CASE STUDY

CMMC Readiness · Defense Industrial Base

InterSec
Ignite . Inspire . Innovate

When the MSP Is the Risk: CMMC Level 2 for a Specialty Metals Supplier

A specialty alloys supplier had a mature quality culture but no cybersecurity program, and an MSP that could not produce CMMC evidence. InterSec turned a mid-engagement MSP change into a compliance gain and built a clean four-user CUI environment.

CLIENT	PROFILE	STATUS
A specialty metals and alloys supplier to defense and aerospace	AS9100D and ISO 9001 certified, four facilities across two states	In progress

4
CUI users on a dedicated, isolated VLAN

~50
Prioritized evidence items, down from 200+

110
NIST SP 800-171 Rev 2 controls in scope

50+
Years supplying defense and aerospace

STANDARD	ENVIRONMENT	CUI FOOTPRINT	CADENCE
CMMC Level 2, NIST 800-171 R2	VLAN-segmented with GCC	4 workstations, separate printer	Biweekly, GRC-tracked

THE CHALLENGE

A specialty alloys supplier with a mature AS9100D quality culture had no cybersecurity program and an MSP that could not produce CMMC evidence. Two months in, a fork appeared: switch providers mid-engagement and absorb transition risk, or build the program on a foundation that might not hold up under an assessor's questions.

THE APPROACH

InterSec structured the work around three priorities: resolve the MSP dependency first, design the CUI architecture deliberately, and build artifacts in parallel rather than in sequence. A mid-engagement transition is preferable to a post-certification reassessment triggered by MSP control failures.

> **The provider you inherit can quietly become the control that fails your assessment.**

THE SOLUTION IN PRACTICE

A CMMC-capable provider was selected and integrated into the biweekly cadence on day one, arriving with usable EDR, managed-firewall, and SIEM evidence. The team then designed a minimal CUI environment: four workstations on their own VLAN, a separate CUI printer, USB blocking via EDR, and a GCC environment for CUI email and storage. Existing quality processes were mapped directly to CMMC controls.

RESULTS & IMPACT

- ✓ MSP transition complete, with change management, SIEM, EDR, and incident response all producing compliance-ready evidence.
- ✓ Four-user, VLAN-isolated CUI environment defined, with GCC confirmed for segregation.
- ✓ Quality-management processes mapped to CMMC controls, reducing duplicated documentation.
- ✓ Clear responsibility matrix now spans client, MSP, and PM partner, ready for an assessor.

KEY TAKEAWAYS

MSP selection is a compliance decision.
Vet CMMC readiness before signing; the provider's ability to produce evidence matters as much as its technical capability.

A mature quality framework accelerates CMMC.
Documented processes and audit familiarity transfer directly to policy. The job becomes mapping, not building from zero.

A small CUI footprint is a strategic advantage.
Scoping access to exactly the users who need it shrinks the assessment surface and makes the program more defensible.

Evidence rationalization is a morale multiplier.
A 200-item list paralyzes a team. A prioritized, visible subset keeps it moving.

CAPABILITIES DEMONSTRATED

CMMC Level 2 Readiness · MSP Capability Assessment · CUI Architecture Design · Policy and Evidence Development · Quality-Framework Mapping

Is your compliance program only as strong as an unvetted MSP?
InterSec prepares manufacturers for CMMC assessment and makes sure the foundation underneath holds.

Let's talk →