SmartSuite

Framework / Cybersecurity / CMMC

CMMC 2.0 – Level 1 / Level 2 / Level 3

CMMC 2.0 sets cybersecurity requirements to protect controlled unclassified information for DoD contractors and suppliers.

What it is

CMMC 2.0 (Cybersecurity Maturity Model Certification) is a US Department of Defense (DoD) cybersecurity compliance framework that establishes requirements for protecting controlled unclassified information (CUI) within the defense industrial base. Its primary purpose is to ensure that contractors and suppliers implement effective cybersecurity controls to safeguard sensitive government data.

Developed and maintained by the DoD, CMMC 2.0 is required for organizations seeking to bid on or participate in federal defense contracts. The framework incorporates cybersecurity practices and processes drawn from standards like NIST SP 800-171 and NIST SP 800-53, covering areas such as access control, incident response, system security, and risk management.

At a glance

PUBLISHER U.S. Department of Defense (DoD)	TYPE Certification / Assurance Program	VERSION CMMC 2.0
EFFECTIVE November 4, 2021	DOMAIN Cybersecurity	FAMILY CMMC
REGION United States	INDUSTRY Aerospace & Defense	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://dowcio.war.gov/CMMC/About/

Why it matters

- **Strengthen cybersecurity governance** Support consistent implementation of security controls, promoting accountability and clear roles across organizational processes and functions.
- **Enhance regulatory alignment** Facilitate compliance with federal requirements and industry standards by aligning controls with NIST and Department of Defense regulations.
- **Increase contract eligibility** Enable organizations to compete for and maintain defense contracts through verified demonstration of effective cybersecurity practices.
- **Improve risk management** Support proactive identification, assessment, and mitigation of security risks that could compromise sensitive government data.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CMMC 2.0

FCI Scope and System Boundary

Document where FCI exists and how it flows to keep scope clean and auditable.

Level 1 Practice Library

Track required practices with owners, procedures, and proof of completion.

Evidence Collection and Attestation Support

Centralize evidence needed for annual self-assessment and affirmation.

Recurring Security Hygiene Cadence

Schedule access reviews, patching, and basic monitoring activities with proof.

Exceptions and Remediation Tracking

Manage gaps, corrective actions, and closure evidence with clear accountability.

Readiness Reporting

Report practice status, open gaps, and progress for leadership review.

Common framework mappings

CIS Controls v8.1 | DFARS 252.204-7012 | FedRAMP Rev. 5 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-171 Rev. 3 | NIST SP 800-172 | NIST 800-53 Rev.5

Official resources

CMMC 2.0 Overview

Provides an official overview of the Cybersecurity Maturity Model Certification 2.0 framework.

acq.osd.mil/cmmc/index.html

CMMC 2.0 Model Documentation

Describes the CMMC 2.0 framework and details its requirements and maturity levels.

acq.osd.mil/cmmc/docs.html

CMMC 2.0 Assessment Guides

Outlines procedures for assessing compliance with CMMC 2.0 controls and practices.

acq.osd.mil/cmmc/assessment-guides.html

Frequently asked questions

What is CMMC 2.0 used for?

CMMC 2.0 is used to ensure defense contractors and suppliers protect Controlled Unclassified Information (CUI) when working with the U.S. Department of Defense. It standardizes cybersecurity practices across the defense industrial base, aligning requirements with data sensitivity and contractual risk.

Is CMMC 2.0 required or certifiable?

Yes, CMMC 2.0 is a mandatory certification for organizations seeking to bid on or execute certain U.S. Department of Defense contracts. Depending on the contract's requirements and the sensitivity of the CUI involved, companies must demonstrate compliance at the appropriate CMMC maturity level, often through independent third-party assessment.

Who needs to comply with CMMC 2.0?

CMMC 2.0 applies to all organizations in the defense supply chain that store, process, or transmit controlled unclassified information on behalf of the U.S. Department of Defense. This includes prime contractors and subcontractors who handle Federal Contract Information (FCI) or CUI.

What are the CMMC 2.0 maturity levels and how do they differ?

CMMC 2.0 is structured into three maturity levels: Level 1 (Foundational), Level 2 (Advanced), and Level 3 (Expert). Each level represents an increasing set of cybersecurity practices and processes, with Level 1 focusing on basic safeguarding, Level 2 incorporating NIST SP 800-171 controls for CUI, and Level 3 addressing advanced, threat-based standards.

What core artifacts or documentation are required for CMMC 2.0 compliance?

Key artifacts for CMMC 2.0 compliance include up-to-date system security plans (SSP), documented cybersecurity policies and procedures, risk assessment reports, and evidence of control implementation. Organizations must also maintain records of self-assessments and, where required, results from independent third-party assessments.

How does CMMC 2.0 relate to other cybersecurity frameworks?

CMMC 2.0 incorporates controls and principles from NIST SP 800-171 and NIST SP 800-53, building on existing federal cybersecurity requirements. Organizations with established compliance programs for these standards may leverage prior efforts as a foundation, but must map and validate their controls against CMMC criteria.

How would SmartSuite support CMMC 2.0?

SmartSuite enables organizations to manage CMMC 2.0 by providing centralized control libraries, robust risk tracking, automated evidence collection, and workflow-driven remediation management. Interactive dashboards assist with real-time compliance monitoring and reporting, helping teams maintain audit readiness and efficiently demonstrate adherence to CMMC requirements.

License included / downloadable: Yes CMMC documentation is published by the U.S. DoD and is publicly available through official DoD resources.

Full framework page and mappings: smartsuite.com/frameworks/cmmc-2-0-cybersecurity-maturity-model-certification

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.