BILLING C

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Chapter I

Defense Acquisition Regulations System

48 CFR Chapter 2

Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward

AGENCY: Office of the Under Secretary of Defense for Acquisition and Sustainment, Department of Defense (DoD).

ACTION: Advanced notice of proposed rulemaking.

SUMMARY: This document provides updated information on DoD's way forward for the approved Cybersecurity Maturity Model Certification (CMMC) program changes, designated as "CMMC 2.0." CMMC 2.0 builds upon the initial CMMC framework to dynamically enhance Defense Industrial Base (DIB) cybersecurity against evolving threats. The CMMC framework is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors and provide assurance that Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) will be protected at a level commensurate with the risk from cybersecurity threats, including Advanced Persistent Threats. Under the CMMC program, DIB contractors will be required to implement certain cybersecurity protection standards, and, as required, perform self-assessments or obtain third-party certification as a condition of DoD contract award.

DATES: [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Visit the updated CMMC website for CMMC 2.0 updates: https://www.acq.osd.mil/cmmc/.

FOR FURTHER INFORMATION CONTACT: Ms. Diane Knight, Office of the Under Secretary of Defense for Acquisition and Sustainment, at 202-770-9100 or diane.l.knight10.civ@mail.mil.

SUPPLEMENTARY INFORMATION:

BACKGROUND

The CMMC program is designed to enhance DIB cybersecurity to meet evolving threats and safeguard the information that supports and enables the Warfighter.

Interim Defense Federal Acquisition Regulation Supplement (DFARS) rule, *Assessing Contractor Implementation of Cybersecurity Requirements* (DFARS Case 2019-D041), effective November 30, 2020, implemented DFARS clause 252.204-7021, *Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement*. This clause implemented the initial version of CMMC program, hereafter "CMMC 1.0."

CMMC 1.0 was designed to protect FCI and CUI shared with and handled by DoD contractors and subcontractors on non-federal contractor information systems. CMMC 1.0 involved five progressively advanced levels of cybersecurity standards and required that DIB contractors undergo a certification process to demonstrate compliance with the CMMC cybersecurity standards at a given level.

In March 2021, the Department initiated an internal assessment of CMMC 1.0 implementation that was informed by more than 850 public comments in response to the interim DFARS rule. This comprehensive, programmatic assessment of CMMC engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation. This review resulted in "CMMC 2.0," which updates the program structure and the requirements to streamline and improve implementation of the CMMC program.

WAY FORWARD

The changes reflected in the CMMC 2.0 framework will be implemented through the rulemaking process. DoD will pursue rulemaking in both: 1) Title 32 of the Code of Federal Regulations (CFR); and, 2) title 48 CFR, to establish CMMC 2.0 program requirements and implement any needed changes to the CMMC program content in 48 CFR. Both rules will have public comment periods.

Publication of title 32 and title 48 CFR rules will implement DoD's requirements for the updated CMMC version 2.0, which include various modifications from CMMC 1.0.
These modifications include:

- Eliminating levels 2 and 4, and renaming the remaining three levels in CMMC 2.0 as follows:
    - Level 1 (Foundational) will remain the same as CMMC 1.0 Level 1;
    - Level 2 (Advanced) will be similar to CMMC 1.0 Level 3;
    - Level 3 (Expert) will be similar to CMMC 1.0 Level 5.
- Removing CMMC-unique practices and all maturity processes from all levels;
- For CMMC Level 1 (Foundational), allowing annual self-assessments with an annual affirmation by DIB company leadership;
- Bifurcating CMMC Level 2 (Advanced) assessment requirements:
    - Prioritized acquisitions involving CUI will require an independent third party assessment;
    - Non-prioritized acquisitions involving CUI will require an annual self-assessment and annual company affirmation;
- For CMMC Level 3 (Expert), requiring Government-led assessments.
- Developing a time-bound and enforceable Plan of Action and Milestone process; and,

- Developing a selective, time-bound waiver process, if needed and approved.

The title 32 CFR rulemaking for CMMC 2.0 will be followed by additional title 48 CFR rulemaking, as needed, to implement any needed changes to the CMMC program content in 48 CFR. DoD will work through the rulemaking processes as expeditiously as possible.

Until the CMMC 2.0 changes become effective through both the title 32 CFR and title 48 CFR rulemaking processes, the Department will suspend the CMMC Piloting efforts and will not approve inclusion of a CMMC requirement in DoD solicitations.

The CMMC 2.0 program requirements will not be mandatory until the title 32 CFR rulemaking is complete, and the CMMC program requirements have been implemented as needed into acquisition regulation through title 48 rulemaking.

Dated: November 8, 2021.

Patricia L. Toppings,

OSD Federal Register Liaison Officer,

Department of Defense.

[FR Doc. 2021-24880 Filed: 11/16/2021 8:45 am; Publication Date: 11/17/2021]