Business and Technology Advisory

March 2025

Cybersecurity Maturity Model Certification (CMMC) Implementation for Department of Defense Contracts

Overview

- On December 16, 2024, the U.S. Department of Defense (DoD) finalized the Cybersecurity Maturity Model Certification (CMMC) rule, which requires that all DoD contractors must implement CMMC to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
- Cooperatives with DoD contracts, such as utility privatization (UP) contracts, must implement CMMC, which aligns with the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information on Nonfederal Systems and Organizations."
- NRECA's Co-op Cyber Goals provide an on-ramp for cooperatives serving military organizations and required to implement CMMC.

CMMC Background

Prior to the 2010 Executive Order (EO) 13556, *Controlled Unclassified Information*, markings for sensitive information varied across government agencies leading to confusion and disparate safeguarding practices across government and indusry. This led to "a patchwork system that failed to adequately safeguard information requiring protection, and unnecessarily restricted information-sharing."[1] The EO established the Controlled Unclassifed Information (CUI) Program to standardize information handled by the executive branch.

In 2019, DoD announced CMMC to secure the Defense Industrial Base (DIB) sector against evolving cybersecurity threats and move away from the "self-attestation" model of security. Between 2019 and today, DoD has gone through several iterations of the CMMC program after engaging with industry and conducting internal reviews on implementation. Currently, the CMMC program has three key features:

- **Tiered Model:** CMMC requires companies with Federal Contract Information (FCI) and CUI to implement cybersecurity standards at progressively advanced levels, depending on the information the companies handle.
- **Assessment Requirement:** CMMC assessments let DoD verify the implementation of cybersecurity standards (NIST 800-171).
- **Phased Implementation:** Once CMMC is fully implemented, certain contractors handling FCI and CUI will be required to achieve certain CMMC levels conditional in their contract awards.

[1] "Cybersecurity Maturity Model Certification (CMMC) Program." https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

CMMC Levels

Organizations Seeking Assessment (OSA) (i.e., military serving cooperatives) that want to comply with program requirements, should be prepared to meet certain requirements for DoD solicitations to be eligible for contract award.

- **Level 1 (Self):** A self-assessment to secure FCI processed, stored, or transmitted in the course of fulfilling the contract. OSA must comply with 15 security requirements set by Federal Acquisitions Regulation (FAR) 52.204-21.
- **Level 2 (Self):** A self-assessment to secure CUI processed, stored, or transmitted in the course of fulfilling the contract. OSA must comply with 110 Level 2 security requirements from NIST SP 800-171 Revision 2.
- **Level 2 (Third-Party):** Differs from self-assessment method of compliance verification. OSAs must hire a CMMC Third-Party Assessment Organization (C3PAO) to conduct an external assessment of the 110 security requirements in NIST SP 800-171. Approved C3PAO are available on the Cyber AB website.
- **Level 3 (Defense Assessment Center):** A government assessment of 24 additional requirements from NIST SP 800-171. OSA must achieve Level 2 compliance before moving to Level 3 assessments. To kick off a Level 3 assessment by the appropriate authority – the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) – OSA can find a point of contact at www.dcma.mil/DIBCAC (include Level 2 certification unique identifier in your email).

DoD has not yet provided guidance on which Level certification UP contracts will require. Military serving cooperatives will need to carefully read contract requirements before submitting cybersecurity plans. Consider reviewing and implementing NIST SP 800-171 security controls as soon as possible.

NRECA Co-op Cyber Goals and CMMC

NRECA's Co-op Cyber Goals Program defines specific cybersecurity goals aimed at helping co-ops achieve high-priority security measures and creates a benchmark for implementing cybersecurity fundamentals. This program was created by NRECA as a voluntary way for co-ops to advance their cybersecurity.

For military serving cooperatives, the Co-op Cyber Goals may provide an initial step toward CMMC compliance. The Co-op Cyber Goals do not encompass all 110 security controls under NIST SP 800-171, but some Cyber Goals can be mapped to 800-171 controls and may help kickstart the journey toward CMMC certification. NRECA is committed to helping its military serving cooperatives with services and resources that will support their efforts to meet CMMC requirements and secure their environments.

Questions?

Military serving cooperatives who would like to learn more about the CMMC program and how NRECA is working to support members can reach out to:

- Lauren Khair, Senior Director of Energy Research and Resilience (lauren.khair@nreca.coop), or
- Adrian McNamara, Cybersecurity Program Manager (adrian.mcnamara@nreca.coop).