Framework Foundations: Cybersecurity Maturity Model Certification (CMMC)

Introduction to CMMC

The Cybersecurity Maturity Model Certification (CMMC) is a U.S. Department of Defense (DoD) framework designed to safeguard sensitive government data – specifically Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) – across the Defense Industrial Base (DIB). It aligns with NIST SP 800-171 and SP 800-172 and establishes tiered cybersecurity requirements based on the sensitivity of data handled.

A recent final rule published in the Federal Register (DFARS Case 2019-D041) formally embeds CMMC into DoD contracting. It mandates verification of CMMC status in the Supplier Performance Risk System (SPRS), annual affirmations of compliance by an affirming official, and phased implementation culminating in full enforcement by November 2025. This rule reinforces CMMC as a contract eligibility requirement and strengthens accountability across the supply chain.

CMMC Objectives:

- Safeguard sensitive DoD data via enforced cybersecurity across the DIB.
- Align security practices to data sensitivity through a tiered maturity model.
- Drive accountability and improvement via assessments and certification.
- Streamline compliance by aligning with NIST SP 800-171/172.
- Ensure contract eligibility through mandatory cybersecurity certification.

Key Requirements

CMMC is structured into three certification levels, each representing a progressively advanced set of cybersecurity practices:

- **Level 1** – Foundational: Focuses on basic safeguarding of FCI, aligned with FAR 52.204-21. Requires annual self-assessment and affirmation.
- **Level 2** – Advanced: Aligns with NIST SP 800-171 and includes 110 practices for protecting CUI. Requires third-party assessment every three years or self-assessment for select programs.
- **Level 3** – Expert: Incorporates NIST SP 800-172 for enhanced protection of critical CUI. Requires a government-led assessment (DIBCAC) every three years.

Organizations must undergo regular assessments to maintain certification:

- **Self-assessments** for Level 1 (annually).
- **Third-party assessments** for Levels 2 and 3 (every three years).
- **Annual affirmations** across all levels to confirm continued compliance.

CMMC also defines 14 cybersecurity domains, such as Access Control, Incident Response, and System Integrity, which group related practices and form the foundation of the framework's security posture.

CMMC Model	Model	Assessment
Level 1	**134 requirements** (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)	• DIBCAC certification assessment every 3 years • Annual Affirmation
Level 2	**110 requirements** aligned with NIST SP 800-171 R2	• C3PAO Certification assessment every 3 years • Self assessment every 3 years for select programs • Annual Affirmation
Level 3	**15 requirements** aligned with FAR 52.204-21	• Annual Self Assessment • Annual Affirmation

How Cisco Security + Splunk Supports Compliance

Cisco offers a comprehensive portfolio of security solutions that can help organizations meet the requirements of CMMC.

CMMC Domain	How Cisco + Splunk Support Compliance	Products
Access Control (AC)	Policy-based access control, network segmentation, multi-factor authentication	Cisco ISE, Cisco Duo, Cisco Secure Network Analytics (SNA), Cisco Secure Firewalls, Cisco Secure Endpoint, Splunk Enterprise Security (ES), Splunk SOAR
Awareness & Training (AT)	Real-time threat intelligence to inform training and awareness	Cisco Talos, Splunk Enterprise Security (ES)
Audit & Accountability (AU)	Continuous monitoring, threat detection, compliance reporting	Cisco Secure Network Analytics (SNA), Cisco XDR, Splunk Enterprise/Cloud, Splunk Enterprise Security (ES)
Configuration Management (CM)	Configuration tracking, change management, automated compliance checks	Cisco FMC, Cisco XDR, Cisco SNA, Splunk Enterprise Security (ES), Splunk ITSI
Identification & Authentication (IA)	Multi-factor authentication, identity visibility, AI-driven analytics	Cisco Duo, Cisco ISE, Cisco Identity Intelligence, Splunk Enterprise Security (ES)
Incident Response (IR)	Incident triage, threat containment, automated response	Talos IR, Cisco XDR, Cisco SNA, Splunk SOAR, Splunk Enterprise Security (ES)
Maintenance (MA)	System updates, security patches, real-time threat protection	Secure Email and Web Manager, Secure Firewall, Cisco Umbrella, Splunk Enterprise Security (ES)
Media Protection (MP)	Data encryption, secure communications, malware protection	Cisco Firepower, Cisco Umbrella, Cisco Secure Email, Splunk Enterprise Security (ES)
Personnel Security (PS)	Access control, user activity monitoring	Cisco Duo, Cisco SNA, Cisco ISE, Splunk Enterprise Security (ES)
Physical Protection (PE)	Video surveillance, electronic access control, situational awareness	Meraki Smart Cameras, Physical Access Manager, Video Surveillance Manager, Splunk Enterprise/Cloud
Risk Assessment (RA)	Risk assessment, threat detection, vulnerability management	Cisco Duo, Cisco SNA, Cisco ISE, Splunk Enterprise Security (ES), Splunk Security Essentials
Security Assessment (CA)	Security audits, compliance checks, continuous monitoring	Meraki Smart Cameras, Physical Access Manager, Video Surveillance Manager, Splunk Enterprise Security (ES)
System & Communications Protection (SC)	Network security, secure communications, threat protection	Cisco Firepower, Cisco Umbrella, Cisco Secure Email, Splunk Enterprise Security (ES)
System & Information Integrity (SI)	Malware protection, threat intelligence, automated response	Cisco Secure Endpoint, Cisco Talos, Cisco XDR, Splunk Enterprise Security (ES), Splunk SOAR

CMMC Compliance with Cisco Security + Splunk

As cybersecurity requirements across the Defense Industrial Base (DIB) become more rigorous, organizations must adopt integrated, scalable solutions that align with CMMC. The framework's tiered structure and emphasis on protecting FCI and CUI demand a proactive, data-driven approach to security.

Cisco and Splunk together provide a foundation for supporting CMMC compliance. The Cisco Security portfolio – anchored by Cisco XDR – offers deep visibility, automated threat detection, and rapid response across all 14 CMMC domains. Splunk complements this with powerful analytics, centralized log management, and orchestration capabilities that streamline audits, assessments, and incident response.

Our solutions enable:

- **Comprehensive coverage of CMMC domains**, from access control and system integrity to audit and accountability.
- **Automated compliance workflows**, reducing manual effort and improving accuracy.
- **Real-time threat detection and response**, powered by Cisco XDR and Splunk SOAR.
- **Scalable support for all certification levels**, from foundational to expert.

By leveraging the Cisco Security portfolio and Splunk, defense contractors can simplify their path to CMMC certification, reduce risk exposure, and ensure operational resilience. This integrated approach not only supports compliance but also strengthens overall cybersecurity maturity – positioning organizations to meet evolving DoD requirements with confidence.

Resources

For more information and guidance on CMMC compliance, please refer to the following resources:

- Cisco: What is CMMC?
- Cisco modernizes government cybersecurity
- Solutions for federal government
- Splunk for public sector
- Splunk for CMMC

P1109080118 10/25