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

Security Concept of Operations (SEC-CONOPS)

8 Dec 2025

A documented, repeatable process for identifying, analyzing, and prioritizing risks affecting the PCOS environment in accordance with NIST SP 800-30 Rev. 1.

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.

Security Concept of Operations (SEC-CONOPS) : Revision History

Revision / Version	Date	Description / Notes
Rev. 1 (1.0.0)	8 Dec 2025	Publication Inception / Creation

1. Purpose and Scope

The **PCOS Security Concept of Operations (SEC-CONOPS)** describes how security is planned, implemented, monitored, and continuously improved within the **Patriot Command Operations System (PCOS) Home Lab**.

It supplements the primary PCOS CONOPS by focusing specifically on:

- Security **objectives** and **assurance goals**
- **Threat model** and security assumptions
- **Security architecture**, control concepts, and operational guardrails
- **Monitoring, detection, vulnerability management, and incident handling**
- **Configuration management and hardening** practices for lab realism

Scope:
This SEC-CONOPS applies to all PCOS components described in the main CONOPS (AREA51, USLINK, COMMAND, UNION, STAR/EAGLE, LIBERTY, DRONE) and any virtual machines or services connected to the PCOS network.

2. Security Objectives

The PCOS Home Lab is intentionally engineered to mirror the mindset and rigor of a classified or SAP-like enclave **without** handling real classified or mission data. Security objectives are:

1. **Confidentiality (Simulated)**
   - Protect credentials, lab configurations, and synthetic data from unauthorized access.
   - Enforce role-appropriate access patterns (ISSO, ISSE, SysAdmin, SOC Analyst) even though all roles are executed by a single operator.
2. **Integrity**
   - Maintain trustworthy configurations for firewall rules, Group Policy, SIEM content, and vulnerability scan baselines.
   - Detect and assess unauthorized or unintended changes to systems, logs, and configurations.
3. **Availability**
   - Keep core lab services (AD, Splunk, Nessus, NAS, pfSense) reasonably available for training and experimentation.
   - Validate backup, restore, and snapshot procedures on LIBERTY and hypervisors.

4. **Assurance & Realism**
   - Demonstrate security engineering practices aligned with **JSIG/RMF thinking**: clear control allocation, continuous monitoring analogues, and documented security operations.
   - Use PCOS as a platform to test control implementations, STIG-like hardening, and security automation.
5. **Safety & Separation**
   - Ensure the lab remains logically separated from any production, employer, or customer networks.
   - Avoid routing PCOS experiments or attacks toward external infrastructure.

3. Security Assumptions and Threat Model

3.1 Security Assumptions

- The operator is **trusted** and acts in good faith while simulating adversary behavior for training.
- PCOS has **no direct trust relationship** with employer or government networks.
- Internet connectivity is used for:
  - OS/Package updates
  - Tool downloads
  - Threat intelligence / documentation
    and is mediated by **AREA51 (pfSense)**.
- All sensitive artifacts (e.g., config backups, diagrams, scripts) reside on **LIBERTY** or controlled repositories under the operator's control.

3.2 Threat Model (Conceptual)

PCOS is used to model threats such as:

- **External Adversaries (Simulated):**
  - Simulated scanning, exploitation, and lateral movement inside the lab network.
  - Malicious traffic modeled from offensive tools executed by the operator from dedicated VMs.
- **Misconfiguration and Insider Error (Realistic):**
  - Misapplied firewall rules, broken GPOs, incorrect NAS permissions, or unsafe Splunk configurations.
  - Unsafe or overly permissive Nessus credentials and scanning scopes.

- **Malware / Untrusted Downloads:**
  - Potential introduction of malware from:
    - Lab malware samples
    - Tools from the internet
  - Risk is constrained by architecture (no route into production networks, regular snapshots).

The SEC-CONOPS is less about protecting high-value mission data and more about **enforcing disciplined security engineering behavior** and verifying that security controls behave as expected.

4. Security Architecture Overview

The **security architecture** of PCOS leverages the base CONOPS structure, but emphasizes:

1. **Perimeter Security (AREA51 + USLINK)**
   - pfSense (AREA51) functions as the **single choke point** for:
     - Inbound/Outbound internet traffic
     - Optional VPN access
   - IDS/IPS features may be enabled to inspect and log simulated attack traffic.
   - USLINK provides Layer 2 connectivity and VLAN segmentation if/when configured to model separated enclaves (e.g., mgmt, server, client, DMZ subnets).
2. **Identity and Access Management (COMMAND)**
   - AD DS on COMMAND is the central authority for:
     - User accounts
     - Computer accounts
     - Group Policies (including security baselines, screen locks, password policies, etc.)
   - Domain membership is required for all production-like Windows systems where realistic behavior is desired.
3. **Security Monitoring and Analytics (UNION + DRONE)**
   - **UNION (Splunk + Nessus)** serves as the:
     - SIEM for log aggregation and correlation
     - Vulnerability scanner for PCOS assets
   - **DRONE (Prometheus/Grafana)** supplements SIEM capabilities with:

        - System resource telemetry
        - Service health visualization
        - Early warning indicators (CPU spikes, disk saturation, etc.)

4. **Data Security and Resilience (LIBERTY)**
    - LIBERTY hosts:
        - Configuration exports
        - Backups, snapshots, and archives
    - NAS permissions and shares (personal, shared, etc.) simulate data classification and access segregation.
5. **Compute and Testbeds (STAR/EAGLE)**
    - STAR (Windows) and EAGLE (Linux) hypervisors host:
        - Test VMs for blue-team detections
        - Attacker VMs for red-team simulations
        - Automation tooling (e.g., scripts, SCAP/PowerShell/Ansible proof-of-concept)

5. Security Roles and Responsibilities (Security Focus)

*These roles overlay the general roles from the primary CONOPS, but scoped to **security responsibilities (Me)***

Role	Key Security Responsibilities
Commander	Approves high-risk experiments; sets security objectives and lab "rules of engagement."
ISSO	Documents controls, maintains this SEC-CONOPS, performs simulated audits and spot checks, tracks "findings" and remediation.
ISSE	Designs control architecture, maps JSIG/NIST style controls to PCOS components, evaluates effectiveness of technical controls.
Network Admin	Maintains secure pfSense rules, VPN policies, VLANs, and core network ACLs; ensures separation from non-lab networks.
SysAdmin	Implements hardening (STIG-like), OS patching, account lifecycle, backup schedules, and least privilege on endpoints and servers.
SOC Analyst	Maintains and tunes Splunk detections, correlation searches, dashboards, and data onboarding (pfSense, Windows, NAS, Pi).
Incident Responder	Runs simulated incidents, executes containment and recovery procedures, performs forensics using Splunk and host logs.

6. Security Operations and Processes

6.1 Access Control and Authentication

- All Windows hosts of interest are **joined to the COMMAND domain**.
- Authentication uses domain accounts with:
  - Strong password policy
  - Role-based groups (e.g., PCOS-Admins, PCOS-Analysts)
- RDP and SSH are limited to designated admin hosts or subnets, mediated via AREA51 rules.
- Privileged accounts are used only when necessary and tested with "just enough administration" concepts where feasible.

6.2 Hardening and Configuration Management

- Systems follow a **STIG-inspired** baseline:
  - Local security policies and GPOs are applied from COMMAND.
  - Services are reduced to minimum necessary for each role.
- Configuration changes are:
  - Documented informally in change notes or a lab "change log."
  - Tested in non-critical VMs before being applied widely.

6.3 Logging, Monitoring, and Detection

- **Splunk (UNION)** receives:
  - Windows Security / Sysmon logs
  - pfSense firewall and VPN logs
  - NAS logging (if configured)
  - Lab application logs as needed
- **Grafana (DRONE)** displays:
  - Resource utilization and service availability metrics
- The operator:
  - Periodically reviews dashboards
  - Tunes detections based on simulated attacks

    - Creates correlation searches to detect:
        - Brute force attempts
        - Lateral movement patterns
        - New administrative account creation
        - Suspicious process starts

6.4 Vulnerability Management

- **Nessus** scans:
    - All PCOS subnets or specific high-value nodes (COMMAND, UNION, LIBERTY, hypervisors, representative clients/servers).
- Vulnerabilities are:
    - Reviewed and prioritized (critical, high, medium, low) in a lab context.
    - Used to test **patching and remediation workflows**, including:
        - OS updates
        - Application patches
        - Configuration changes and compensating controls

6.5 Incident Response (Simulated)

Incident handling in PCOS is used to **practice a disciplined methodology**, even though incidents are synthetic:

1. **Detection**
    - Alert from Splunk, Grafana, Nessus, or manual observation.
2. **Analysis & Scoping**
    - Use Splunk searches, Windows logs, pfSense logs, and host inspection to determine scope and potential impact.
3. **Containment**
    - Apply pfSense rules, disable accounts, or isolate VMs/networks via switch or hypervisor.
4. **Eradication & Recovery**
    - Remove malicious artifacts (if any), rebuild affected VMs if appropriate, restore from LIBERTY snapshots/backups.
5. **Lessons Learned & Control Updates**
    - Capture a short after-action note:

        - What was detected?
        - What worked?
        - What needs a new detection or new control?
    - Update Splunk dashboards, firewall rules, GPOs, or documentation accordingly.

7. Business Continuity & Backup (Lab Context)

Even in a home-lab context, PCOS treats continuity as a security objective:

- **LIBERTY NAS** maintains:
    - Snapshots for critical shares
    - Backups of configs (pfSense, Splunk, Nessus, AD exports, documentation)
- Hypervisors maintain **VM snapshots** or exports for:
    - Key infrastructure nodes (COMMAND, UNION, etc.)
- Recovery exercises are periodically run to:
    - Restore VMs from snapshots
    - Test re-joining machines to the domain
    - Validate that Splunk remains able to ingest and search historical data after disruptions

8. Compliance Mindset and Use as Training Platform

While PCOS is not an accredited federal system, the SEC-CONOPS intentionally **mirrors the mindset** of:

- NIST RMF / JSIG **control thinking**
- DoD enclave architectures
- Enterprise SIEM/SOC operational patterns

The lab is used to:

- Practice mapping conceptual controls to real components (e.g., AC, AU, CM, IR, SC families).
- Test implementations that could later be applied in real JSIG/RMF environments.
- Develop automation concepts (e.g., Sentinel Auditmation) for:
    - Control validation
    - Continuous monitoring

  - Security data correlation

9. Conclusion

This SEC-CONOPS defines **how PCOS is secured and how security is operated**, not just how the system functions. It:

- Clarifies security objectives and threat assumptions
- Defines the security architecture and control allocation
- Documents ongoing monitoring, vulnerability management, and incident handling
- Reinforces PCOS as a realistic, disciplined **security engineering training ground**

Updates to this SEC-CONOPS should occur whenever:

- New major components are added (e.g., additional SIEM, new hypervisors).
- Security tooling or monitoring architecture significantly changes.
- New standardized workflows (e.g., STIG automation, SCAP pipelines) are incorporated.