CASE STUDY

CMMC Readiness · Defense Industrial Base

InterSec
Ignite . Inspire . Innovate

Closing the CMMC Level 2 Gap for a Manufacturer with Legacy IT and Cloud Hesitancy

A Virginia manufacturer with minimal IT staff, aging infrastructure, and reservations about the cloud risked losing DoD contracts under DFARS 7012. InterSec's phased NIST 800-171 approach closed the gaps and reached CMMC Level 2 in nine months.

CLIENT	PROFILE	STATUS
A Virginia-based defense manufacturer	Minimal cybersecurity staff, aging infrastructure, cloud-hesitant	Completed

9
Months to CMMC Level 2

110
NIST 800-171 controls met

14
Control families addressed

3
Quick wins: MFA, encryption, VPN

DRIVER	ENVIRONMENT	APPROACH	ENABLEMENT
DFARS 7012, CMMC Level 2	On-premise plus partial cloud	Phased, quick-wins first	Hands-on staff training

THE CHALLENGE

The firm had to comply with DFARS 7012 while working around aging IT and genuine skepticism about the cloud, with DoD contracts at stake. The obstacles were as much about resources and culture as technology: no dedicated cybersecurity oversight, no clear way to manage and protect CUI, and a deadline that, if missed, meant significant revenue loss. The company needed a path scaled to its capacity.

THE APPROACH

InterSec secured executive backing first, then deployed a field-tested readiness framework so the organization aligned top-down. Bringing leadership in early cleared the cloud-hesitancy roadblock by making the security investment and governance responsibilities explicit. A gap analysis fed a prioritized roadmap that led with practical quick wins, MFA, encryption, and secure VPNs, so the company saw early progress on its highest-risk exposures.

> **Aging infrastructure didn't need to be replaced to be made compliant, only understood.**

THE SOLUTION IN PRACTICE

The team scoped CUI first, identifying where sensitive data lived across on-premise systems and the partial cloud footprint. InterSec then overhauled policies and procedures, establishing the asset management, vulnerability scanning, and encryption practices the company had lacked. Because a program is only as strong as its people, the work included hands-on staff training so employees understood the new processes rather than working around them.

RESULTS & IMPACT

- ✓ CMMC Level 2 requirements were met within nine months.
- ✓ Employees adopted the new processes, making the program sustainable rather than a one-time push.
- ✓ Quick fixes to high-risk areas reduced the most pressing threats early.
- ✓ DoD contracts were protected with a foundation for ongoing risk management.

KEY TAKEAWAYS

Executive backing clears cultural roadblocks.
Cloud hesitancy is rarely solved by technical argument alone. Leadership alignment on investment and governance moves it.

Lead with quick wins.
MFA, encryption, and secure VPNs reduce real risk fast and build momentum for the longer program.

Scope CUI before protecting it.
Knowing where sensitive data actually lives keeps the effort focused and the budget realistic.

Train the people, not just the systems.
Employee adoption is the difference between a program that lasts and one that lapses after the deadline.

CAPABILITIES DEMONSTRATED

CMMC Level 2 Roadmap · CUI Scoping and Protection · Legacy IT Modernization · Secure Cloud Adoption · Staff Training and Awareness

Limited IT staff and aging systems are the norm, not a disqualifier.
InterSec prepares defense manufacturers for assessment with a roadmap scaled to their resources.

Let's talk →