

Validating and Rebuilding a Legacy CMMC Program for a Navy Ship-Preservation Subcontractor

A ship-preservation subcontractor under new ownership inherited a five-year-old compliance baseline and a pending platform decision. InterSec validated the legacy program, ran a structured CUI-tool evaluation, and rebuilt on a clean cloud foundation.

<p>CLIENT A Navy ship-preservation subcontractor</p>	<p>PROFILE Industrial coatings for Navy primes, in business since the late 1980s</p>	<p>STATUS ● In progress</p>
---	---	--

<p>60 → 110 SPRS baseline to target</p>	<p>4 Dedicated CUI workstations</p>	<p>35+ Years serving the Navy</p>	<p>6 Platform factors compared</p>
--	--	--	---

<p>STANDARD CMMC Level 2, self-assessment</p>	<p>ARCHITECTURE 4 workstations on isolated VLAN</p>	<p>PLATFORM FedRAMP-authorized cloud CUI</p>	<p>EMAIL Migrating off legacy on-premise</p>
--	--	---	---

— THE CHALLENGE

The company entered with a prior baseline, an SPRS score of roughly 60 from a 2020 audit, but under new ownership that inherited the program without full knowledge of how it was built. Partial documentation, changed leadership, and an on-premise email server predating modern CUI handling created a specific problem. And a fundamental decision, which CUI platform to build on, was still open, blocking the policy and technical work.

— THE APPROACH

The first principle was validation before acceleration: InterSec treated the 2020 documentation as a draft requiring review, not a foundation ready to extend. The second was to give the technology decision its own phase, holding the policy and technical tracks until the platform question was settled, accepting a short delay in exchange for a clean execution phase with no rework.

Inherited compliance documentation is a draft to be validated, never a finish line to be trusted.

— THE SOLUTION IN PRACTICE

The platform decision came out of a structured evaluation of two cloud CUI options, judged on FedRAMP status, audit readiness, shared responsibility, M365 integration, cost at four-user scope, and CMMC track record. Keeping CUI in the cloud simplified the compliance boundary, so the legacy email server was flagged for migration. Four CUI workstations sit isolated on a separate VLAN, with firewall-managed VPN and cloud CUI management, and the MSP was engaged against a documented question set.

— RESULTS & IMPACT

- ✓ The CUI platform is selected after a structured evaluation and is piloting with six users.
- ✓ The 2020 baseline has been reviewed and updated, with the SSP and POA&M refreshed.
- ✓ A four-workstation, VLAN-isolated architecture is defined, with firewall-managed VPN logging.
- ✓ MSP responsibilities are documented, covering logging, patching, and remote access.

— KEY TAKEAWAYS

Inheriting a legacy program requires validation before acceleration.

New owners who did not build a program cannot vouch for it. Validate what exists before building on it.

Simplifying the boundary reduces assessor risk.

Moving CUI to the cloud and retiring legacy on-premise systems shrinks the assessment surface.

Technology selection deserves its own phase.

Building a policy and technical program before the platform is chosen invites rework. Resolve it first.

MSP documentation must be proactive.

Defining shared responsibility before an assessor asks is a common, avoidable failure mode.

CAPABILITIES DEMONSTRATED

CMMC Level 2 Readiness

Legacy Baseline Validation

CUI Platform Evaluation

CUI Architecture Design

MSP Responsibility Mapping

An inherited program and an open platform decision are where wrong assumptions get expensive.

InterSec validates what you already have and rebuilds on a foundation that will hold.

Let's talk →