SmartSuite

Framework / Cybersecurity / CMMC

CMMC 2.0 – Level 2

CMMC 2.0 Level 2 requires DoD contractors to implement NIST-aligned security controls to protect Controlled Unclassified Information.

What it is

CMMC 2.0 Level 2 is a cybersecurity compliance framework that helps organizations implement and maintain robust security controls to protect Controlled Unclassified Information (CUI) within the defense industrial base. This level aims to ensure that contractors handling sensitive government data implement practices aligned with federal requirements to mitigate cyber threats.

Developed and administered by the U.S. Department of Defense (DoD), CMMC 2.0 Level 2 aligns closely with NIST SP 800-171, requiring organizations to demonstrate adherence to more than 100 specific cybersecurity practices. It is primarily used by DoD contractors and subcontractors that store, process, or transmit CUI and covers areas such as access control, incident response, risk management, and system integrity.

At a glance

PUBLISHER U.S. Department of Defense (DoD)	TYPE Certification / Assurance Program	VERSION 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 implementation of defined security practices, improving oversight and accountability for protecting sensitive government data.
- **Enhance regulatory alignment** Align organizational controls with federal standards, helping contractors clearly demonstrate compliance with Department of Defense expectations.
- **Promote operational resilience** Reduce vulnerability to cyber threats by establishing controls addressing risk management, system integrity, and business continuity.
- **Increase audit readiness** Facilitate the maintenance of proper documentation and readiness for assessment, supporting contract competitiveness and regulatory obligations.

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

How SmartSuite supports CMMC 2.0 L2

CUI Scope and Enclave Boundaries

Define CUI boundaries, enclaves, and dependencies with audit-ready documentation.

800-171 Alignment Library

Track Level 2 requirements mapped to 800-171 with owners and evidence.

SSP and POA&M Operations

Maintain SSP content and manage POA&Ms through remediation and retesting.

Evidence and Assessment Readiness

Centralize proof for each requirement with timestamps and reviewer history.

Continuous Compliance Cadence

Schedule recurring activities for access, patching, logging, and incident readiness.

CMMC Assessment Readiness Reporting

Report readiness, gaps, and remediation progress across systems and teams.

Common framework mappings

CIS Controls v8.1 | CMMC 2.0 | CMMC 2.0 Level 3 | ISO 27001:2022 | NIST CSF 2.0 | NIST SP 800-161 Rev.1 | NIST 800-171 Rev. 3 | NIST 800-53 Rev.5

Official resources

CMMC 2.0 Model Overview

Provides an overview of the CMMC 2.0 framework and its compliance requirements for contractors.

acq.osd.mil/cmmc/index.html

CMMC 2.0 Assessment Guide for Level 2

Outlines the assessment process and practices for organizations seeking CMMC Level 2 certification.

acq.osd.mil/cmmc/docs/CMMC_Assessment_Guide_Level-2_v2.pdf

CMMC 2.0 Program Enhancements

Describes updates and improvements in the CMMC 2.0 framework for cybersecurity compliance.

acq.osd.mil/cmmc/program_enhancements.html

Frequently asked questions

What is CMMC 2.0 Level 2 used for?

CMMC 2.0 Level 2 is designed to protect Controlled Unclassified Information (CUI) within the defense industrial base by requiring the implementation of specific cybersecurity controls. It ensures that organizations working with the U.S. Department of Defense (DoD) mitigate cyber risks and safeguard sensitive government data.

Is CMMC 2.0 Level 2 mandatory for DoD contractors?

Yes, CMMC 2.0 Level 2 is mandatory for DoD contractors and subcontractors that store, process, or transmit CUI, as specified in applicable contract requirements. Certification, often through third-party or self-assessments, is required prior to contract award to demonstrate compliance.

What organizations are in scope for CMMC 2.0 Level 2?

CMMC 2.0 Level 2 applies to all organizations in the defense supply chain that handle, process, or store Controlled Unclassified Information as part of DoD contracts. This includes both primary contractors and their subcontractors.

What are the key requirements and control families for CMMC 2.0 Level 2?

CMMC 2.0 Level 2 requires organizations to comply with all 110 security controls from NIST SP 800-171, organized into control families such as access control, incident response, and risk assessment. Required artifacts include documented policies, procedures, and evidence supporting control implementation.

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

How do organizations implement CMMC 2.0 Level 2 controls?

Organizations implement CMMC 2.0 Level 2 by mapping NIST SP 800-171 controls to existing security policies and practices, identifying gaps, remediating deficiencies, and documenting control effectiveness. Regular risk assessments and continuous monitoring are essential for ongoing compliance.

How does CMMC 2.0 Level 2 align with other frameworks like NIST SP 800-171?

CMMC 2.0 Level 2 is closely aligned with NIST SP 800-171, adopting its 110 controls as the baseline for compliance. This harmonization enables organizations already compliant with NIST SP 800-171 to streamline the path to CMMC 2.0 Level 2 certification.

What are the ongoing compliance and assessment requirements for CMMC 2.0 Level 2?

Ongoing compliance for CMMC 2.0 Level 2 involves conducting periodic self-assessments or third-party assessments as required, maintaining documentation and evidence of control operation, remediating findings, and ensuring continuous improvement of the security program.

How would SmartSuite support CMMC 2.0 Level 2?

SmartSuite helps organizations manage CMMC 2.0 Level 2 by importing control libraries, facilitating risk tracking for suppliers, and centralizing control management. It supports collection of compliance evidence, maintains audit readiness, delivers remediation workflows, and provides reporting dashboards to monitor and demonstrate compliance.

License included / downloadable: Yes CMMC 2.0 documentation is published by the U.S. DoD and the model and level requirements are freely available. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/cmmc-2-0-l2

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