Cybersecurity Resilience 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.

Cybersecurity Resilience Plan : Revision History

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

LETTER FROM THE PCOS CYBERSECURITY PLANNER

Greetings,

The PCOS Cybersecurity Governance Authority is pleased to present the PCOS Cybersecurity and Cyber Resilience Plan. This plan represents an intentional, structured effort to design, operate, and continuously improve a resilient cybersecurity environment that mirrors enterprise and federal best practices while remaining feasible for a single-operator laboratory environment.

This plan aligns with guidance from CISA, NIST SP 800-53, NIST SP 800-160 Volumes 1 and 2, and RMF-based system authorization principles. While PCOS is not a regulated operational environment, the plan is designed to realistically simulate governance, risk management, and cyber resilience practices used in classified and mission-critical systems.

The objectives outlined in this plan emphasize resilience, recoverability, secure-by-design architecture, and disciplined operational practices. The Cybersecurity Plan is reviewed and approved by the PCOS Cybersecurity Governance Authority and serves as a living document that will evolve as the system matures.

Sincerely,

Reece Niemuth, MBA, CISSP-ISSEP, CCSP
PCOS System Owner
PCOS Cybersecurity Governance Authority

VISION AND MISSION

Vision	Mission
To maintain a resilient, defensible, and recoverable cybersecurity environment that reflects federal cybersecurity engineering principles and supports continuous learning, testing, and improvement.	To design, operate, and sustain PCOS using secure-by-design architecture, disciplined governance, and risk-informed cyber resilience practices that protect system availability, integrity, and recoverability.

CYBERSECURITY PROGRAM GOALS AND OBJECTIVES

Program Goal	Objectives
1. Establish Cyber Resilience Governance	1.1 Maintain documented governance artifacts 1.2 Review cybersecurity posture annually 1.3 Track system changes via formal change logging
2. Improve Detection and Visibility	2.1 Centralize security logging 2.2 Periodically validate audit coverage
3. Enhance Resilience and Recovery	3.1 Maintain tested backups 3.2 Document recovery procedures
4. Manage Risk Proactively	4.1 Perform periodic vulnerability assessments 4.2 Track risks through POA&M lifecycle
5. Strengthen Secure Configuration Practices	5.1 Maintain software and hardware baselines

CYBERSECURITY PLAN ELEMENTS

1) Manage, Monitor, and Track

PCOS maintains authoritative inventories of hardware, software, and system components. Version-controlled baselines are used to track configuration drift. Changes are documented via a system change log aligned to CM principles in NIST SP 800-53.

2) Monitor, Audit, and Track

Security-relevant events are centrally logged and periodically reviewed. Monitoring emphasizes system health, authentication activity, and configuration integrity rather than continuous SOC-style monitoring.

3) Enhance Preparedness

Preparedness is achieved through documented procedures, tabletop-style reviews, and controlled testing activities. The focus is on recoverability and containment, not real-time response operations.

4) Assessment and Mitigation

PCOS conducts vulnerability assessments using tools such as OpenSCAP and Nessus on a periodic basis. Findings are prioritized based on likelihood and impact and tracked through POA&M artifacts.

BEST PRACTICES AND METHODOLOGIES

PCOS aligns with the following cybersecurity best practices:

- Multi-factor authentication where feasible
- Centralized and enhanced logging
- Encryption for data at rest and in transit
- Elimination of unsupported or end-of-life systems
- Prohibition of default credentials
- Regular backup and restore validation
- Use of trusted and well-defined network boundaries

PCOS leverages NIST SP 800-53 and NIST SP 800-160 as guidance rather than compliance checklists.

SAFE ONLINE SERVICES

Online services are restricted to trusted internal services. External exposure is minimized, and services are documented, authenticated, and monitored.

CONTINUITY OF OPERATIONS

Continuity planning focuses on **system recoverability**, **data integrity**, and **service restoration**. COOP procedures reference the PCOS BIA and DRP artifacts and are validated periodically.

WORKFORCE

PCOS is operated by a single person simulating multiple official roles in the most accurate manner possible. Workforce capability is maintained through continuous professional development, certifications, and hands-on system testing aligned to NICE workforce principles.

CONTINUITY OF COMMUNICATIONS AND DATA NETWORKS

Network resilience is achieved through segmentation, documented network architecture, and configuration baselines. Critical services are prioritized for recovery.

CRITICAL INFRASTRUCTURE RISK

PCOS dependencies such as power, networking, and storage are identified and mitigated through redundancy where feasible and documented recovery strategies.

CYBER THREAT INDICATOR INFORMATION SHARING

PCOS leverages publicly available threat intelligence, vendor advisories, and CISA publications to inform defensive posture.

LEVERAGE CISA SERVICES

CISA guidance, publications, and frameworks are used as reference sources for resilience and risk management practices.

IT / OT MODERNIZATION REVIEW

PCOS periodically evaluates system architecture to ensure alignment between infrastructure capabilities and cybersecurity objectives.

CYBERSECURITY RISK AND THREAT STRATEGIES

Cyber risk strategies are documented and revisited during major system changes or assessment cycles.

RURAL COMMUNITIES

Not applicable. PCOS is a standalone environment.

FUNDING & SERVICES

PCOS is self-funded. Investment prioritizes core infrastructure, security tooling, and resiliency improvements. Capital investment is documented in the System Hardware Inventory / Baseline Documentation.

ASSESS CAPABILITIES

Capabilities are assessed whenever possible given single user time constraints. The system owner uses current workplace opportunities, academic research topics, and personal curiosity to inform and assign planning / system activity priority.

IMPLEMENTATION PLAN

Organization, Roles, and Responsibilities

- ISSO: Governance, risk management, documentation, assessments
- System Owner: Infrastructure and operations (combined role)

Resource Overview and Timeline

- Year 1: Baseline stabilization, documentation, assessments, and tooling development / testing
- Year 2: Resilience testing, refinement, automation enhancements, and tooling development / testing

METRICS

Objective	Metric	Description
Vulnerability Management	% of findings tracked	POA&M completeness
Resilience	Backup success rate	Restore validation
Governance	Artifact currency	Annual review status