Forcepoint

Solution Brief

Forcepoint Solutions to Meet CMMC Requirements

Challenge:

- **CMMC Compliance Complexity:** The CMMC framework, built on NIST 800-171 standards, poses significant challenges for Defense Industrial Base organizations due to the difficulty of continuously identifying and securing intellectual property like CUI data across the enterprise.
- **Supply Chain Security:** Protecting the DIB supply chain is crucial for national security, yet many organizations struggle to implement robust security measures.
- **Limited Visibility and Control:** Lack of visibility and control over data flow within complex environments hinders effective security posture.

Solutions:

- **Data Security Everywhere Approach:** Forcepoint offers a comprehensive suite of data security capabilities to help organizations enforce a strong data security posture
- **Award Winning Data-First Security:** Forcepoint is a recognized industry-leader in data security, dedicated to protecting sensitive information wherever it resides. Our solutions provide organizations with comprehensive visibility and control across all environments.
- **Federal Expertise:** With extensive experience working with the federal government, Forcepoint understands the unique challenges and requirements of CMMC compliance.

The Cybersecurity Maturity Model Certification (CMMC) is a key step in strengthening the U.S. Department of War (DoW) security and safeguarding Controlled Unclassified Information (CUI) within the Defense Industrial Base (DIB) supply chain. CMMC is set to drive one of the most significant industry shifts from non-compliant to compliant services.

Defense manufacturers and suppliers need appropriate controls for CUI data in place this year as third-party assessments of CMMC compliance become mandatory for all new contract awards in November of 2026. At Forcepoint we are committed to supporting this mission and making it easier for all organizations to prove that they are actively identifying and securing sensitive information continuously across the enterprise.

We understand the serious challenges confronting our government and strongly support the CMMC as a critical initiative for the DoW to enhance national security efforts. Mitigating the significant loss of CUI can be a complex challenge and failing to do so poses significant national security risks. This is why we are proud to offer solutions that make it easier for DIB organizations to meet and exceed these exacting standards. We are here to help shoulder the burden of identifying CUI, controlling access to CUI, and mitigating risks of exposed CUI data.

What is CMMC?

The CMMC program is aligned with the DoW's information security requirements for DIB partners. It is designed to ensure the protection of sensitive unclassified information shared by the Department with its contractors and subcontractors. This program gives the DoW greater assurance that its contractors and subcontractors are meeting the necessary cybersecurity standards for acquisition programs and systems that handle controlled unclassified information.

Based on the US Department of Commerce's National Institute of Standards and Technology (NIST) 800-171 standards, the CMMC advances the existing Defense Federal Acquisition Regulation Supplement (DFARS) regulations by adding a cybersecurity verification component.

Every business, regardless of size, that sells directly or indirectly to the DoW will need some level of CMMC compliance. The DoW's stated goal is for CMMC to be cost-effective and affordable for smaller businesses to implement at the lower CMMC levels.

Strengthening Defense Supply Chain Security

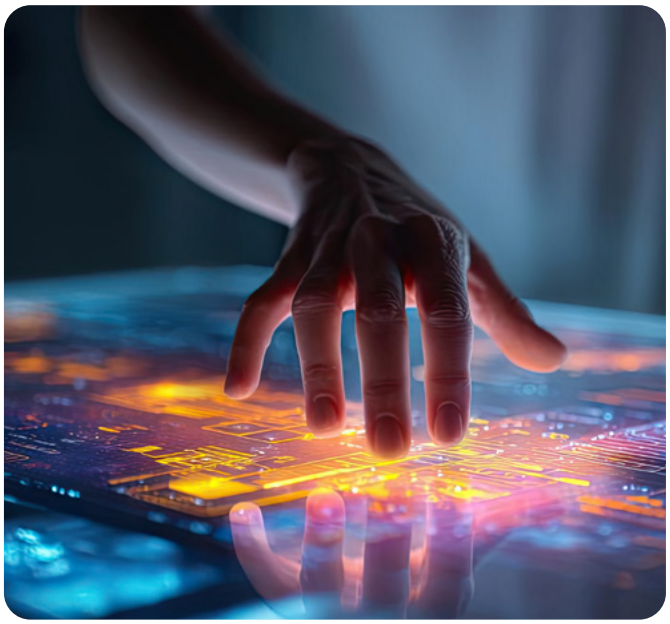
The CMMC is about strengthening and maturing cybersecurity policies and processes for all DIB members. Strengthening the security of the supply chain is a key requirement.

Supply chain attacks have proven a powerful way to gain access to a target to disrupt and degrade their capabilities. As such, it is critically important to strengthen the protection of the federal government supply chain, especially for DIB suppliers as their infrastructure, systems, and data are high-value targets for espionage, sabotage, and other malicious activity.

Establishing standardized security practices and robust third-party risk management is essential for safeguarding the DIB supply chain. The U.S. Congress has mandated supply chain best practices and recommended legislative or policy changes to encourage their adoption by the private sector. Forcepoint is committed to helping DIB members implement these practices, ensuring their supply chains are secure and compliant with CMMC.

NIST's cybersecurity frameworks continue to provide guidance and best practices, DIB members must continue to leverage NIST's guidance. The private sector DIB members must focus security policies and processes on end-to-end risk management; strong supplier management; hardware manufacturing and order fulfillment to allow for management of personnel, facility, and product security. The DIB members must have active security engagements in the public-private partnerships. Forcepoint's solutions align with these frameworks, helping organizations implement NIST's guidance and meet CMMC requirements.

For DIB organizations, meeting CMMC requirements is less about adopting more security tools and more about proving—credibly and continuously—that CUI is known, protected, and governed. Forcepoint's combination of Data Security Posture Management (DSPM), Data Detection and Response (DDR), and Data Loss Prevention (DLP) are particularly well suited to this challenge because they align precisely with how CMMC assessors evaluate risk: where CUI resides, who can access it, how it is used, and whether protections are effective over time.



Forcepoint DSPM establishes the foundation. One of the most common failure points in CMMC readiness is incomplete or inaccurate CUI inventories. CUI is often scattered across cloud storage, SaaS platforms, data lakes, file shares, and backups, which can extend well beyond traditional security perimeters. DSPM continuously discovers and classifies sensitive data, identifying where CUI exists, how sensitive it is, and how it is exposed. For CISOs and GRC leaders, this transforms CMMC scoping from a manual, interview-driven exercise into an evidence-based process. DSPM directly supports CMMC practices across Access Control, Risk Management, Asset Management, and Security Assessment by providing a continuously updated, auditor-defensible view of CUI risk.

Forcepoint DDR builds on this visibility by shifting security from static controls to active risk monitoring. CMMC requires not just that controls exist, but that organizations can demonstrate they are effective. DDR correlates data sensitivity with user behavior, access patterns, and anomalous activity to detect potential misuse, compromise, or insider risk involving CUI. This capability is especially valuable for meeting System and Information Integrity and Audit and Accountability expectations, as it provides contextual insight into how CUI is actually accessed and used. For GRC teams, DDR enables faster investigations, clearer narratives during assessments, and stronger evidence that data risks are actively managed, not discovered after the fact.

Forcepoint DLP delivers the enforcement layer required to operationalize CMMC policies. Once CUI is identified and risks are understood, organizations must prevent unauthorized disclosure, transfer, or exfiltration—across endpoints, networks, cloud services, and email. Forcepoint DLP enforces consistent, policy-driven protections regardless of where CUI moves, supporting key CMMC Access Control and CUI flow requirements. Importantly, DLP also generates detailed logs and reports that align directly with assessor expectations for proof of control effectiveness.

Together, DSPM, DDR, and DLP form a data-centric compliance architecture that resonates with both CISOs and GRC professionals. CISOs gain reduced breach and insider-risk exposure tied to CUI, while GRC leaders gain continuous evidence, clearer audit narratives, and lower compliance friction. Rather than treating CMMC as a periodic checkbox exercise, Forcepoint enables DIB organizations to demonstrate sustained, measurable protection of CUI—turning compliance from a disruptive event into an operational state of confidence.

Forcepoint does not simply help organizations meet CMMC controls; it helps them prove, defend, and maintain CUI protection in the way assessors and DoW stakeholders expect.

	CMMC INTENT	DSPM	DDR	DLP	OUTCOME
Access Control (AC)	Limit access to CUI to authorized users, systems, and processes; control CUI flow.	Identifies where CUI resides, who has access to it, highlights excessive permissions and over-exposure of data while providing an easy way to move files and change access permissions to help enforce the Principle of Least Privilege.	Transforms DSPM by moving from regular scans to continuous data monitoring for near real-time alerting as data is changed or put at risk and provides data lineage details.	Enforces policy-based controls to prevent unauthorized transmission, sharing, or exfiltration of CUI across endpoints, email, cloud, and network channels.	Organizations can demonstrate not just access policies, but **effective control over CUI access and movement.**
Risk Assessment (RA)	Identify, assess, and manage risks to CUI.	Assesses data risk based on sensitivity, exposure, access paths, and configuration weaknesses.	Elevates risk assessment by continuously monitoring changes to access and changes to the data for near real-time alerting of changes in risk and provides data lineage visibility.	Facilitates risk assessments with detailed forensic reports on sensitive data movements that violate policy.	Risk assessments move from periodic, manual exercises to **continuous, data-driven risk management.**
System and Information Integrity (SI)	Protect systems and data from flaws, misuse, and malicious activity.	Identifies insecure storage configurations, stale data, and unprotected CUI that increase integrity risk.	Detects anomalous access, unusual data interactions, and potential insider or compromised-account activity involving CUI.	Prevents integrity-impacting actions such as unauthorized copying, uploading, or transmission of sensitive data.	Integrity controls are validated at the data level, where CMMC impact is highest.
Audit and Accountability (AU)	Log, review, and retain evidence of actions affecting CUI.	Provides historical and current evidence of where CUI exists and how	Produces contextual activity records tied directly to sensitive data interactions.	Generates detailed forensic logs demonstrating policy effectiveness.	GRC teams gain **audit-ready evidence** without manual log stitching or narrative gaps.
Security Assessment (CA)	Periodically assess and continuously monitor control effectiveness.	Assesses whether CUI is properly identified and protected.	Continuously validates whether controls are effective under real-world usage conditions.	Demonstrates ongoing enforcement aligned to documented policies.	CMMC assessments shift from point-in-time snapshots to **continuous compliance readiness.**
Media Protection (MP)	Control and protect CUI on digital media throughout its lifecycle.	Identifies where CUI is stored and highlights unmanaged or high-risk data locations requiring media controls.	Detects anomalous access, download, or staging behaviors that indicate improper media handling.	Enforces policy controls on CUI copied to removable media, local storage, or external destinations.	Organizations can demonstrate **controlled handling of CUI on media**, with preventive enforcement and evidence that policies are consistently applied—reducing a common CMMC audit exposure area.
System and Communications Protection (SC)	Protect and control communications that transmit CUI.	Establishes data context by identifying CUI subject to communications protection.	Flags anomalous or high-risk communication patterns involving CUI.	Enforces content-aware controls on CUI in motion across email, web, cloud, and network channels.	Communications involving CUI are **continuously monitored, controlled, and auditable**, enabling organizations to prove that CUI is protected in transit

Forcepoint

Forcepoint.com/contact

[FP-CMMC-Solution Brief-EN] 09Feb2026