BitLyft

OPERATING SECURITY FOR CMMC LEVEL 2

A TECHNICAL GUIDE TO CMMC LEVEL 2

INDEX

INTRODUCTION

CMMC Compliance is an Operational Challenge

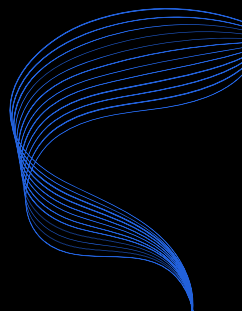
The Cybersecurity Maturity Model Certification (CMMC) program represents a major shift in how the Department of War (Formally Department of Defense) protects sensitive information across the Defense Industrial Base.

For many years, contractors relied on self-attestation against security frameworks such as NIST SP 800-171. While these requirements technically existed, enforcement was inconsistent and implementation varied widely across the supply chain.
CMMC changes that model.

Under CMMC 2.0, contractors must now demonstrate that the systems responsible for handling Controlled Unclassified Information (CUI) meet defined security practices and are capable of operating those controls in real environments.

Certification requires verification through an independent third-party assessor, meaning organizations must be able to demonstrate not only that controls exist, but that they are actively functioning.
For many contractors, the challenge is not understanding the framework.

The challenge is operating the technical security capabilities required to meet it.



WHY CMMC LEVEL 2 IS DIFFICULT

CMMC Level 2 aligns closely with the 110 security requirements defined in NIST SP 800-171, which focus on protecting Controlled Unclassified Information within contractor environments.While these requirements are well documented, implementation can be complex, particularly for small and mid-sized organizations within the Defense Industrial Base.

Security Monitoring

Many organizations deploy security tools such as endpoint protection or identity management systems, but cannot continuously monitor security telemetry across those platforms.

Incident Detection

Without centralized logging or behavioral analytics, suspicious activity often goes undetected until after an incident has occurred.

Investigation and Response

CMMC expects organizations to have the capability to investigate security events and respond appropriately, but most contractors do not maintain a full security operations center.

Log Collection and Retention

Several NIST 800-171 controls require organizations to generate, retain, and review audit logs across multiple systems. Without centralized visibility, these logs provide limited security value.

Resource Constraints

Building and staffing an internal SOC capable of 24/7 monitoring can require significant investment in both personnel and technology.

UNDERSTANDING CMMC ENCLAVE

One of the most effective strategies for achieving CMMC compliance is the implementation of a CMMC enclave. A CMMC enclave is a defined environment that isolates the systems responsible for storing, processing, or transmitting Controlled Unclassified Information.By clearly defining the boundary of this environment, organizations can focus their compliance efforts on the systems that directly interact with CUI rather than applying the full scope of NIST SP 800-171 controls across their entire corporate infrastructure.

Enclaves Typically Include

1. Workstations that access CUI
2. Servers that store or process CUI
3. Identity systems used for authentication
4. Applications used to manage defense contract data
5. Logging and monitoring systems supporting the enclave

Establishing this boundary helps organizations maintain a clear CMMC scope, which is critical during third-party assessments.

The Operational Security Gap

Implementing technical controls is only part of the CMMC requirement. Organizations must also demonstrate that those controls are actively monitored and maintained.

For example:

- Access control policies must be enforced and reviewed
- Audit logs must be generated and analyzed
- Security alerts must be investigated
- Incidents must be documented and responded to appropriately

This operational layer is where many organizations struggle.
Even when security tools are in place, the processes required to monitor, investigate, and respond to security events often remain incomplete.

NIST SP 800-171:

The Security Foundation Behind CMMC Level 2

At the core of **CMMC Level 2** are the security requirements defined in **NIST Special Publication 800-171**.

NIST SP 800-171 was developed to define how non-federal organizations should safeguard **Controlled Unclassified Information (CUI)** when it resides on contractor systems rather than government networks. The framework establishes **110 security requirements across 14 control families**, designed to protect the confidentiality, integrity, and availability of sensitive defense information.

While CMMC defines **how compliance is assessed**, NIST SP 800-171 defines **what security controls must exist** within contractor environments.

For organizations pursuing **CMMC Level 2 certification**, these 110 requirements form the technical and operational foundation of the assessment.

14 Control Families of NIST

1. **Access Control (AC) -** Limit access to authorized users and devices.
2. **Awareness & Training (AT) -** Ensure personnel understand cybersecurity responsibilities
3. **Audit & Accountability (AU) -** Track system activities to detect and analyze incidents.
4. **Configuration Management (CM) -** Establish secure baseline configurations and manage system changes.
5. **Identification & Authentication (IA) -** Verify user identities and enforce strong authentication.
6. **Incident Response (IR) -** Prepare for, detect, and respond to security incidents.
7. **Maintenance (MA) -** Manage and control system maintenance activities securely.
8. **Media Protection (MP) -**Safeguard data on physical and digital media.
9. **Personnel Security (PS) -** Screen and manage personnel before granting system access.
10. **Physical Protection (PE) -**Limit physical access to systems and facilities.
11. **Risk Assessment (RA) -** Identify and prioritize cybersecurity risks.
12. **Security Assessment (CA) -** Periodically evaluate and verify control effectiveness.
13. **System & Communications Protection (SC) -** Protect network boundaries and communications.
14. **System & Information Integrity (SI) -**Detect, report, and correct system flaws and malicious activity.

NIST vs. CMMC

Aspect	NIST 800-171	CMMC 2.0
Purpose	Defines *what* security controls must exist	Defines *how* compliance is assessed
Orgin	Created by NIST	Managed by the DoD
Structure	110 requirements across 14 control families	3 maturity levels based on NIST controls
Assessment	Self-assessment (SPRS submission)	Third-party or DoD assessment
Focus	"Do this"	"Prove you've done it"

NIST = the standard. CMMC = the certification.

Organizations compliant with NIST 800-171 are already 80–90% of the way toward CMMC Level 2 readiness.

Implementing the Controls

For many contractors, implementing NIST SP 800-171 controls begins with activities such as:

- ✓ Identifying where **CUI resides**
- ✓ Defining the **CMMC enclave**
- ✓ Conducting a **gap assessment**
- ✓ Developing a **System Security Plan (SSP)**
- ✓ Tracking deficiencies through a **Plan of Action and Milestones (POA&M)**

Contractors must also report their compliance progress through the Supplier Performance Risk System (SPRS), where organizations submit a score reflecting how many of the 110 controls have been implemented.

However, implementing controls is only part of the challenge. CMMC requires organizations to demonstrate that these controls are actively operating and continuously monitored. This operational requirement is where many contractors encounter difficulty.

Security tools may be deployed, but without continuous monitoring, investigation, and response capabilities, organizations may struggle to demonstrate that their controls are functioning effectively.

BITLYFT HELPS DOD CONTRACTORS OPERATE CMMC SECURITY

Many organizations within the Defense Industrial Base do not maintain a dedicated Security Operations Center (SOC) capable of continuously monitoring and responding to threats within their CMMC enclave.

As a result, contractors often face several operational challenges:

- ✓ Limited visibility into security activity across systems handling CUI
- ✓ Alert fatigue from existing security tools
- ✓ Difficulty investigating security events
- ✓ Lack of 24/7 monitoring capability
- ✓ Resource constraints that prevent building an internal SOC

This is where External Security Providers (ESPs) play an important role in supporting CMMC security operations. BitLyft provides these capabilities through TRUE MDR, its managed detection and response service powered by the BitLyft AIR® security automation platform. True MDR enables organizations to operate continuous security monitoring, investigation, and response capabilities aligned with the operational security practices required to protect CUI.

How BitLyft Simplifies Compliance

At BitLyft, we transform compliance from a burden into a strength. Our True MDR platform is powered by BitLyft AIR®. Bringing automation, intelligence, and human expertise to streamline security operations and compliance maintenance.

Core Capabilities

1. **Security Information & Event Management (SIEM) -** AU, SC, SI: centralized log management and anomaly detection.
2. **Security Orchestration, Automation & Response (SOAR) –** IR, SI: automated incident response and remediation
3. **User & Entity Behavior Analytics (UEBA)–** AC, AU, IA: detects insider threats and unauthorized access.
4. **Central Threat Intelligence (CTI) –** RA, CA, SC: contextual threat awareness and proactive defense
5. **SOC Expertise –** AT, IR, SI: real-time human analysis and escalation.

With BitLyft, you gain:

- 24/7 monitoring and automated detection
- Integrated compliance reporting for NIST & CMMC
- Tier 3 SOC analysts as an extension of your team
- Simplified evidence collection for audits

BitLyft's Commitment to CMMC

BitLyft operates at a CMMC Level 2–equivalent security posture and is currently pursuing formal CMMC Level 2 certification, with certification expected to be completed in early 2026.

This commitment ensures that BitLyft's internal security practices align with the same standards required of organizations within the Defense Industrial Base.

By combining experienced security analysts, automation through the BitLyft AIR® platform, and deep experience supporting regulated industries, BitLyft helps contractors strengthen their security operations while working toward or maintaining CMMC compliance.

With TRUE MDR and the BitLyft AIR® platform, organizations gain the visibility, monitoring, and response capabilities needed to protect Controlled Unclassified Information and support long-term compliance with CMMC.

Want to learn how BitLyft can support your CMMC journey? Please contact us sales@bitlyft.com

GLOSSARY

CUI: Controlled Unclassified Information

DFARS: Defense Federal Acquisition Regulation Supplement

SSP: System Security Plan

POA&M: Plan of Action and Milestones

SPRS: Supplier Performance Risk System

CMMC: Cybersecurity Maturity Model Certification

SIEM: Security Information and Event Management

SOC: Security Operations Center

SOAR: Security Orchestration, Automation, and Response