CASE STUDY

CMMC Readiness · Defense Industrial Base

InterSec
Ignite . Inspire . Innovate

Unifying Two Companies Under One CMMC Level 2 Program After an Acquisition

A 200-person defense contractor that had just acquired a manufacturer needed to bring two separate IT environments under one CMMC Level 2 program before DoD deadlines hit. InterSec unified identity, policy, and controls across both, reaching an SPRS score of 110.

CLIENT	PROFILE	STATUS
A Virginia-based acquisition-support contractor	200+ employees, recently acquired a smaller manufacturer	Completed

110
SPRS score achieved

200+
Employees across the combined org

2
Companies unified into one program

1
Active Directory and policy baseline

STANDARD	SITUATION	SEQUENCE	METHOD
CMMC Level 2, NIST 800-171	Post-acquisition, two IT environments	Identity first, then controls	Phased, risk-based integration

THE CHALLENGE

After the acquisition, two organizations had to operate under one CMMC-compliant framework, with looming DoD deadlines and no margin for error. An acquisition doubles the policy and attack surface on the same day. The acquired employees were not in the parent's Active Directory, legacy security policies varied with no common baseline, and the timeline demanded swift alignment of controls.

THE APPROACH

InterSec ran a phased, risk-based integration rather than a single disruptive cutover. Pre-built CMMC templates and methodical remediation phases closed the most urgent gaps first while steadily folding in the rest. The sequencing decision mattered most: identity came first, because access control cannot be enforced across systems that have not been unified, and almost every other control depends on it.

> **Two compliant companies do not automatically add up to one compliant company.**

THE SOLUTION IN PRACTICE

The work began with a current-state analysis of tools, processes, and vulnerabilities across both entities. The team then executed the remediation plan, deploying MFA, configuring vulnerability scanning, and unifying documentation into one coherent set. The integration centered on identity: acquired staff were transitioned into the parent's Active Directory, with password policies and access controls aligned across the combined workforce.

RESULTS & IMPACT

- ✓ Both entities now operate under one compliant framework, reaching an SPRS score of 110.
- ✓ Integrated identity and access reduced the confusion and risk of two separate environments.
- ✓ Critical DoD deadlines were met without disrupting active project work.
- ✓ Contract renewals were protected through on-time alignment.

KEY TAKEAWAYS

An acquisition doubles the compliance surface overnight.
Treat post-merger integration as a security project, not just an IT migration.

Start with identity.
You cannot enforce access control across systems you have not unified, and most other controls depend on it.

Phase remediation against the deadline.
Closing the highest-risk gaps first protects contract eligibility while the rest follows.

Reconcile policy, do not staple two sets together.
One coherent baseline is what an assessor expects to see.

CAPABILITIES DEMONSTRATED

CMMC Level 2 Readiness · Post-Acquisition Security Integration · Identity and Access Unification · Policy Reconciliation · Phased Remediation

A merger is one of the riskiest moments for a compliance program.
InterSec unifies security across newly combined organizations and prepares them for CMMC assessment.

Let's talk →