PEI CMMC Readiness & Two-Server Compliance Proposal

Pacific Engineering Inc. (PEI) CMMC 2.0 Readiness & Two-Site Infrastructure Proposal

Prepared by: Xavione Gordon Sr. & Faizon [Last Name]

Date: October 2025

Why We're Having This Conversation

The Original Plan

"We were tasked with standing up two servers – one in Omaha, one in Roca"

The Critical Discovery

"but we discovered something critical: **Before we can connect anything, PEI must build it under federal cybersecurity compliance (CMMC 2.0).**"

CMMC reality: 110 controls, DoD compliance, audit readiness.

The Rule That Changes Everything

CMMC 2.0 Regulation

32 CFR / DFARS 48 CFR: DoD's mandatory cybersecurity certification.

Effective Dates

32 CFR Final Rule: Dec 16, 2024

48 CFR Acquisition Rule: Effective Nov 10, 2025

Impact on PEI

PEI must prove compliance to maintain or renew DoD contracts.

Verification: Through SPRS (Supplier Performance Risk System).

"No compliance = no contract renewals after 2026."

What SPRS Is (Simplified)

Think of SPRS as PEI's "Cybersecurity Report Card."

01

Complete a CMMC Self-Assessment

110 controls must be evaluated and documented.

02

Upload Score and System Security Plan (SSP)

Submit our compliance documentation to the SPRS system.

03

CEO Affirmation

Have Dexter Myers (CEO) sign an affirmation.

> If we're not in SPRS: DoD sees "0" – PEI becomes ineligible for contract awards.

The Two-Server Reality

Mirrored Configuration

Both servers will mirror each other.

Secure Enclave Operation

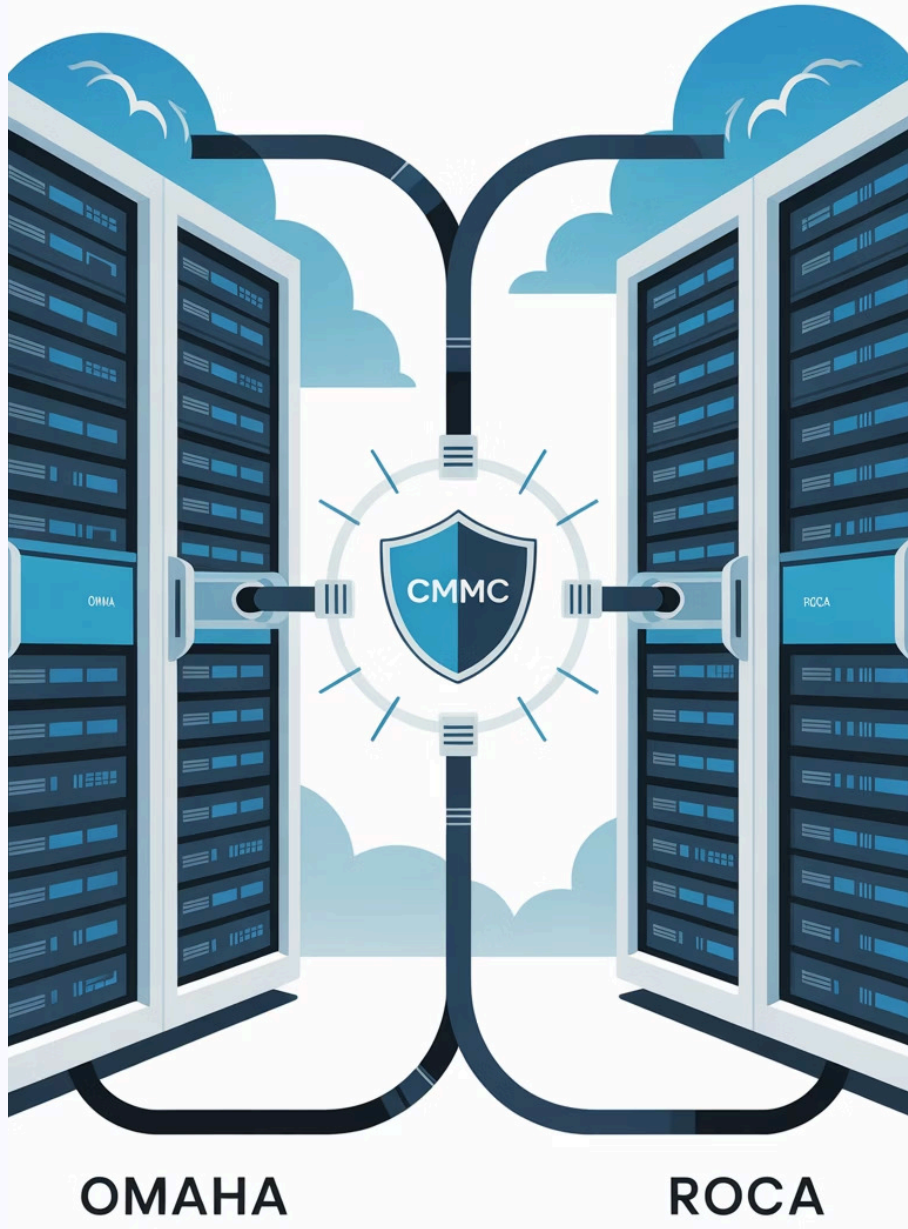
Both will operate inside a secure, auditable enclave:

- MFA-protected VPN connection between sites.
- Centralized Active Directory domain.
- Encrypted traffic & backups.
- Logging, monitoring, and evidence retention.

NIST 800-171 Controls

Every configuration must satisfy NIST 800-171 controls.

"They can talk to each other – but only through a CMMC-compliant framework."



Why We Can't 'Just Plug Them In'

Building Fast

- Basic Windows setup
- Shared logins
- No audit trail
- Unknown risk

Building Compliant

- Hardened domain-controlled systems
- MFA & Role-based Access
- Continuous logging & reporting
- Certified compliance & contract protection

"If we build the servers wrong now, we'll have to rebuild them later – and risk failing a federal audit."

Our Roadmap (Oct 2025 – Sep 2026)

✅ Ready before Oct 2026 renewal

Hardware & Tools (Meeting CMMC Requirements)

Core Equipment (Duplicated for Both Sites):

Servers

(2) Dell PowerEdge R520 or R360 servers (Proxmox virtualization)

Backup Systems

(2) UPS + NAS backup systems

Network Security

(2) UniFi Dream Machine SEs (firewall/VPN)

Managed switches (L2+ VLAN support)

Security Tools

Endpoint protection (Defender, Sysmon, Wazuh SIEM)

Secure remote backup + audit logging

> "Each site will mirror the other – identical builds for redundancy and compliance."

Internal CCP Training vs Outsourcing

Category	Without CCP (Consultants)	With CCP (In-House)
Gap Assessment	$10k - $25k	$0 - $5k
Documentation	$3k - $10k	$0 - $2k
Remediation	$10k - $30k	$0 - $5k
C3PAO Audit	$15k - $25k	$15k - $25k
Total Cost	**$60k-$100k+**	**$20k-$35k**

$7K

Investment in CCPs

Total for training & certification (Xavione + Faizon)

$40K-$70K

Savings

Per compliance cycle

Budget Scenarios

Cost Category	Without CCP	With CCP
Hardware (servers, network, UPS)	$15k - $20k	$15k - $20k
CCP Training (Xavione + Faizon)	–	$7k
Software/Tools	$5k	$5k
External C3PAO Audit	$15k - $25k	$15k - $25k
Total Project Cost	**$60k-$80k**	**$40k-$55k**

Risk vs Reward

If We Ignore CMMC

- Fast now, fail later
- 0 in SPRS (disqualified)
- Hardware wasted
- No documentation

If We Build for Compliance

- Pass audit, stay contract-eligible
- SPRS score uploaded, renewal secure
- Long-term compliant infrastructure
- Fully auditable, repeatable system

The Ask

Approve CCP Training

$7,000 for Xavione & Faizon

Approve Hardware & Tools Budget

$15,000 - $20,000

Authorize CMMC-Aligned Build Plan

Oct 2025 - Sep 2026

"We'll still build the Omaha ↔️ Roca setup — but we'll do it the right way — compliant, secure, and audit-ready."

Closing

"CMMC is the gatekeeper to every DoD contract."

If we build PEI's servers without compliance, we'll lose eligibility before we even connect them.

If we do it right – we protect every future contract and bring compliance expertise in-house.