Naval Facilities Engineering Systems Command

NAVFAC SOUTHEAST

Cybersecurity Maturity Model Certification (CMMC) V2 NIST 800-171 Controls

Presented by: Keith Long

Panel: Antonio Jefferson, Joe Ellis, Charlie Weaver & Kevin Gaddist

11 Jan 2024

CIO Cybersecurity POCs

CYBERSECURITY PROGRAM OVERSIGHT

CIO2 CYBERSECURITY

CIO2: Joseph Ellis
joseph.p.ellis.civ@us.navy.mil
Cybersecurity Division Director

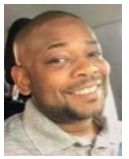
CIO: Andrea Freeman
Command Information Officer
andrea.l.freeman.civ@us.navy.mil

CIO4 OPERATIONAL TECHNOLOGY

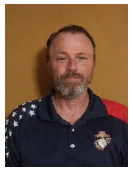
CIO4: Charlie Weaver
charles.r.weaver12.civ@us.navy.mil
Operation Technology Division Director

CIO21: Maria Lopez
maria.t.lopez.civ@us.navy.mil
RMF Team Lead
Risk Management Framework (RMF)
Requests for Authority-to-Operate (ATO)

CIOPM: Antonio Jefferson
antonio.s.jefferson2.civ@us.navy.mil
Cybersecurity Contracts Program Manager
Red Zone Commissioning and BOD Support
Construction and Design Contracts Review

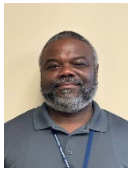


CIO41: Kevin Gaddist
kevin.k.gaddist.civ@us.navy.mil
OT Enterprise Support Branch Manager
Control System Platform Enclave (CSPE)
Continuous Monitoring Support



CIO42: Bobby Kelley
bobby.j.kelley.civ@us.navy.mil
Control Systems Support Branch Manager
AMI, SCADA, DDC, and HVAC Support
Cyber Hygiene & Continuous Monitoring Support

CIO43: Paddy Jackson
paddy.o.jacksonv.civ@us.navy.mil
Information Systems Security Engineer Team Lead
Cybersecurity Commissioning Support
Risk Management Framework (RMF) Support



CIO44: Keith Long
keith.d.long2.civ@us.navy.mil
CyCx Team Lead
Cybersecurity Commissioning Support
Construction and Design Contracts Review

Overview of the CMMC Program

Cybersecurity Maturity Model Certification (CMMC) program is aligned to DoD's information security requirements for Defense Industrial Base (DIB) partners. It is designed to enforce protection of sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program provides the Department increased assurance that contractors and subcontractors are meeting the cybersecurity requirements that apply to acquisition programs and systems that process controlled unclassified information.

CMMC Key Features

The CMMC 2.0 program has three key features:

1. Tiered Model: CMMC requires that companies entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for requiring protection of information that is flowed down to subcontractors.

2. Assessment Requirement: CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.

3. Implementation through Contracts: Once CMMC is fully implemented, DoD contractors that handle sensitive controlled unclassified information will be required to achieve a particular CMMC level as a condition of contract award.

CMMC 2.0 Model

CMMC 2.0 model is streamlined to three cybersecurity levels versus five levels and aligns the requirements at each level with well-known and widely accepted NIST cybersecurity standards.

- Eliminates CMMC 1.0 Levels 2 and 4 which were developed as transition levels and never intended to be assessed requirements
- Establishes three progressively sophisticated levels, depending on the type of information:
  - Level 1 (Foundational) –for companies with Federal Contract Information (FCI) only; information requires protection but is not critical to national security
  - Level 2 (Advanced) –for companies with Controlled Unclassified Information (CUI)
  - Level 3 (Expert) –for the highest priority programs with CUI; Requirements will mirror NIST SP 800-171 and NIST SP 800-172
- Eliminates all CMMC unique practices and maturity processes: Work with NIST to address identified gaps in the NIST SP 800-171
- Level 2 aligns with NIST SP 800-171
- Level 3 will use a subset of NIST SP 800-172 requirements

Simplifies the CMMC standard for companies, while safeguarding critical Department information

CMMC 2.0 Assessments

CMMC Level 1 (Foundational) will require DIB company self-assessments

CMMC Level 2 (Advanced) may require third-party or self-assessments, depending on the type of information

- Requires third-party assessments for prioritized acquisitions: Companies will be responsible for obtaining an assessment and certification prior to contract award
- Requires self-assessments for other non-prioritized acquisitions: Companies will complete and report a CMMC Level 2 self-assessment and submit senior official affirmations to Supplier Performance Risk Systems (SPRS)

CMMC Level 3 (Expert) will be assessed by government officials

Eases assessment requirements for companies not handling information related to prioritized acquisitions

Allowance of POA&Ms & Waivers

CMMC 2.0 will allow limited use of POA&Ms

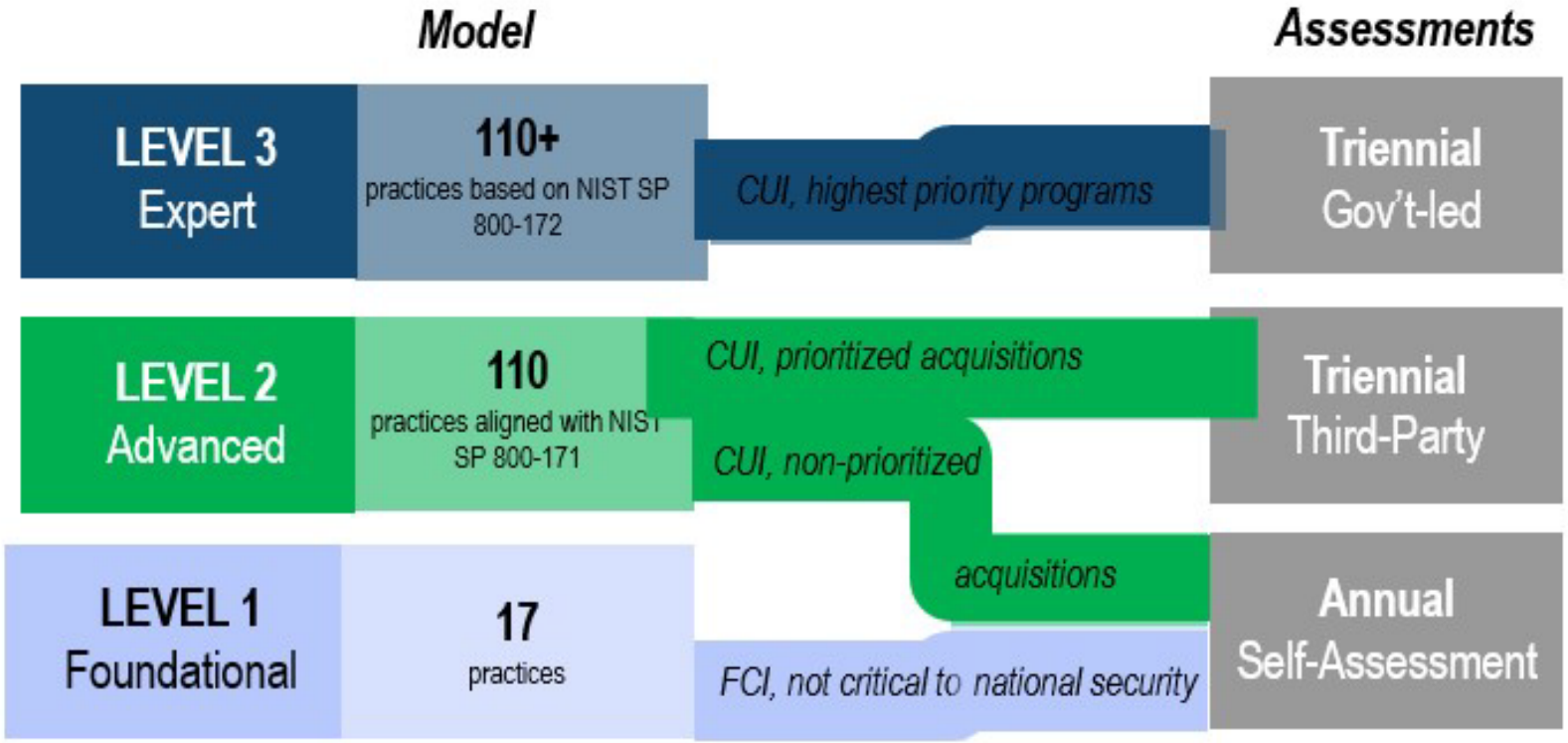
- **Strictly time-bound:** Potentially 180 days; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Limited use:** Will not allow POA&Ms for highest-weighted requirements; will establish a "minimum score" requirement to support certification with POA&Ms

Waivers will be allowed on a very limited basis, accompanied by strategies to mitigate CUI risk

- **Only allowed in select mission critical instances:** Government program office will submit the waiver request package including justification and risk mitigation strategies
- **Strictly time bound:** Timing to be determined on a case-by-case basis; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Will require senior DoD approval to minimize potential misuse of the waiver process**

Limited use of POA&Ms and waivers could allow the Department and DIB companies flexibility to meet evolving threats and make risk-based decisions

CMMC 2.0 Tailors Model and Assessment Requirements



Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

Rulemaking – Codifying CMMC 2.0

Changes will be released through a interim rule. A 60-day public comment period and concurrent congressional review will be included prior to the rule becoming effective.

- DoD has **mandatory rulemaking obligations** for CMMC that must be addressed as part of the CMMC 2.0 implementation
  - Rulemaking under 32 CFR is required to establish the CMMC program
  - Rulemaking under 48 CFR is required to update the contractual requirements in the DFARS to implement the CMMC 2.0 program
  - The DoD is suspending the CMMC Piloting effort and mandatory CMMC certification
- Timeline to complete all rulemaking requirements will be 9 to 24 months
  - The DoD will continue to encourage the DIB sector to enhance their cybersecurity posture during the interim period
  - The Department is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC 2.0 Level 2 certification in the interim period
  - The DIB's participation in CMMC will be voluntary until rulemaking formally implements CMMC 2.0

CMMC Timing

The 60-day comment period for the CMMC proposed rule began on December 26th, upon publication in the Federal Register.

When the comment period ends on February 26, 2024, DoD will adjudicate and respond to all relevant comment. This process could take 12-18 months, with the Final Rule expected to be published in late 2024 or early 2025. Once CMMC is incorporated into DFARS, contractors may be required to achieve CMMC certification prior to contract award. CMMC will be fully phased in over a 3 year period

Comments on the Proposed Rule

The comment period is your opportunity to directly influence the shape of the CMMC program. DoD is bound by law to consider and respond to comments. Comments can be submitted at the Federal eRulemaking Portal (https://www.regulations.gov) until February 26 2024.

Getting Ready for CMMC

Once CMMC is finalized, you will be required to meet its requirements.

CMMC will be phased in over time; however, you may not necessarily have more time to achieve CMMC certification. For example, your organization could be down the supply chain from another contractor subject to CMMC, in which case, per DFARS 252.204-7020, that contractors must flow down CMMC requirements to your organization.

As Matt Travis (CEO of the CyberAB) noted in a recent Preveil webinar: "If you're one of those companies…hoping that the protracted rule-making will save you, you're misguided and that's a pretty reckless way to run your business".

The average small company in the DIB will need 12-18 months to prepare for its CMMC assessment. That means that now is the time to improve your cybersecurity posture.

Security requirements of CMMC Level 2 mirror NIST SP 800-171, and so your most efficient path to CMMC Level 2 certification is via NIST SP 800-171 compliance.

NAVFAC Southeast Preparation For CMMC

- Communicating/Collaborating with Industry Partners
- Sending staff to CMMC certification training
- Developing templates and checklist to help review existing infrastructure and identify potential changes
- Preparing to conduct site visits

Questions?

How does this impact Joint Ventures? Based on Small Business Administration (SBA) regulation 13 C.F.R. § 125.8(e), CMMC should not be required from small business Joint Ventures (JVs). Instead, a small business JV should satisfy the requirement for CMMC on a given DOD contract as long as at least one of the JV partners that will handle the covered information on the contract has the necessary level of CMMC.

See the article located at:
https://www.congress.gov/117/meeting/house/112809/witnesses/HHRG-117-SM24-Wstate-TWilliamsJ-20210624.pdf

2. Where can I find a list of authorized C3PAO companies?
https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending