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

Audit and Log Review Procedures (Continuous Monitoring Plan)

12 Dec 2025

Authored By	Reece Niemuth
System Identifier	PCOS-Homelab
Date of Latest Revision	12 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.

Audit Log Review Procedures : Revision History

Revision / Version	Date	Description / Notes
Rev. 1 (1.0.0)	12 Dec 2025	Publication Inception / Creation

1. Purpose

The purpose of this Continuous Monitoring (ConMon) Plan is to define how audit logging, log review, and security monitoring activities are performed for the Patriot Command Operations System (PCOS). This plan establishes a practical, risk-based approach to monitoring system activity in support of system integrity, availability, and security awareness, while remaining appropriate for the intended use of PCOS as a research, training, and cybersecurity upskilling environment.

2. Scope

This plan applies to audit logs and security-relevant events generated by PCOS systems, including operating systems, network components, security tools, and supporting infrastructure. Continuous monitoring activities focus on identifying conditions that could negatively impact system availability, integrity, or security posture.

Disclaimer: Continuous monitoring activities for PCOS are intentionally scoped and prioritized to reflect the system's non-production, research, and training purpose. Monitoring cadence and depth may be adjusted based on available time and competing system objectives, including automation development, system testing, and cybersecurity exercises, while maintaining reasonable assurance of system security and availability.

3. Continuous Monitoring Philosophy

PCOS is a non-production system and does not require the same monitoring rigor as mission-critical or operational federal systems. Continuous monitoring is therefore implemented using a **tiered, risk-based approach**, emphasizing:

- Protection of core system availability
- Detection of unauthorized access or misuse
- Identification of significant configuration or security drift

Monitoring activities are performed at a cadence that balances effectiveness with real-world time and resource constraints.

4. Audit Logging Strategy

4.1 Log Sources

Audit logs may include, but are not limited to:

- Operating system security and system logs

- Authentication and authorization events
- Network device logs
- Security tooling logs (e.g., monitoring, scanning, alerting platforms)

Log sources are selected based on their relevance to system security and availability.

4.2 Log Collection and Retention

Logs are collected and retained in a manner that supports retrospective review, troubleshooting, and security analysis. Retention periods are determined based on system purpose and available storage, rather than strict regulatory minimums.

5. Log Review and Analysis

5.1 Review Prioritization

Log review activities are prioritized based on risk:

High Priority (More Frequent Review)

- Administrative or privileged account activity
- Authentication failures or anomalies
- Indicators of potential compromise
- Availability-impacting events

Lower Priority (Less Frequent Review)

- Routine system events
- Expected background activity
- Test or research-related events

5.2 Review Cadence

Log review is performed at intervals appropriate to risk and system use, including:

- Event-driven reviews following significant changes or incidents
- Periodic reviews on a **semi-annual to annual basis** for general system health
- Ad hoc reviews as time and circumstances permit

This cadence is intentional and documented to reflect PCOS's non-operational nature.

6. Continuous Monitoring Activities

Continuous monitoring activities may include:

- Review of audit logs and alerts
- Assessment of baseline configuration health
- Identification of anomalous or unexpected system behavior
- Review of monitoring tool outputs and dashboards

Activities focus on producing **actionable insights**, not exhaustive compliance metrics.

7. Findings, Actions, and Documentation

Monitoring activities may result in:

- No action required
- Configuration adjustments
- Security hardening improvements
- Documentation of observed risks or deviations

Significant findings are documented and may inform future risk assessments, configuration updates, or remediation activities.

8. Integration with Other Security Processes

Continuous monitoring supports and informs:

- Incident response activities
- Patch and vulnerability management
- Secure configuration procedures
- Future security assessments and authorization artifacts

9. Roles and Responsibilities (Single User)

- **ISSO**: Defines monitoring scope, priorities, and review cadence
- **System Administrator**: Supports log collection and monitoring tooling

- **Users**: Report anomalies or suspicious behavior

10. Limitations and Assumptions

PCOS continuous monitoring activities are intentionally scoped to reflect the system's research and training purpose. Monitoring cadence, depth, and automation are adjusted based on available time, resources, and system risk. This plan does not claim full regulatory equivalence with operational federal systems.

11. Enforcement

Failure to follow this plan may increase system risk or reduce situational awareness. Deviations from planned monitoring activities are documented when appropriate.

PCOS References – Audit and Log Review Procedures

1) **NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations**
   - *AU, CA, SI Control Families*

2) **NIST SP 800-92 Guide to Computer Security Log Management**
   - *General Management Guidance for Federal System Event Data*

3) **NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations**
   - *DoD / NIST Governance Framework for Continuous Monitoring of Federal System Events*