PRONTOTECH
(703) 881-4605

What is CMMC Compliance?

If you are a contractor or subcontractor working with the Department of Defense (DoD), you may have heard of the Cybersecurity Maturity Model Certification (CMMC) program. CMMC is a new framework that requires formal third-party audits of your cybersecurity practices to ensure that you can protect sensitive unclassified information, such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), that is shared by the DoD.

CMMC was initially launched in 2020, but it has undergone significant changes since then. In November 2021, the DoD announced a revised version of CMMC, designated as CMMC 2.0, which aims to simplify and streamline the certification process, reduce costs and barriers for small businesses, and enhance cybersecurity across the Defense Industrial Base (DIB).

PRONTOTECH
(703) 881-4605

What is CMMC 2.0?

CMMC 2.0 is a revised version of CMMC that introduces some key changes to the original framework. Some of the main differences are:

- CMMC 2.0 reduces the number of certification levels from five to three: Basic, Intermediate, and Advanced. Each level corresponds to a set of cybersecurity practices and processes that contractors must implement and document.

- CMMC 2.0 allows contractors to self-assess their compliance at the Basic level, which covers the minimum security requirements for handling FCI. Contractors can use a self-assessment tool provided by the DoD and submit their results online.

- CMMC 2.0 requires contractors to obtain third-party certification at the Intermediate and Advanced levels, which cover the additional security requirements for handling CUI. Contractors must undergo an audit by an independent CMMC Third-Party Assessor Organization (C3PAO) accredited by the Cyber AB (formerly CMMC Accreditation Body).

- CMMC 2.0 aligns its cybersecurity practices and processes with existing standards and frameworks, such as NIST SP 800-171, NIST SP 800-53, ISO/IEC 27001, and CIS Controls.

- CMMC 2.0 aligns its cybersecurity practices and processes with existing standards and frameworks, such as NIST SP 800-171, NIST SP 800-53, ISO/IEC 27001, and CIS Controls.

PRONTOTECH
(703) 881-4605

Steps to CMMC 2.0 Compliance

1. Identify what type of unclassified information your organization will handle and determine the CMMC certification level you need. You can use the DoD's online tool to help you with this step.

2. Conduct a readiness assessment and gap analysis to determine how prepared your organization is for a compliance audit and which areas require immediate attention. You can use a self-assessment tool or consult a CMMC Registered Provider Organization (RPO) for guidance.

3. Implement a cybersecurity detection and alerting system that can monitor your network activity, detect threats, and alert you of any incidents or breaches. You can use a security information and event management (SIEM) solution or a managed security service provider (MSSP) for this purpose.

4. Develop a System Security Plan (SSP) that documents your cybersecurity practices and processes, roles and responsibilities, policies and procedures, and tools and technologies. You can use a template provided by NIST or consult a CMMC RPO for assistance.

5 Stay up to date with the latest developments and guidance on CMMC 2.0 by visiting the official website: https://dodcio.defense.gov/CMMC/.

6 Talk to your subcontractors and suppliers and ensure that they are also compliant with CMMC 2.0 requirements at the appropriate level. You can use contractual clauses or agreements to enforce this requirement.

7 Evaluate your internal resources and capabilities and determine if you need external help to achieve compliance. You can hire a CMMC RPO or a C3PAO to assist you with your preparation and certification process.

8 Stay agile and flexible and be ready to adapt to any changes or updates in CMMC 2.0 requirements as they are finalized.