

Cybersecurity Maturity Model Certification (CMMC) 2.0



USG shutdown precluded this earlier-submitted presentation from occurring

Learning Objectives

- Definition of CMMC
- Importance of implementing CMMC
- Key organizations in the CMMC process

Agenda

- Program Overview and History
- CMMC Safeguarding requirements for CUI and FCI on Non-Federal Information Systems
- Cybersecurity requirements and the CMMC clause
- Revised CMMC Framework requirements
- CMMC Alignment to NIST SP 800-171 Revisions
- Difference between Conditional, Final CMMC status and Post Assessment
- CMMC Scoring Methodology and Standards of Acceptance
- CMMC Phase Implementation requirements
- CMMC Process of Obtaining Certification
- CMMC Ecosystem
- NAVFAC Southeast Command Information Office (CIO) preparations for CMMC
- Q&A / Discussion

What is Cybersecurity Maturity Model Certification?



Cyber Maturity Model Certification (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 Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) on its unclassified contractor information systems.

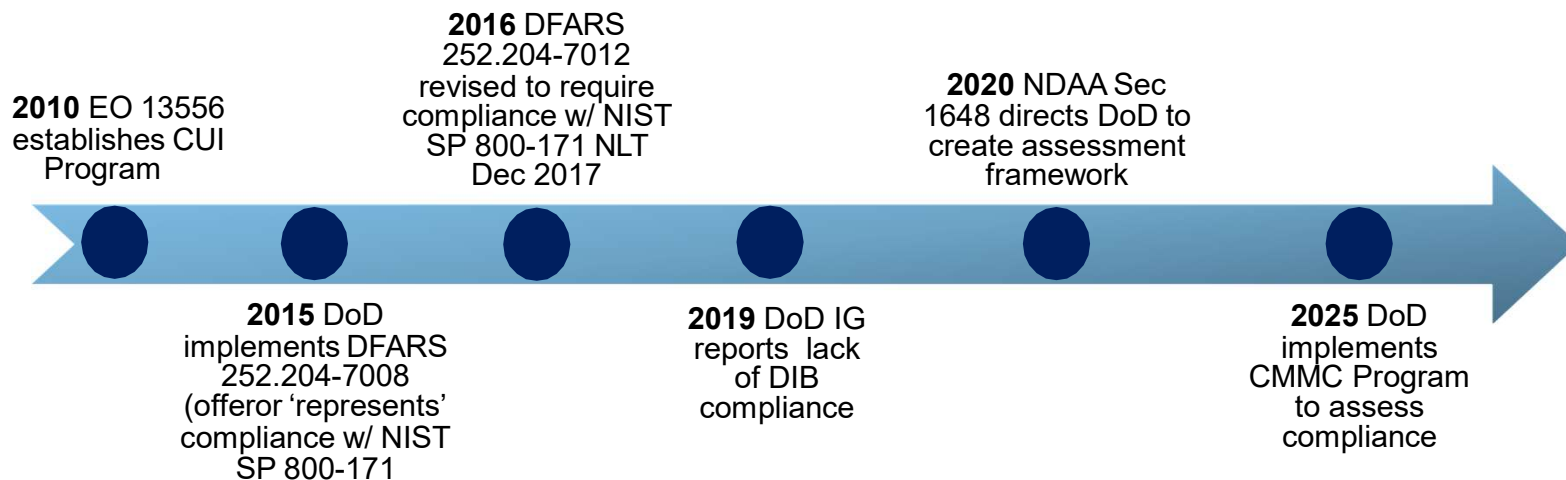
- New DoD solicitations
- New DoD procurement instruments including contracts, task orders, delivery orders
- As a condition to exercise an option period
- Subcontractors are subject to flow-down requirements (*Prime contractors pushes down CMMC requirements to subcontractors based on type of information*)



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 DoD contractors and subcontractors comply with DoD requirements to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).



**CLEARED
For Open Publication**
Oct 15, 2024

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Safeguarding FCI and CUI

Safeguarding Requirements for Non-federal Information Systems

FCI

- Information that is not marked as public or for public release and is not designated as CUI
- Defined in Federal Acquisition Regulation (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 Code of Federal Regulations (CFR) Part 2002
- Minimum safeguarding requirement: NIST SP 800-171

Existing DoD Cybersecurity Requirements

Defense Federal Acquisition Regulation (DFARS)

- **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 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
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

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 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

**CMMC Assessment &
Certification Process**

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&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:
- 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 Supplier Performance Risk System (SPRS) and reviewed by contracting officers and requiring activities**

Standards Acceptance

Contractors and subcontractors that completed a Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (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.
- **Scope of the CMMC Level 2 Final Certification Assessment is identical to the scope of the High Assessment**



Phased Implementation of CMMC Requirements

Phase 1 – Initial Implementation

- Begins at 48 CFR Rule Effective Date (*October 2025)
- Where applicable, solicitations will require Level 1 or 2 Self-Assessment

Phase 2

- Begins 12 months after Phase 1 start
- Where applicable, solicitations will require Level 2 Certification

Phase 3

- Begins 24 months after Phase 1 start
- Where applicable solicitations will require Level 3 Certification

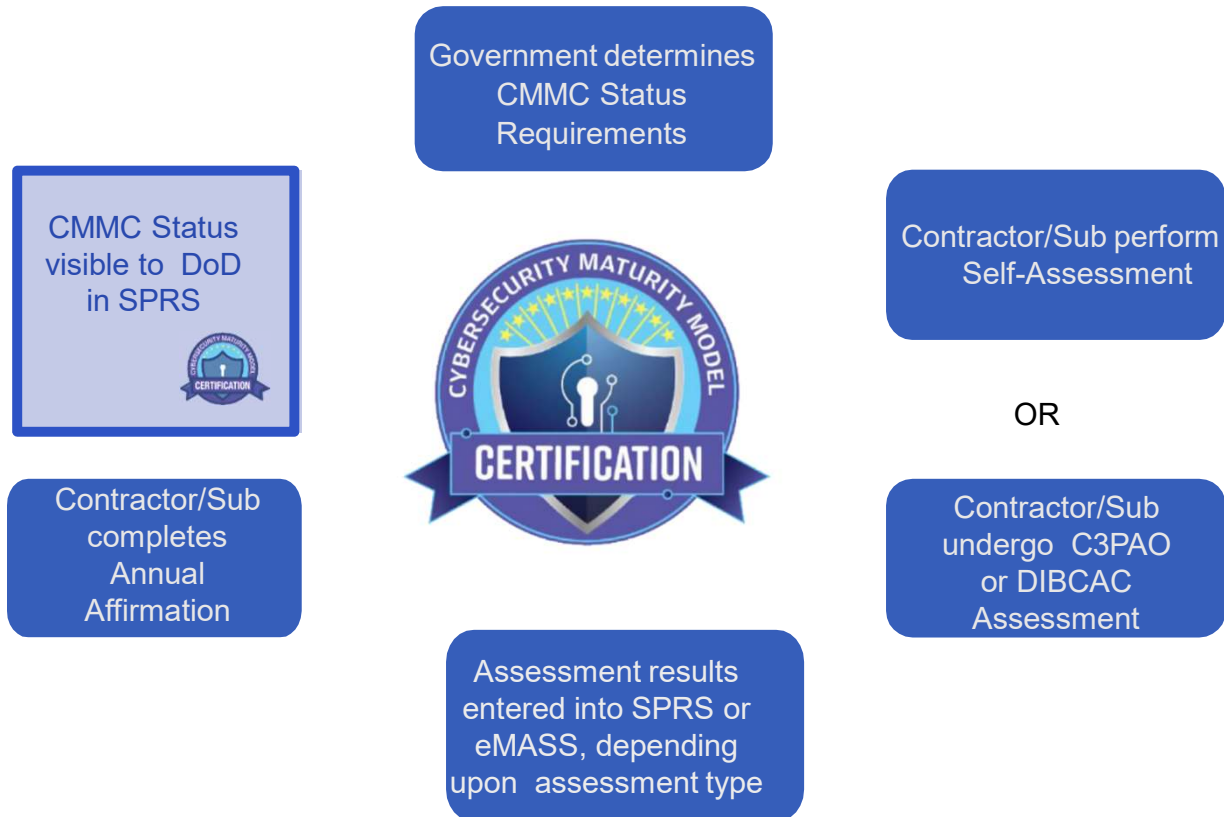
Phase 4 – Full Implementation

- Begins 36 months after Phase 1 start
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

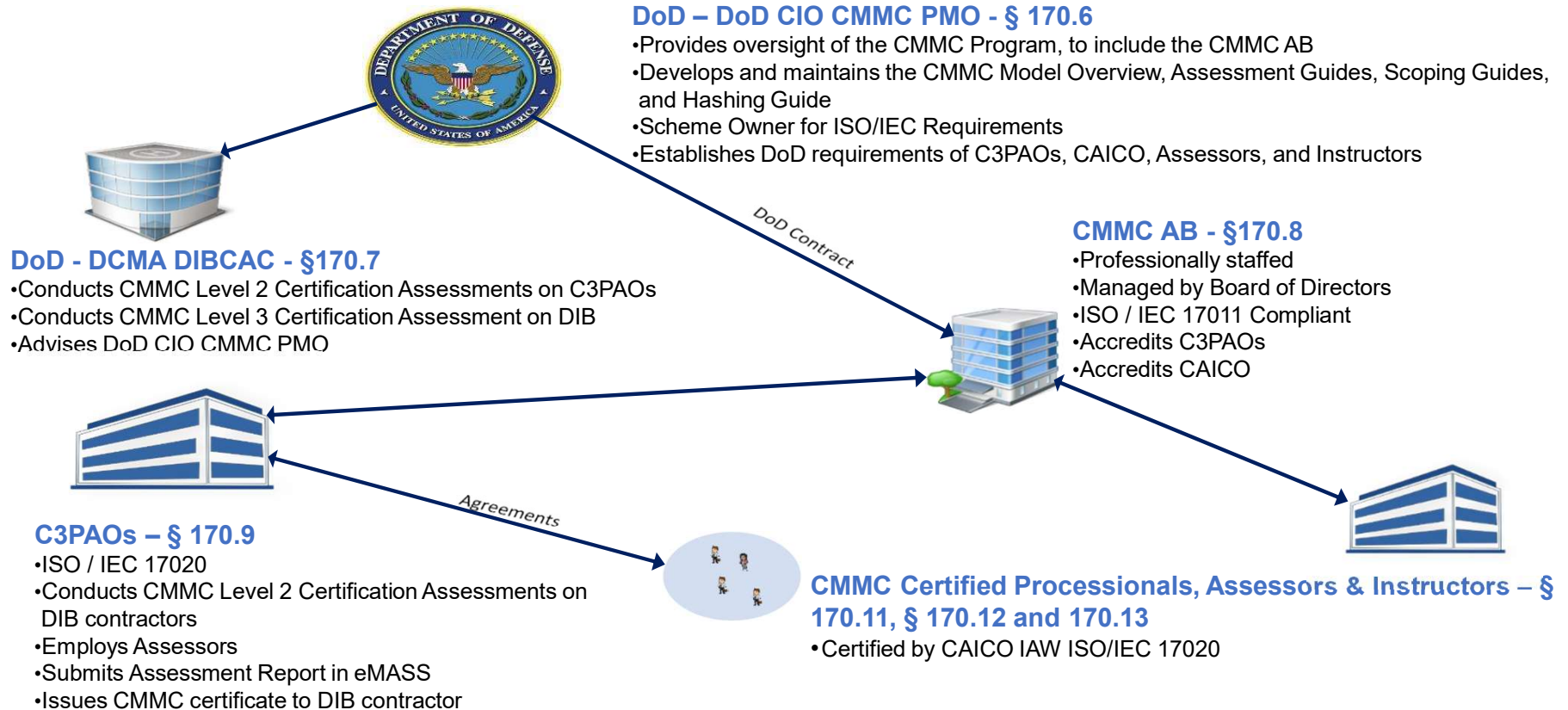
The 48 Code of Federal Regulations (CFR) focuses on the acquisition aspect of CMMC which will incorporate CMMC requirements in solicitations and contracts.

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

CMMC Process - OSA Perspective



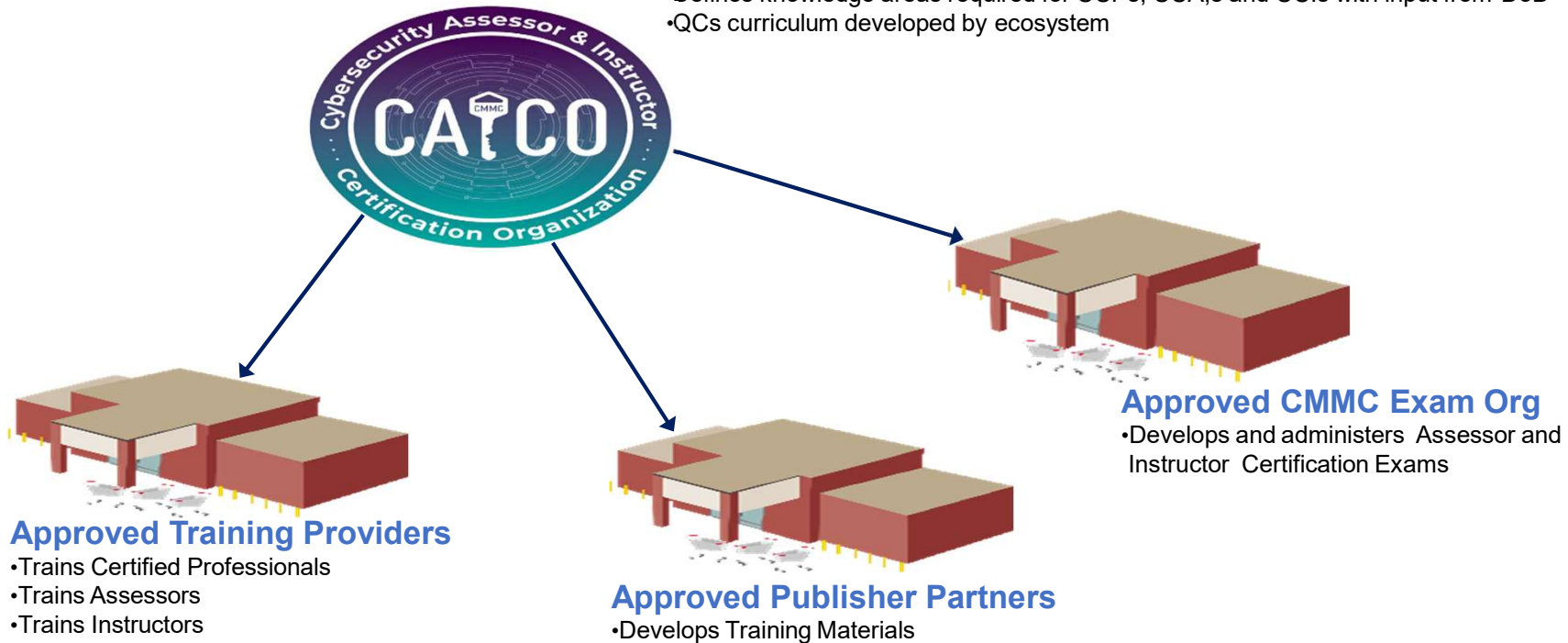
CMMC Ecosystem



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



NAVFAC Southeast Preparation For CMMC

- Communicating and Collaborating with Industry Partners on CMMC compliance
- Collaborating with contracting officials and designated government Cyber Assessment Team to participate in assessing privatized Operational Technology (OT) systems and (2) identifying potential changes needed to safeguard FCI and CUI



Frequently Asked Questions

- If the government has a contract with a private industry to run a operational technology (OT) system does the CMMC rules apply? **If the OSC runs the OT and the OT is managed and ran by a member of the DIB than the OT is in scope. Additionally, the contract established between the government and the OSC is a contract, which means the OSC must be CMMC Level 2 certified, and the OT is in scope**
- In regard to the CMMC process from the OSA perspective, the government determines CMMC status requirements; are these requirements determined by the location or the mission? For example, would the CMMC status requirements for a government contract at Fort Liberty be based on its location or mission? **The location is not relevant. The requirements are based on the type of data the contract includes. Requirements for a specific type of assessment are listed in the contract-specific clause 252.202-7021**
- Does CMMC affect current DoD Contracts? **CMMC will affect new DoD contracts, starting from 2025. However, the transition may vary depending on the type of contract. Existing contracts will not require CMMC certification unless they are modified or renewed after the CMMC rules are fully implemented**



Frequently Asked Questions

- In regard to CMMC scoring methodology, the results for all levels are posted in SPRS and reviewed by contracting officers and requiring activities; who are the requiring activities? **The required activity is the program office for the department (i.e. Army, Air Force, Navy, Marines)**
- What's the difference between DCMA DIBCAC and C3PAO? **A C3PAO performs CMMC assessments on companies to determine their cybersecurity maturity level, while DCMA DIBCAC is the organization that manages and oversees the CMMC assessment process, including accrediting C3PAOs. The C3PAOs act as independent auditors, evaluating companies against CMMC standards to determine their compliance level, whereas DCMA DIBCAC sets the CMMC standards and ensures the quality of C3PAO assessments**



SUMMARY

- **Failing to meet CMMC requirements**, whether through negligence or mishandling of sensitive information like Federal Contract Information (FCI) or Controlled Unclassified Information (CUI), can lead to severe consequences for contractors and subcontractors in the Defense Industrial Base (DIB)
- **Prime Contractor Liabilities**: Prime contractors are accountable for their subcontractors' CMMC compliance. If a subcontractor is non-compliant, the prime contractor faces risks like contract termination, negative impact on Supplier Performance Risk System (SPRS) scores, and diminished competitiveness
- **Suspension or Debarment**: The government may suspend or debar a company from participating in federal contracts if they fail to meet cybersecurity requirements
- **Loss of Contracts**: Non-compliance can result in the loss of existing DoD contracts and being deemed ineligible to bid on future ones
- **Legal Action**: The DoD may pursue legal action for breach of contract, resulting in costly legal battles and potential settlements
- **Increased Scrutiny**: Expect increased audits and scrutiny from regulatory bodies and contracting officers



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 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/#/>
- **Locate a C3PAO**, visit the CMMC Accreditation Body Marketplace at 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>



CMMC 2.0 Details and
Links to Key Resources

CIO Cybersecurity POCs



CYBERSECURITY PROGRAM OVERSIGHT

CIO2 CYBERSECURITY MANAGEMENT



CIO2: William Smiley
Cybersecurity Division Director
904-542-9056 | william.l.smiley4.civ@us.navy.mil



CIO: Andrea Freeman
Command Information Officer
904-542-4191 | andrea.l.freeman.civ@us.navy.mil

CIO4 CYBERSECURITY INFRASTRUCTURE AND ENGINEERING



CIO4: Antonio Jefferson
Operation Technology Division Director
904-542-5839 | antonio.s.jefferson2.civ@us.navy.mil



CIO2.1: Keith Long & Lydell Sapp
Construction and Design Contracts Review /
Cybersecurity Commissioning (CyCx)
904-542-8434 | keith.d.long2.civ@us.navy.mil
904-542-8484 | lydell.d.sapp.civ@us.navy.mil



CIOD: Joseph Ellis
Defensive Cybersecurity Operations
Analyze Cyber Threats and Vulnerabilities
(904) 542-3648 | joseph.p.ellis.civ@us.navy.mil



CIO41: Bobby Kelley
Control Systems Platform Enclave Brch Manager
ACAS, HBSS and VMWARE Support
904-542-2490 | bobby.j.kelley.civ@us.navy.mil



CIO42: Kevin Gaddist
Facilities Related Control Systems Brch Manager
AMI, SCADA, DDC, and HVAC Support
904-542-8495 | kevin.k.gaddist.civ@us.navy.mil



CIO43: Paddy Jackson
Information Systems Security Engineer Lead
DRAGOS / Cybersecurity Threat Analysis
904-542-5488 | paddy.o.jackson.civ@us.navy.mil

Q&A / Discussion



Acronym Definitions

- **CMMC** - Cybersecurity Maturity Model Certification
- **FCI** - Federal Contract Information
- **CUI** - Controlled Unclassified Information
- **DFARS** - Defense Federal Acquisition Regulation
- **SPRS** - Supplier Performance Risk System
- **FIPS** - Federal Information Processing Standards
- **DCMA** - Defense Contract Management Agency
- **DIBAC** - Defense Industrial Base Cybersecurity Assessment Center
- **OSA** - Organization Seeking Assessment
- **OSC** - An Organization Seeking Certification
- **MFA** - Multi-Factor Authentication
- **OT** - Operational Technology (OT)
- **NIST SP 800-171** - National Institute of Standards & Technology Special Publication
- **CAICO** – Cybersecurity Assessor & Instructor Certification Organization