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

Secure Configuration Procedures

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.

Secure Configuration Procedures : Revision History

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

1. Purpose

The purpose of these Secure Configuration Procedures is to establish a standardized approach for configuring PCOS systems in a secure, consistent, and repeatable manner. These procedures ensure that system configurations reduce attack surface, support system integrity, and align with recognized cybersecurity standards, while remaining appropriate for the intended use of PCOS as a research, training, and cybersecurity upskilling environment.

2. Scope

These procedures apply to all PCOS system components, including operating systems, virtual machines, network devices, security platforms, and supporting infrastructure. Secure configuration practices apply throughout the system lifecycle, including initial build, configuration changes, maintenance, and system restoration.

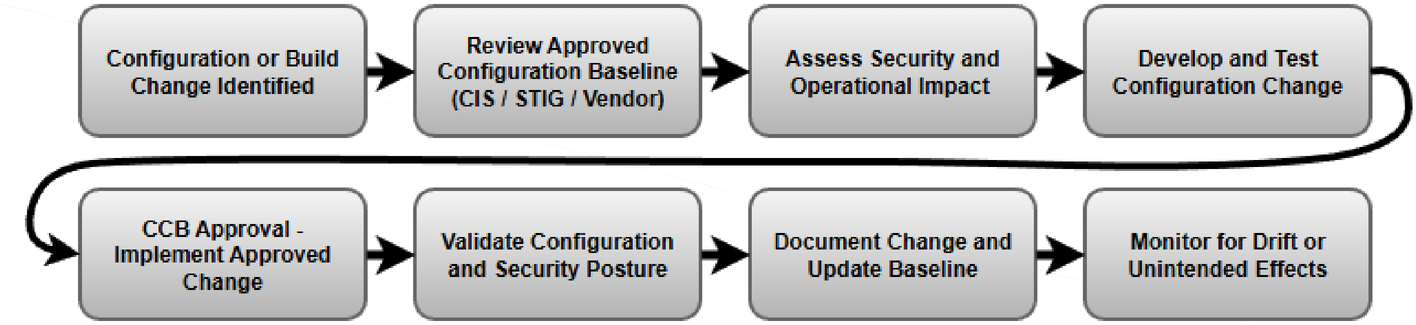
Configuration or Build Change Identified
Review Approved Configuration Baseline (CIS / STIG / Vendor)
Assess Security and Operational Impact
Develop and Test Configuration Change
CCB Approval - Implement Approved Change
Validate Configuration and Security Posture
Document Change and Update Baseline
Monitor for Drift or Unintended Effects

Figure 1 – Holistic Approach to Secure Configuration Management of PCOS

3. Configuration Baseline Approach

PCOS utilizes documented configuration baselines as the foundation for secure system builds. Baselines are derived from:

- Vendor-recommended secure configuration guidance
- DISA STIGs and/or CIS Benchmarks where applicable
- System-specific operational requirements

Baseline configurations are tailored to balance security, functionality, and usability consistent with the system's research and training objectives.

4. Secure Build Procedures

Initial system builds follow a standardized process, including:

- Installation of supported operating systems and software versions
- Removal or disabling of unnecessary services, features, and default accounts
- Application of baseline security configurations
- Verification of configuration settings prior to operational use

Default credentials are changed prior to system use.

5. Configuration Management and Change Control

Configuration changes are controlled and documented to prevent unauthorized or unintended modifications. Change control procedures include:

- Documentation of configuration changes
- Validation of security impact prior to implementation
- Testing of changes where feasible
- Rollback planning for significant changes

Emergency changes are documented after implementation.

6. Configuration Validation and Compliance

Secure configurations are periodically validated using available tools and methods, including:

- Manual configuration reviews
- Configuration comparison against documented baselines
- Automated or semi-automated checks where feasible (e.g., STIG or benchmark tools)

Validation frequency is commensurate with system complexity and change activity.

7. Configuration Drift Management

PCOS recognizes that configuration drift may occur due to system updates, patches, or testing activities. Drift is managed by:

- Identifying deviations from approved baselines
- Evaluating security impact

- Restoring baseline configurations or formally accepting deviations where appropriate

8. Protection of Configuration Data

System configuration files, scripts, and documentation are protected from unauthorized access and modification. Access is limited to authorized personnel and configuration data is included in backup and restoration activities.

9. Roles and Responsibilities (Single User)

- **ISSO**: Defines secure configuration requirements and approves deviations
- **System Administrator**: Implements and maintains secure configurations
- **Users**: Operate systems in accordance with approved configurations

10. Continuous Improvement

Secure configuration procedures are reviewed and updated periodically to reflect changes in system architecture, threat landscape, or applicable guidance. Lessons learned from testing, incidents, and system changes are incorporated to improve configuration effectiveness.

PCOS References – Secure Configuration Procedures

1) NIST SP 800-53 **Security and Privacy Controls for Information Systems and Organizations**
   - *CM-2, CM-6, CM-7, SI-7 Control Families*

2) DISA STIGs / CIS Benchmarks **Security Technical Implementation Guides and Security Requirements Guides for the Department of Defense (DOD) information technology systems as mandated by DODI 8500.01.**
   - *Secure Provisioning, Baselining, and Security / Risk Posture Management*

3) NIST SP 800-160 **Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems**
   - *Secure System Engineering Principles (Maintenance)*

4) NIST SP 800-70 **National Checklist Program for IT Products**
   - *National Checklist Program for Configuration Procedures / Plans Governance*