Patriot Command Operations System (PCOS)

"Fortiter et Fideliter"

A living testbed for secure configuration, continuous monitoring, and automation — engineered to elevate my ability to protect information, sustain operations, and support the mission of the DoD cyber landscape

Concept of Operations (CONOPS)

8 Dec 2025

Authored By	Reece Niemuth
System Identifier	PCOS-Homelab
Date of Latest Revision	7 Dec 2025
Publication Version	Revision 1 (1.0.0)

CONTAINS NO CLASSIFIED OR SENSITIVE INFORMATION. THIS ARTIFACT SERVES TO DOCUMENT, IN PROFESSIONAL MANNER, A TRAINING RESOURCE FOR SELF-EDUCATION IN THE FIELD OF FEDERAL SYSTEMS ENGINEERING, MAINTENANCE, CYBERSECURITY RESEARCH, AND RELATED.

Concept of Operations (CONOPS) : Revision History

Revision / Version	Date	Description / Notes
Rev. 1 (1.0.0)	7 Dec 2025	Publication Inception / Creation

1. Preface of PCOS Concept of Operations

The Patriot Command Operations System (PCOS) is a mission-focused, home-lab operational ecosystem engineered to replicate realistic security engineering, ISSO workflows, monitoring, vulnerability management, and enterprise-grade defensive cyber operations. The PCOS environment is composed of integrated compute nodes, a domain controller, virtualization platforms, a centralized SIEM (Splunk), a vulnerability management server (Nessus), a NAS for resilient storage, a firewall (pfSense), centralized networking infrastructure, and a Raspberry Pi running Grafana/Prometheus for telemetry.

PCOS was designed to:

- Enable hands-on simulation of DoD-style secure system operations
- Model typical JSIG/RMF workflows
- Support end-to-end cybersecurity engineering experimentation
- Provide a training environment analogous to a small-scale SAP network
- Enable rapid prototyping of automation tools and security baselines

This CONOPS describes how PCOS operates, the roles within the environment, the major components, the guiding principles, and the operational flow used to monitor, protect, and sustain the home lab environment.

2. Introduction

2.1 Purpose

The purpose of this Concept of Operations (CONOPS) is to describe how PCOS is used, maintained, monitored, defended, and evolved. It provides both:

- **An executive/administrative view** of how the environment supports cybersecurity readiness, training, and research
- **A technical/operational view** of how each component functions, interoperates, and supports defensive cyber operations

PCOS acts as an operational proving ground for ISSO, ISSE, and cybersecurity engineering functions, supporting tasks such as:

- Vulnerability identification and remediation
- Security baselining (SCAP/STIG)
- Log aggregation and SIEM analytics
- Endpoint and server hardening

- Network security monitoring
- STIG/SCAP workflows
- Domain, identity, and access control management
- Incident simulation and response

2.2 System Overview

PCOS is an integrated environment composed of:

- **AREA51** – pfSense Firewall
- **USLINK** – Network Switch (Managed; PoE)
- **COMMAND** – Windows Domain Controller
- **UNION** – Splunk + Nessus server
- **STAR1–X / EAGLE1–X** – Windows/Linux hypervisors for VM workloads
- **LIBERTY** – NAS providing storage, snapshots, and data resilience
- **DRONE** – Raspberry Pi running Prometheus/Grafana for metrics and alerting

The system replicates a small-scale secured enclave, providing realistic operational context and supporting defensive cyber workflows from endpoint to SIEM.

2.3 CONOPS Structure (Ends, Ways, Means)

- **Ends:** A functioning, resilient, and monitored cyber operations environment to train, experiment, and demonstrate security engineering expertise.
- **Means:** PCOS hardware components, software baselines, network architecture, SIEM/Vuln tools, monitoring agents, and user workflows.
- **Ways:** Using standardized processes, ICS-like command coordination, automated telemetry, centralized logging, and orchestrated security operations.

3. Operational Assumptions

- The operator (you) functions as **Commander, ISSO, ISSE, and System Administrator simultaneously**.
- All PCOS components remain online unless under maintenance.

- Security controls (e.g., firewall rules, AD policies, STIG configurations) must be manually engineered and applied.
- Monitoring, alerting, scanning, and log aggregation occur continuously.
- The environment is intentionally designed for iterative experimentation, misconfiguration testing, and automation development.

4. PCOS Design and CONOPS Enabling Elements

The PCOS design is influenced by modern cybersecurity CONOPS principles, including:

4.1 Shared Collaborative Environment

Though operated by a single user, PCOS is built to behave like a multi-stakeholder cyber operations center. Splunk dashboards, Nessus results, Windows Event Logs, AD data, and NAS snapshots collectively form a real-time situational awareness picture.

4.2 Ubiquitous Access and Remote Manageability

All nodes are reachable via:

- RDP / RealNVC Connect
- SSH
- Splunk Web
- pfSense WebUI
- NAS WebUI
- Grafana WebUI

Remote access allows management from any workstation inside the PCOS network.

4.3 Asset Identification & Geolocation Analogue

PCOS uses:

- Static IP assignments
- Hostname conventions
- Centralized AD domain identity

…as proxies for “location services” in incident command analogies.

4.4 User-Created Visualizations

Splunk dashboards, Nessus results, Grafana charts, and AD topology diagrams provide layered situational awareness.

4.5 Multi-Modal Communication / Interaction

PCOS supports:

- **Speech analogue:** Administrative alerting, Windows event notifications
- **Gesture:** Visual dashboards, tagging indicators, topology diagrams
- **Sketch:** Draw.io diagrams for architecture and workflows

4.6 Technology Neutral & Open Architecture

PCOS uses:

- Windows
- Linux
- pfSense (FreeBSD)
- NAS OS
- Raspberry Pi OS (Debian-based)

…ensuring cross-platform interoperability.

4.7 No Application Lock-In

All primary control is via browser-based tools—Splunk, Nessus, Grafana, pfSense, NAS UI—mirroring NICS's "no install required" philosophy.

4.8 Incidents and Rooms Analogue

Although PCOS is not an emergency response system, the equivalent concepts exist:

- **Incidents:** Security events, vulnerabilities, outages, misconfigurations
- **Rooms:** Splunk dashboards, Nessus scan spaces, Grafana panels, AD consoles

These isolated workspaces allow focused investigation and coordination.

4.9 Full Historical Logging

Splunk indexes:

- Windows Security Logs
- Syslogs from pfSense
- NAS logs
- Sysmon (optional)

- Pi monitoring metrics

…providing forensic replay akin to NICS's archived operational history.

4.10 Designed for the "Tired-Dirty-Hungry Operator"

PCOS tooling is designed to be simple, clean, and quickly actionable, allowing rapid triage and decision-making under pressure (under obvious simulation conditions).

5. PCOS Roles and Responsibilities

Even though operated by one person, PCOS simulates real-world cybersecurity roles

Role	Responsibilities
Commander (Self-Designation)	Strategic direction, system integrity, recovery planning
ISSO	Auditing, documentation, risk management, compliance, secure configs
ISSE	System engineering, architecture, STIG validation, technical controls
Network Admin	VLANs, routing, firewall rules, switch management
SysAdmin	Patching, hardening, identity management, VM lifecycle
SOC Analyst	Splunk monitoring, detection, threat analysis
Incident Responder	Triage, containment, eradication, recovery

6. System Components and Operations

6.1 AREA51 – Firewall

- Manages network segmentation, NAT, VPN, IDS/IPS (optional), routing
- Logs forwarded to Splunk
- Single point of perimeter enforcement

6.2 USLINK – Switch

- Centralized network interconnect
- Connects all PCOS assets for Layer 2 communication
- Supports consistent IP allocations

6.3 COMMAND – Domain Controller

- AD DS, DNS, Group Policy
- Authentication backbone
- STIG-style hardening test environment

6.4 UNION – Splunk + Nessus

- SIEM ingestion, dashboards, analytics
- Vulnerability management lifecycle
- Serves as the "intelligence fusion node"

6.5 STAR / EAGLE Hypervisors

- Host Windows/Linux workloads
- VM testbeds for misconfiguration simulation, STIG testing, automation development

6.6 LIBERTY – NAS

- Centralized storage, caching, snapshots
- SMB access
- Hosts backups and Splunk/Nessus file exports

6.7 DRONE – Monitoring Node

- Runs Prometheus & Grafana
- Collects metrics from: Pi, hypervisors, NAS (if configured), network throughput
- Early-warning behavioral telemetry

7. Operational Workflows

7.1 Routine Operations

1. Systems remain online 24/7
2. Telemetry continuously flows to Splunk & Grafana
3. Nessus scans run on schedule or on-demand
4. AD authentication is used by all Windows systems
5. Logs are forwarded to UNION for correlation
6. Snapshots/backups occur on LIBERTY

7.2 Security Monitoring Flow

1. Host logs → Splunk
2. Network events → pfSense → Splunk
3. NAS logs → Splunk (optional)

4. Behavioral telemetry → Grafana
5. Analyst (you) triages alerts

7.3 Incident Workflow

1. Detection via Splunk or Grafana
2. Classification and scope identification
3. Containment via firewall rules or system isolation
4. Forensic review in Splunk
5. Patch / remediate
6. Add lessons learned to baselines

8. Executive/Administrator Perspective

From a high-level perspective, PCOS provides:

- Instant visibility into system health, vulnerabilities, and security posture
- A unified view of endpoints, servers, network devices, and storage
- Consistent operational insight without needing physical interaction
- A realistic testbed for designing security engineering automation tools (e.g., Sentinel Auditmation)

Executives (in this case, you acting in that role) can see:

- Security posture in real time
- Trends in system behavior
- Operational workload capacity
- Effects of new controls or configurations immediately

9. Technical/Operational Perspective

From the operator's viewpoint:

- Alerts, logs, and metrics are available instantly
- AD, firewall, and SIEM workflows are identical to enterprise operations
- System misconfigurations can be safely tested

- Control implementations can be validated (STIG-style)
- Incident response steps can be rehearsed end-to-end

PCOS gives the operator complete hands-on access to the entire system stack from network to application.

10. Conclusion

The Patriot Command Operations System (PCOS) Home Lab is a fully functional, realistic cyber operations environment designed to:

- Train high-end cybersecurity engineering skills
- Simulate enterprise-level ISSO/ISSE workflows
- Support continuous experimentation and optimization
- Provide an end-to-end monitored, secure, and resilient infrastructure
- Enable research into automation, analytics, compliance, and defensive cyber operations

This CONOPS serves as the foundation for how PCOS is used, managed, expanded, and matured.