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 CMMC program changes, designated as "CMMC 2.0." CMMC 2.0 builds upon the initial Cybersecurity Maturity Model Certification (CMMC) framework to dynamically enhance DIB cybersecurity against evolving threats. Under the CMMC program, Defense Industrial Base (DIB) contractors will be required to implement certain cybersecurity protection standards, and, as required, obtain Cybersecurity Maturity Model Certification as a condition of DoD contract award. 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. With CMMC 2.0, the Department is introducing several key changes that build on and refine the original CMMC framework.

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

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, which directed contractors to the Cybersecurity Maturity Model Certification (CMMC) 1.0 framework that was associated with DoD's initial vision for the CMMC framework.

The CMMC model 1.0 was designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) shared with and handled by DoD contractors and subcontractors on non-Federal contractor information systems. CMMC 1.0 used a certification process to assess a DIB contractor's compliance with the cybersecurity standards set forth in the CMMC Model. The CMMC Program is designed to enhance DIB cybersecurity to meet evolving threats and safeguard the information that supports and enables our warfighters, a top priority for the Department of Defense.

In March 2021, the Department initiated an internal assessment of the CMMC program's 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: 1) title 32 of the Code of Federal Regulations (CFR), to establish the CMMC 2.0 program; and, 2) title 48 CFR, to implement any needed changes to the CMMC program content in 48 CFR. Both rules will have public comment periods. Publication of the title 32 and title 48 CFR rules will implement DoD's requirements for the updated CMMC version 2.0, which include various modifications from the current program structure. These modifications include:

- Eliminating levels 2 and 4 and removing CMMC-unique practices and all maturity processes from the CMMC Model;
- Allowing annual self-assessments with an annual affirmation by DIB company leadership for CMMC Level 1;
- Bifurcating CMMC Level 3 requirements to identify prioritized acquisitions that would require independent assessment, and non-prioritized acquisitions that would require annual self-assessment and annual company affirmation;
- CMMC Level 5 requirements are still under development;
- Development of a time-bound and enforceable Plan of Action and Milestone process; and,
- Development of 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 to establish the contractual requirements and any needed changes to the CMMC program content resulting from the CMMC 2.0 changes codified in 32 CFR. The CMMC program team 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 1, 2021.

Patricia L. Toppings,

OSD Federal Register Liaison Officer,

Department of Defense.

[FR Doc. 2021-24160 Filed: 11/4/2021 8:45 am; Publication Date: 11/5/2021]