DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2023-OS-0096]

Cybersecurity Maturity Model Certification (CMMC) Program Guidance

AGENCY: Office of the Department of Defense Chief Information Officer (CIO), Department of Defense (DoD).

ACTION: Notice of availability: CMMC guidance.

SUMMARY: The Department of Defense announces the availability of eight guidance documents for the CMMC Program. These documents provide additional guidance for the CMMC model, assessments, scoring, and hashing.

DATES: Comments must be received by [INSERT DATE 60 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may use the following methods to submit comments on these guidance documents, identified by agency name, docket number DoD-2023-OS-0096, and title.

Comment Submission Methods include:

• Federal eRulemaking Portal: https://www.regulations.gov. Follow the instructions for submitting comments.

• Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name, docket number, and title for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Diane Knight, Office of the DoD CIO, 202–770–9100 or osd.mc-alex.dod-cio.mbx.cmmc-32cfr-rulemaking@mail.mil.

SUPPLEMENTARY INFORMATION:

CMMC Model Overview

DoD-CIO-00001 (ZRIN 0790-ZA17)

This document focuses on the CMMC Model as set forth in 32 CFR 170.14 of the CMMC Program proposed rule (See docket DoD-2023-OS-0063 on Regulations.gov). The model incorporates the security requirements from: 1) FAR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*, 2) NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and 3) a selected set of the requirements from NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*. The CMMC Program is designed to provide increased assurance to the DoD that defense contractors and subcontractors are compliant with information protection requirements for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) and are protecting such information at a level commensurate with risk from cybersecurity threats, including Advanced Persistent Threats (APTs).

CMMC Assessment Guide – Level 1

DoD-CIO-00002 (ZRIN 0790-ZA18)

This document provides guidance in the preparation for and execution of a Level 1 Self-Assessment under the CMMC Program as set forth in 32 CFR 170.15. CMMC Level 1 focuses on the protection of FCI, which is defined in 32 CFR 170.4 and 48 CFR 4.1901 as:

> *Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information*

provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

CMMC Level 1 is comprised of the 15 basic safeguarding requirements specified in Federal Acquisition Regulation (FAR) Clause 52.204-21.

CMMC Assessment Guide – Level 2

DoD-CIO-00003 (ZRIN 0790-ZA19)

This document provides guidance in the preparation for and execution of a Level 2 Self-Assessment or Level 2 Certification Assessment under the CMMC Program as set forth 32 CFR 170.16 and 170.17 respectively. An *Assessment* as defined in 32 CFR 170.4 means:

The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization as defined in 32 CFR 170.15 to 32 CFR 170.18. For CMMC Level 2 there are two types of assessments:

- *A Self-Assessment is the term for the activity performed by an entity to evaluate its own CMMC Level, as applied to Level 1 and some Level 2.*
- *A CMMC Level 2 Certification Assessment is the term for the activity performed by a Certified Third-Party Assessment Organization (C3PAO) to evaluate the CMMC Level of an OSC.*

32 CFR 170.16(b) describes contract or subcontract eligibility for any contract with a CMMC Level 2 Self-Assessment requirement, and 32 CFR 170.17(b) describes contract or subcontract eligibility for any contract with a CMMC Level 2 Certification Assessment requirement. Level 2 Certification Assessment requires the OSA achieve either a Level 2 Conditional Certification Assessment or a Level 2 Final Certification Assessment, as described in 32 CFR 170.4, obtained through an assessment by an accredited Certified Third-Party Assessment Organization (C3PAO).

CMMC Assessment Guide – Level 3

DoD-CIO-00004 (ZRIN 0790-ZA20)

This document provides guidance in the preparation for and execution of a Level 3 Certification Assessment under the CMMC Program as set forth in 32 CFR 170.18. Certification at each CMMC level occurs independently. An *Assessment* as defined in 32 CFR § 170.4 means:

> *The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system, or organization as defined in 32 CFR 170.15 to 32 CFR 170.18*.

A *CMMC Level 3 Certification Assessment* as defined in 32 CFR 170.4 is the term for the activity performed by the Department of Defense to evaluate the CMMC Level of an OSC. For CMMC Level 3, assessments are performed exclusively by the DoD.

An OSC seeking a CMMC Level 3 Certification Assessment must have first received a CMMC Level 2 Final Certification Assessment, as set forth in 32 CFR 170.18, for all applicable information systems within the CMMC Assessment Scope, and the OSC must implement the Level 3 requirements specified in 32 CFR 170.14(c)(4). This is followed by the CMMC Level 3 assessment conducted by the DoD.

OSCs may also use this guide to perform CMMC Level 3 self-assessment (for example, in preparation for an annual affirmation); however, they are not eligible to submit results from a self-assessment in support of a CMMC Level 3 Certification Assessment. Only the results from an assessment by the DoD are considered for award of a CMMC Level 3 Certification Assessment. Level 3 reporting and affirmation requirements can be found in 32 CFR 170.18 and 32 CFR 170.22.

CMMC Scoping Guide – Level 1

DoD-CIO-00005 (ZRIN 0790-ZA21)

This document provides scoping guidance for Level 1 of CMMC as set forth in 32 CFR 170.19. Prior to a Level 1 CMMC Self-Assessment the OSA must specify the CMMC Assessment Scope. The CMMC Assessment Scope defines which assets within the OSA's environment will be assessed and the details of the self-assessment.

This guide is intended for OSAs that will be conducting a CMMC Level 1 self-assessment and the professionals or companies that will support them in those efforts.

CMMC Scoping Guide – Level 2

DoD-CIO-00006 (ZRIN 0790-ZA22)

This document provides scoping guidance for Level 2 of CMMC as set forth in 32 CFR 170.19. Prior to a Level 2 Self-Assessment or Level 2 Certification Assessment, the OSA must specify the CMMC Assessment Scope. The CMMC Assessment Scope defines which assets within the OSA's environment will be assessed and the details of the assessment.

This guide is intended for OSAs that will be conducting a CMMC Level 2 Self-Assessment in accordance with 32 CFR 170.16, OSCs that will be obtaining a CMMC Level 2 Certification Assessment in accordance with 32 CFR 170.17, and the professionals or companies that will support them in those efforts. OSCs are a subset of OSAs as all organizations will participate in an assessment, but self-assessment cannot result in certification.

CMMC Scoping Guide – Level 3

DoD-CIO-00007 (ZRIN 0790-ZA23)

This document provides scoping guidance for Level 3 of CMMC as set forth in 32 CFR 170.19. Prior to conducting a CMMC assessment, the Level 3 CMMC Assessment Scope must be defined as set forth in 32 CFR 170.19(d). The CMMC Assessment Scope defines which assets within the OSC's environment will be assessed and the details of the assessment.

When seeking a Level 3 Certification, the OSC must have a CMMC Level 2 Final Certification Assessment for the same scope as the Level 3 assessment. Any Level 2 Plan of Action and Milestones (POA&M as set forth in 32 CFR 170.4) items must be closed prior to the initiation of

the CMMC Level 3 assessment. The CMMC Level 3 CMMC Assessment Scope may be a subset of the Level 2 CMMC Assessment Scope (e.g., a Level 3 data enclave with greater restrictions and protections within the Level 2 data enclave).

This guide is intended for OSCs that will be obtaining a CMMC Level 3 assessment and the professionals or companies that will support them in those efforts.

CMMC Hashing Guide

DoD-CIO-00008 (ZRIN 0790-ZA24)

This guide assumes that the reader has a basic understanding of command line tools and scripting. During the performance of a CMMC assessment, the assessment team will collect objective evidence using a combination of three assessment methods:

- examination of artifacts,
- affirmations through interviews, and
- observations of actions.

Because these OSA artifacts may be proprietary, the assessment team will not take OSA artifacts offsite at the conclusion of the assessment. For the protection of all stakeholders, the OSA must retain the artifacts. This guide describes how to provide a cryptographic reference (or hash) for each artifact used in the assessment as discussed in 32 CFR 170.17 and 170.18.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2023-27281 Filed: 12/22/2023 8:45 am; Publication Date: 12/26/2023]