



# CMMC from an Assessor Organization's Viewpoint

July 2024



# CMMC

## What CMMC is NOT:

**A requirement that you DO anything other than to assess yourself, or get a third party assessment every three years (with your own internal annual review) as appropriate in your contract.**





# CMMC Timeline

## 2017 NIST 800-171 CUI



Defense contractors are required to meet NIST 800-171 when handling controlled unclassified information (CUI)



## 2020 CMMC 1.0 Released

Cybersecurity Maturity Model Certification (CMMC) framework: Standardized cybersecurity approach over entire Defense Industrial Base, including suppliers. *Interim Rule effective 11/30/20*

## 2021 CMMC 2.0



Streamlined model announced after public comments. *November 2021*

## 2023 NIST SP 800-171 r.3



Revised draft guidelines announced for CUI. *Final to be published early 2024*

## 2023 CMMC Review Complete

CMMC regulatory process is completed: DoD submitted CMMC rule to the OIRA in July. November 2023 OIRA completed their review.

## OIRA

## 2023/4 CMMC Rule Published

Late December/Early January publication. Likely will be published as a Proposed Rule, followed by a comment period.



# CMMC

## Requirements of DFARS 7024 (as of June 9, 2023!):

- RFP must include plans for the continuation of essential contractor services during periods of crisis, which must address:
  - Contracting Officer **SHALL** consider **SPRS Score**
  - Provision of essential personnel and resources for operation continuity for <30 days during a crisis
  - Noted challenges in maintaining essential contractor services
  - Time lapse between acquisition of essential personnel and on-site availability during crisis
  - Alternate facility relocation or WFH components, processes, requirements, and identification & training of designated personnel
  - Alert and notification procedures for mobilizing designated personnel
  - Methods of responsibility expectation communications with employees during the crisis

# PATH TO COMPLIANCE

## Overlooked aspects of CMMC 2.0

- **Self-attestation- *with teeth***- Enforcement of False Claims Act. Sr. Company officials now personally held accountable to self-attestation
- **Timeline Window:** shrinking for OSCs- 1-15 months to comply vs 5-year roll out
- **Providers (ESP'S) likely included in SSP-** MSPs, SIEM/SOC, Cloud hosting services
- **Collecting artifacts:** Hashed- new process of collecting and storing objective evidence
- **POA&MS:** New-found accountability- timebound and enforceable



# CMMC

## What is FCI? Federal Contract Information

- Covered in FAR 52.204-21
- Info contained in contracts
- Not for public release
- Not classified
- Requires safeguarding
- Correlates to Level 1 CMMC
- Contract performance reports
- Organizational/programmatic charts (any charts or diagrams issued by the DoD)
- Proposal responses
- Past performance information
- Contract information
- Procedures
- “information, not intended for public release, that is provided or generated for the Government under a contract to deliver a product or service to the Government.”

# CMMC

## What is CUI? Controlled Unclassified Information

- DFARS 252.204-7012
- Correlates to Level 2+ for CMMC
- Privacy information (including health)
- Tax information
- Law enforcement
- Critical infrastructure information
- Controlled technical information
- Financial information
- Intelligence information
- Privilege information
- Anything you create on behalf of the DoD
- Unclassified nuclear information
- Procurement and acquisition
- System or Network vulnerabilities
- Export Controlled Information
- ITAR information
- Standards
- Research and or Engineering Data
- And more.....<https://www.archives.gov/cui>



# CMMC

## LEVEL 2

### Advanced Cyber Hygiene

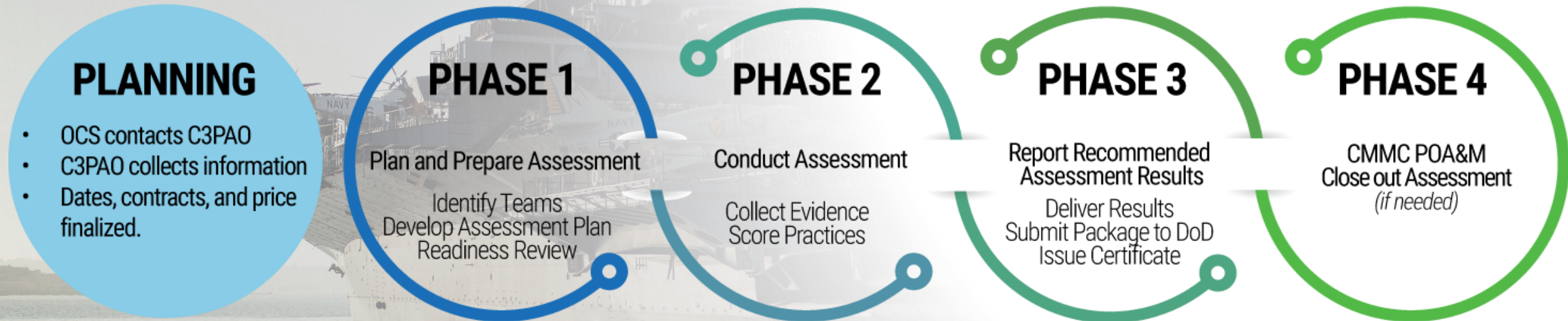
- Level 2 assessment requires that policies and procedures are not only documented, but also managed and supported by appropriate projects and resource plans.
- There are 110 practices (320 v2, 445 v3 “things to do or have”) from NIST SP 800-171 Revision 2 standards that promotes good cyber hygiene.
- Certification from C3PAO required, self-attested annual review, certification must renew every 36 months.
- DFARS 252.204-7012 Don't forget c-g

[https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.](https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting)



# PATH TO COMPLIANCE

## CMMC Assessment Process





# PATH TO COMPLIANCE

## CMMC Assessment Process

### Assessment Plan :

- Objective Evidence – SSP!
  - Asset inventory
  - Environment/system description and boundary
  - Description of how each of the 110 practices implemented
  - Network diagram
  - CUI diagram
  - Artifact Change control history



# PATH TO COMPLIANCE

## Best Practices to Readiness

### LEAD FIRST

- KNOW thyself: environments, contracts, staff
- Budget

### SCOPE WELL

- What is in scope? Determines everything.
  - Consider an enclave approach
    - Microsoft
    - Google
    - On-Prem
- Good News/Bad News: Inheritance, tools and consultants

# PATH TO COMPLIANCE

## CMMC and ISO 27001 Cross mapping

60%+ in common

Are you closer than you think??



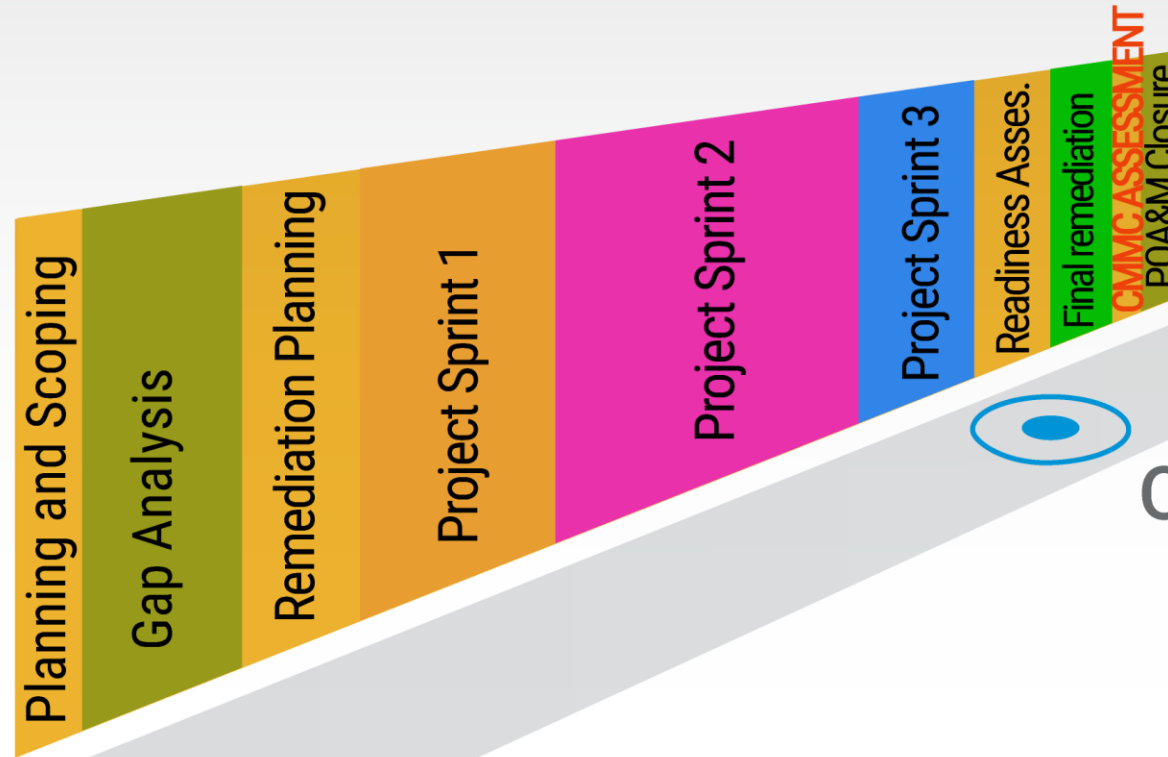
Kill Chain Category	CMMC 2.0 Practice #	NIST SP 800-171 R2 Control	NIST SP 800-171 Control #	NIST CSF	ISO 27001:2013	ISO 27002:2022
Documentation	CA.L2-3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational	3.12.2			
	CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements	3.12.4	PR.IP-7		
Secure Architecture	SC.L1-3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal	3.13.1	PR.PT-4	13.1.1 13.1.2	8.20 8.21
	SC.L1-3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	3.13.5	PR.AC-5	13.1.3	8.20 8.22
	SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within	3.13.2		14.1.2 14.2.5	8.12 8.26
	SC.L2-3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by	3.13.6		13.2.1	5.14 8.20
Procedures / Rules of Behavior	MP.L2-3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3.8.1	PR.PT-2	8.2 8.2.3 8.3	5.9 5.10 5.12
	MP.L2-3.8.2	Limit access to CUI on system media to authorized users.	3.8.2	PR.PT-2		7.10
Change Management	CM.L2-3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	3.4.3	PR.IP-1 PR.IP-3	12.1.2 14.2.2	8.19 8.32
	CM.L2-3.4.4	Analyze the security impact of changes prior to implementation.	3.4.4	PR.IP-3		
	CM.L2-3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	3.4.5	PR.IP-1		
Incident Response Operations	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	3.6.1	RS.RP-1	16.1.3 16.1.4 16.1.5	5.24 5.25 5.26 6.8
	IR.L2-3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	3.6.2	RS.CO-2 RS.CO-3	16.1.3 16.1.4	5.24 5.25
	IR.L2-3.6.3	Test the organizational incident response capability.	3.6.3	DE.DP-3		
Situational Awareness	AU.L2-3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and	3.3.1	DE.CM-1 DE.CM-3		
	AU.L2-3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their	3.3.2	DE.CM-1 DE.CM-3	12.4.1	8.15
	AU.L2-3.3.3	Review and update logged events.	3.3.3			8.16
	AU.L2-3.3.4	Alert in the event of an audit logging process failure.	3.3.4			
	AU.L2-3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful.	3.3.5	DE.AE-3		8.15





# CMMC Phased Timeline

**CMMC Compliance implementation effort over 12 months**



October 2024?





April 2025?

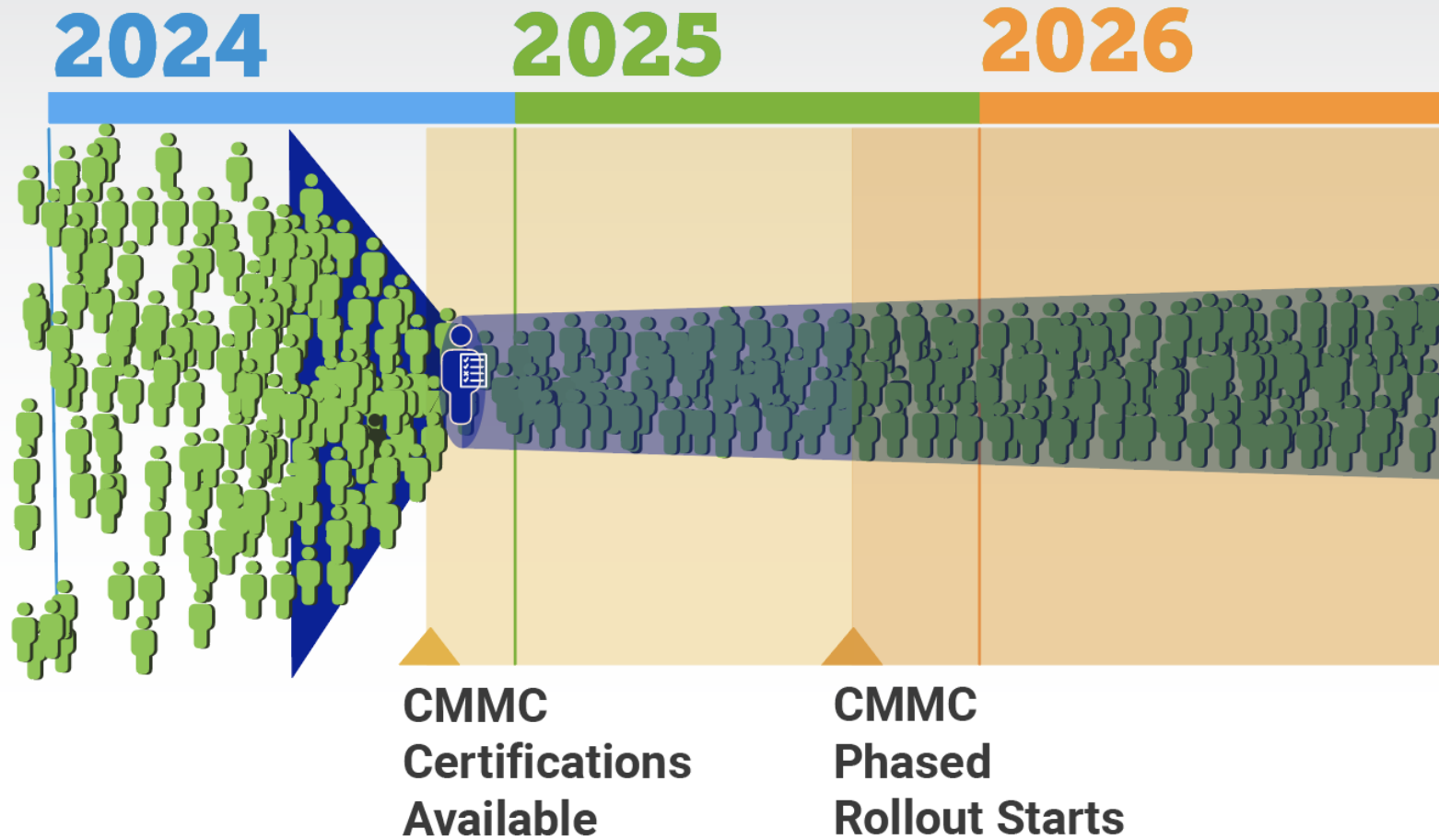




# CMMC C3PAO Certifications & Availability

 Organizations Seeking Assessments (70,000+)

 CMMC Assessment Organizations (<60)





# Links

- DOD FedRAMP memo:
  - <https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf>
  -
- **32 CFR (CMMC Program)**
  - Downloadable PDF of Federal Register text (this version has page numbers): <https://public-inspection.federalregister.gov/2023-27280.pdf>
  - Federal Register home page for CMMC and comments: <https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program>
  - Docket Information (the rule agenda): <https://www.regulations.gov/docket/DOD-2023-OS-0063>
  - Public comments posted regarding rule: <https://www.regulations.gov/document/DOD-2023-OS-0063-0001>
  - Regulatory Impact Analysis 32 CFR Part 170 (analysis of changes and cost): <https://www.regulations.gov/document/DOD-2023-OS-0063-0003>
  - Initial Regulatory Flexibility Analysis 32 CFR (benefits and costs, impact to small business): <https://www.regulations.gov/document/DOD-2023-OS-0063-0002>
- **CMMC Guides (assessment guides, scoping, etc)**
  - CMMC Guidance documents home and comments page: <https://www.regulations.gov/docket/DOD-2023-OS-0096/document>
  - Notice of Guidance for CMMC: <https://www.regulations.gov/document/DOD-2023-OS-0096-0001>
  - CMMC Model Overview: <https://www.regulations.gov/document/DOD-2023-OS-0096-0006>
  - Scoping Guide – CMMC Level 1: <https://www.regulations.gov/document/DOD-2023-OS-0096-0007>
  - Scoping Guide – CMMC Level 2: <https://www.regulations.gov/document/DOD-2023-OS-0096-0003>
  - Scoping Guide – CMMC Level 3: <https://www.regulations.gov/document/DOD-2023-OS-0096-0008>
  - Assessment Guide – CMMC Level 1: <https://www.regulations.gov/document/DOD-2023-OS-0096-0002>
  - Assessment Guide – CMMC Level 2: <https://www.regulations.gov/document/DOD-2023-OS-0096-0005>
  - Assessment Guide – CMMC Level 3: <https://www.regulations.gov/document/DOD-2023-OS-0096-0004>
  - Hashing Guide (used during assessments only): <https://www.regulations.gov/document/DOD-2023-OS-0096-0009>
- **Assessment Reporting Templates**
  - Assessment reporting home and comments page: <https://www.regulations.gov/document/DOD-2023-OS-0097-0001>
  - Paperwork Reduction Act review: <https://downloads.regulations.gov/DOD-2023-OS-0097-0001/content.docx>
  - CMMC Level 2 Pre-Assessment Reporting: [https://downloads.regulations.gov/DOD-2023-OS-0097-0001/attachment\\_2.xlsx](https://downloads.regulations.gov/DOD-2023-OS-0097-0001/attachment_2.xlsx)
  - CMMC Level 2 Assessment Results Reporting: [https://downloads.regulations.gov/DOD-2023-OS-0097-0001/attachment\\_4.xlsx](https://downloads.regulations.gov/DOD-2023-OS-0097-0001/attachment_4.xlsx)
  -