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

Media Protection 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.

Media Protection Plan : Revision History

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

1. Purpose

The purpose of this Media Protection Plan is to establish requirements for the protection, control, and handling of digital and physical media within the Patriot Command Operations System (PCOS). This policy ensures that removable media and system storage are managed in a manner that protects system integrity and reduces the risk of unauthorized data exposure, while remaining consistent with the intended use of PCOS as a cybersecurity research and training environment.

2. Scope

This policy applies to all forms of digital and physical media associated with PCOS, including removable storage devices, system storage media, backup media, and any media used to store or transfer PCOS-related data or configurations.

3. Media Classification and Usage

PCOS is a non-production research and training environment. Media usage is therefore limited to supporting system build, maintenance, backup, testing, and research activities. Media is categorized as follows:

- **System Media**: Internal storage used by servers, virtual machines, and infrastructure components
- **Removable Media**: External devices such as USB drives or external disks
- **Backup Media**: Media used for storing system backups and recovery data

Media containing transient test data or non-sensitive artifacts may be treated with reduced handling requirements, provided security risk is minimized.

4. Removable Media Controls

The use of removable media is **restricted by default** and permitted only when required for legitimate system purposes, such as:

- Initial system installation or recovery
- Transfer of system backups or configuration data
- Controlled testing or research activities

When removable media is used:

- Media must be approved prior to use

- Media must be scanned for malicious content before and after use
- Unauthorized or personally owned media is prohibited unless explicitly approved

5. Media Protection and Storage

Media must be protected against unauthorized access, damage, and loss. Protection measures include:

- Logical access controls on systems storing media data
- Physical protection of storage devices consistent with lab environment controls
- Storage of backup media in locations separate from primary system components when feasible

6. Media Sanitization and Disposal

Media containing PCOS system data or configurations must be sanitized prior to reuse or disposal. Sanitization methods are selected based on media type and risk, and may include:

- Logical wiping or secure erase functions
- Destruction or permanent removal from service when appropriate

Sanitization activities are documented where feasible.

7. Media Transport

Media transported outside of the immediate PCOS environment is minimized. When transport is necessary:

- Media is protected against loss or tampering
- Transport is limited to authorized individuals
- Media is returned or properly disposed of following use

8. Incident Handling

Loss, theft, damage, or suspected compromise of media must be reported promptly to the designated security authority (ISSO/ISSM). Media-related incidents are handled in accordance with established incident response procedures.

9. Roles and Responsibilities (Single User)

- **ISSO**: Defines media protection requirements and approves exceptions
- **System Administrator**: Implements and enforces media controls
- **Users**: Follow approved media handling and usage procedures

10. Enforcement

Failure to comply with this Media Protection Plan may result in revocation of system access or other corrective actions as appropriate.

PCOS References – Media Protection Policy

1) **NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations**
   - *MP-2, MP-5, MP-6, MP-7Control Families*

2) **NIST SP 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems**
   - *Secure System Handling Principles*