CASE STUDY

CMMC Readiness · Defense Industrial Base

InterSec
Ignite . Inspire . Innovate

Right-Sizing CMMC Level 2 for a Small Navy Industrial-Services Contractor

A small shipyard-services contractor with no IT staff faced a CMMC Level 2 requirement written into an active Navy contract. InterSec built a lean, defensible self-assessment program a two-person team could run and keep running.

CLIENT	PROFILE	STATUS
A small Navy industrial-services contractor	Calibration, fabrication, and machine work; skilled trades, no IT staff	In progress

100+
Target SPRS score

2
Dedicated CUI laptops

<10
Devices in the CUI scope

0
Dedicated IT or security staff

STANDARD	FOOTPRINT	MODEL	MONITORING
CMMC Level 2, self-assessment	2 laptops, segregated Wi-Fi	Milestone-based, tied to SPRS	Documented manual log review

THE CHALLENGE

A Navy contract surfaced with an explicit CMMC Level 2 requirement. The company had no prior cybersecurity program, no IT staff, and a tight budget. The hard part was organizational: how to build a credible, auditor-ready program for a two-person client-side team running a hands-on industrial business, without a compliance burden that swamps daily operations.

THE APPROACH

InterSec, a Cyber AB Registered Practitioner Organization, structured the work around three principles: keep it lean, make it milestone-driven, build for sustainability. The self-assessment path was the right call, since the contract allowed an SPRS submission rather than a formal audit. Milestone-based payments, tied to SPRS scores of 70 and then 100, aligned accountability directly with compliance outcomes.

> **The right program for a five-person shop is the smallest one that still passes.**

THE SOLUTION IN PRACTICE

The infrastructure reflected the reality of a lean team: two encrypted, locked-down laptops for CUI work; a small-office firewall with documented rules and segregated Wi-Fi; free and low-cost vulnerability scanning taught hands-on; a GCC subdomain for CUI email; and documented manual log review instead of an expensive SIEM. The client owned policy drafting, while the SSP and POA&M were tracked in a GRC platform, and live sessions walked the IT lead through scanning and firewall setup.

RESULTS & IMPACT

- ✓ A lean CUI architecture is built and documented.
- ✓ The full policy suite is near complete, with the SSP and POA&M tracked in the GRC platform.
- ✓ The milestone model kept the client responsive to measurable progress.
- ✓ Hands-on enablement means the client can sustain its own program.

KEY TAKEAWAYS

Right-sizing the path is strategy, not a shortcut.
A full third-party audit would have been disproportionate in cost and likely to fail first time. Steering a client to the right path is part of the job.

Milestone pricing changes client behavior.
When the next payment depends on measurable progress, data calls get answered and artifacts get uploaded.

Lean teams need hands-on enablement.
For a company without IT staff, a single live working session is the difference between stalled and progressing.

Fold compliance into infrastructure changes.
A network upgrade documented as it happens produces better evidence than retroactive notes.

CAPABILITIES DEMONSTRATED

CMMC Level 2 Readiness · CUI Scoping · Self-Assessment and SPRS · Policy and Evidence Development · Technical Enablement

A small team and a tight budget are not reasons to over-build a program.
InterSec prepares defense contractors for CMMC assessment scaled to how they actually operate.

Let's talk →