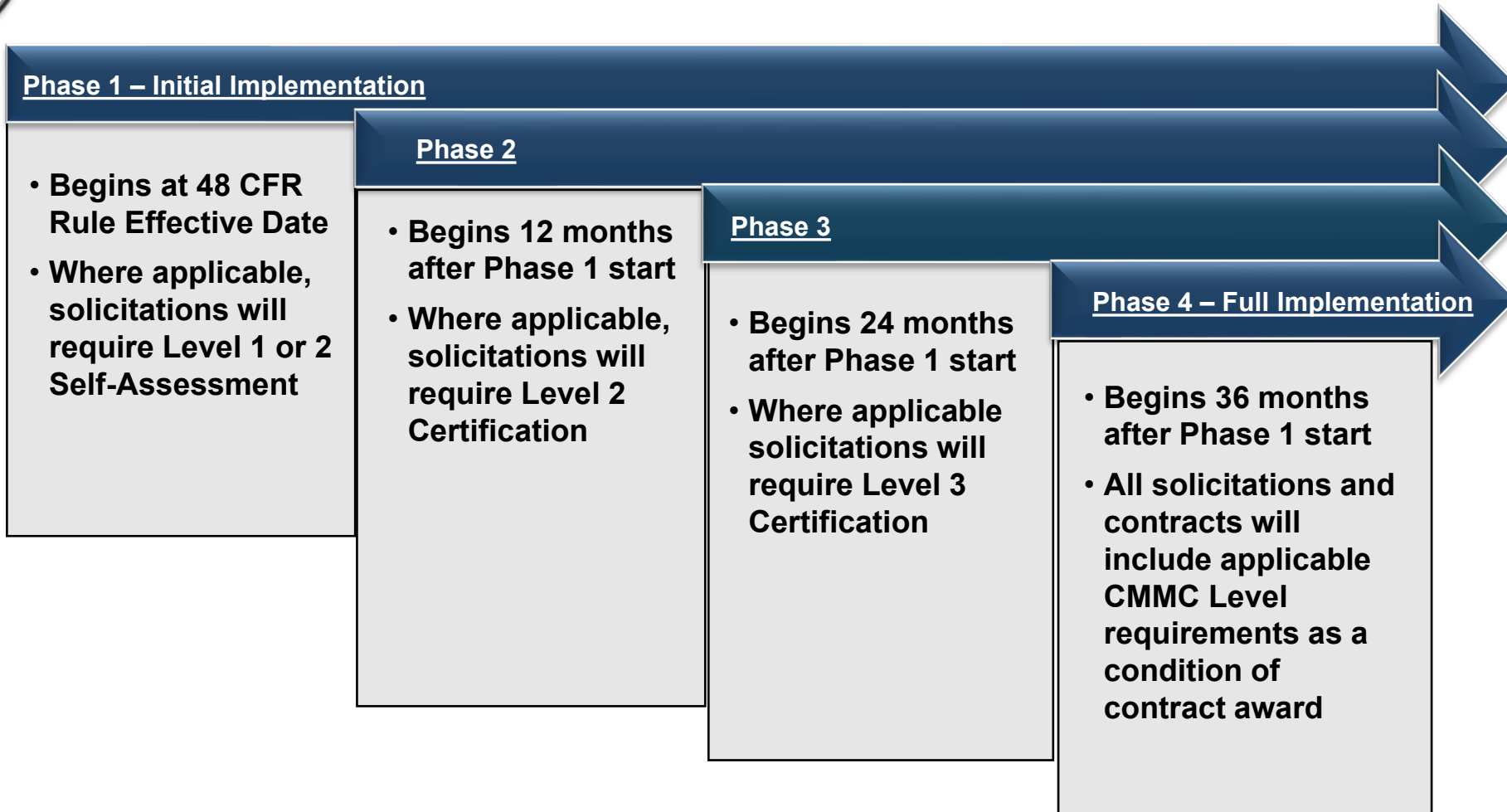
# Standards Acceptance

Contractors and subcontractors that completed a DCMA DIBCAC High Assessment aligned with CMMC Level 2 Scoping are eligible for CMMC Level 2 Final Certification Assessment under the following conditions:

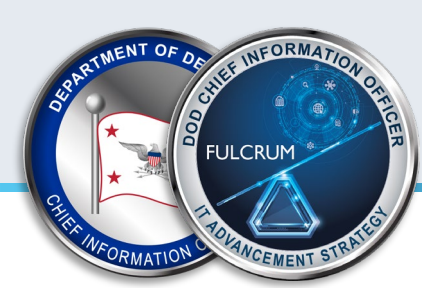
- **Achieved a perfect score with no open POA&M from a DCMA DIBCAC High Assessment conducted prior to the effective date of the CMMC rule**
  - CMMC Level 2 will be valid for 3 years from the date of the original High Assessment.
  - Eligible High Assessments include those conducted under DCMA's Joint Surveillance authority.
- **Scope of the CMMC Level 2 Final Certification Assessment is identical to the scope of the High Assessment**



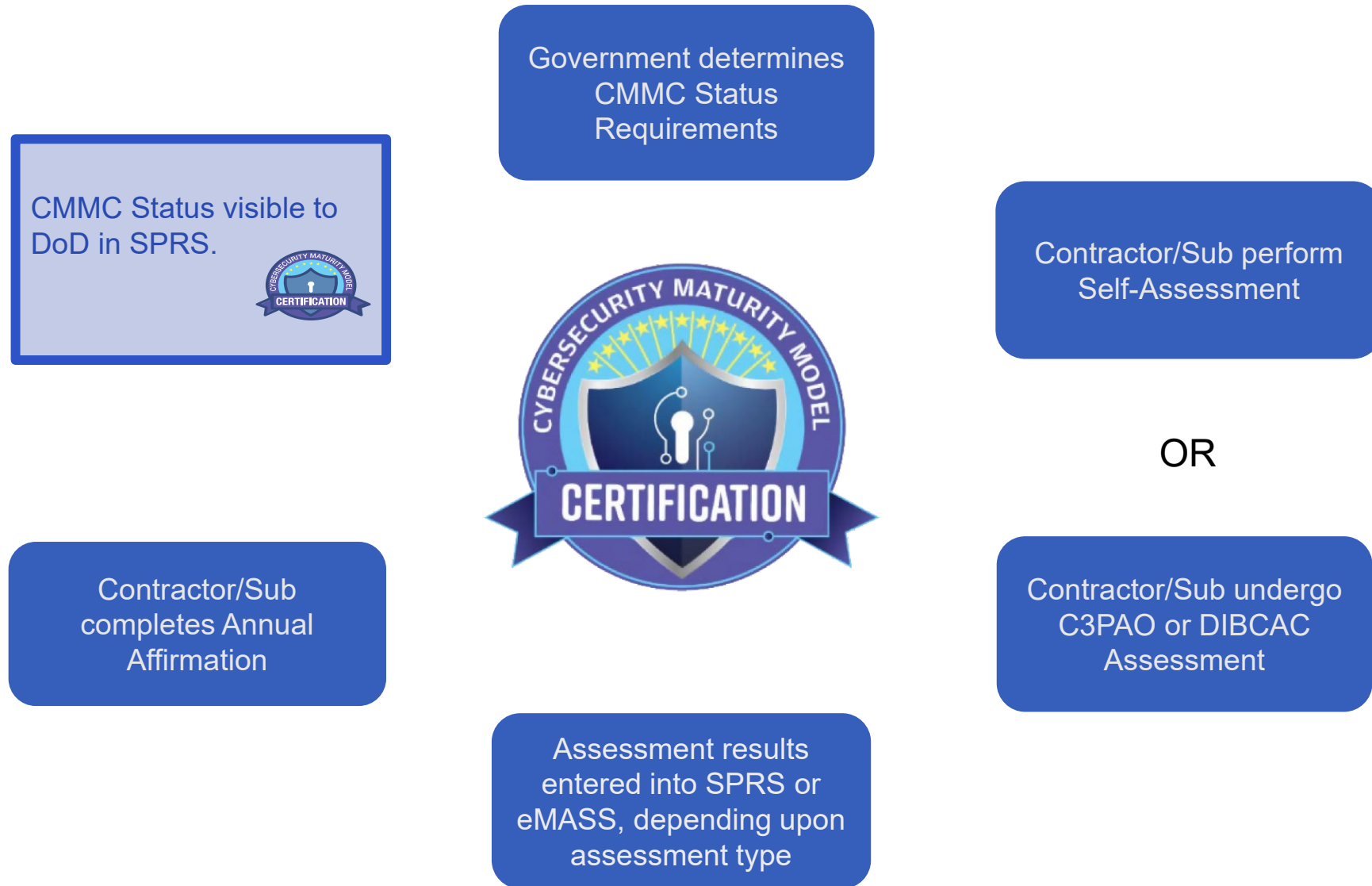
# Phased Implementation of CMMC Requirements



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



# CMMC Process - OSA Perspective



Government determines CMMC Status Requirements

CMMC Status visible to DoD in SPRS.



Contractor/Sub perform Self-Assessment

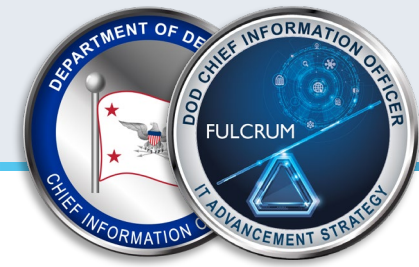
OR

Contractor/Sub undergo C3PAO or DIBCAC Assessment



Contractor/Sub completes Annual Affirmation

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



# 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

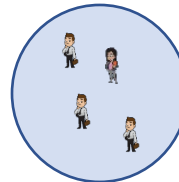
- ISO / IEC 17020
- Conducts CMMC Level 2 Certification Assessments on DIB contractors
- Employs Assessors
- Submits Assessment Report in eMASS
- Issues CMMC certificate to DIB contractor



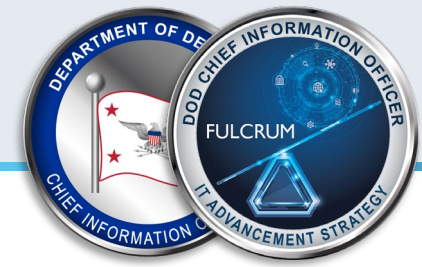
Agreements

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

- Certified by CAICO IAW ISO/IEC 17020





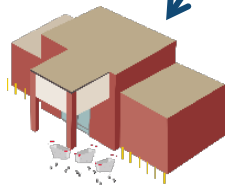


# CAICO



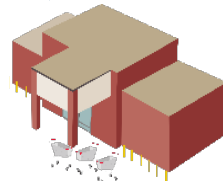
## CMMC Assessor and Instructor Certification Organization - §170.10

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



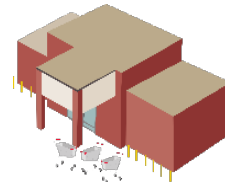
### Approved Training Providers

- Trains Certified Professionals
- Trains Assessors
- Trains Instructors



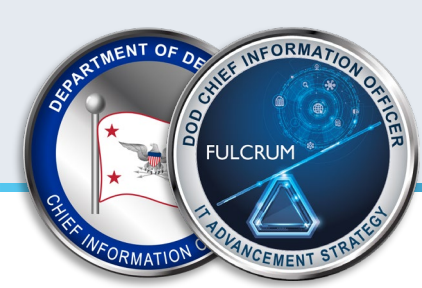
### Approved Publisher Partners

- Develops Training Materials



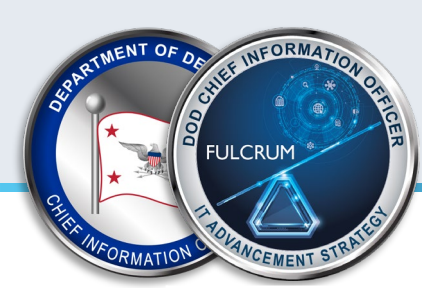
### Approved CMMC Exam Org

- Develops and administers Assessor and Instructor Certification Exams



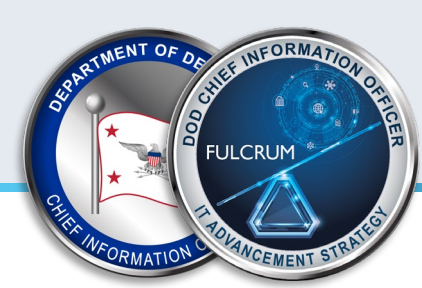
# Additional Resources

- Please refer to the **official DoD CMMC Program website**, including the FAQ page, for more information about CMMC: <https://dodcio.defense.gov/CMMC/>
- **DoD no-cost cybersecurity compliance resources** can be found at [dibnet.dod.mil](http://dibnet.dod.mil) under *DoD 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](http://cyberab.org).
- To **obtain additional information on CMMC Assessments, Scoping, and Hashing**, visit: <https://dodcio.defense.gov/cmmc/Resources-Documentation/>
- The Department's **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>



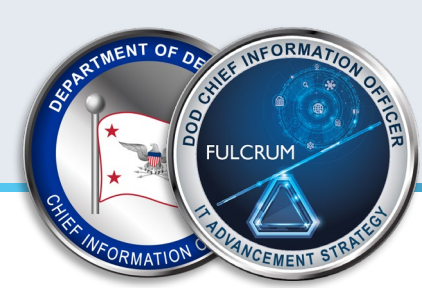
# Acronym Glossary

Acronym	Meaning
<b>AB</b>	Accreditation Body
<b>CAICO</b>	Cybersecurity Assessor and Instructor Certification Organization
<b>CIO</b>	Chief Information Officer (DoD)
<b>CFR</b>	Code of Federal Regulations
<b>CMMC</b>	Cybersecurity Maturity Model Certification
<b>CCPs/CCAs/CCIs</b>	CMMC Certified Professionals/Assessors/Instructors
<b>C3PAO</b>	Certified Third-Party Assessment Organization
<b>CUI</b>	Controlled Unclassified Information
<b>DCMA</b>	Defense Contract Management Agency
<b>DFARS</b>	Defense Federal Acquisition Regulation Supplement
<b>DIB</b>	Defense Industrial Base
<b>DIBCAC</b>	Defense Industrial Base Cybersecurity Assessment Center
<b>DoD</b>	Department of Defense
<b>eMASS</b>	Enterprise Mission Assurance Support Service



# Acronym Glossary Cont'd

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