Business Impact Analysis (BIA)

Conducted on 12 Dec 2025

Authored By	Reece Niemuth
System Identifier	PCOS-Homelab

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.

1. Overview

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the Patriot Command Operations System (PCOS). The BIA identifies and prioritizes mission and supporting system components by correlating them to the functions they enable and characterizing the impact of system unavailability.

This BIA supports the development of the PCOS Information System Contingency Plan (ISCP) and informs continuity, disaster recovery, and cyber resiliency planning activities.

1.1 Purpose

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports and using this information to characterize the impact on the process(es) if the system were unavailable.

The BIA is composed of the following three steps:

1. **Determine mission/business processes and recovery criticality.** Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

This document is used to build the PCOS Information System Contingency Plan (ISCP) and is included as a key component of the ISCP. It also may be used to support the development of other contingency plans associated with the system, including, but not limited to, the Disaster Recovery Plan (DRP) or Cyber Incident Response Plan.

2. System Description

PCOS is a standalone, non-production cybersecurity lab environment designed to simulate enterprise and DoD-aligned system security engineering, monitoring, and authorization workflows. The system supports cybersecurity operations, testing, documentation development, and continuous monitoring simulation.

Operating Environment

- Mixed Windows and Linux virtualized infrastructure
- pfSense firewall, managed switch, NAS storage, monitoring and logging platforms
- Segmented internal network with defined trust boundaries

Physical Location

- Single residential location
- Dedicated rack-mounted lab equipment with UPS protection

Users

- Single system owner/operator acting in ISSO/ISSE capacity

External Dependencies

- Internet service provider (ISP)
- Vendor update repositories (Microsoft, Linux package repos, Nessus, OpenSCAP)

Backup and Recovery

- Periodic system backups
- Manual restore procedures
- No real-time replication

(Refer to SSP and Architecture Diagrams for full technical detail.)

3. BIA Data Collection

BIA data was collected through system owner analysis, architectural review, and operational assumptions consistent with a representative cybersecurity lab environment. No interviews were required due to single-user system ownership.

3.1 Determine Process and System Criticality

Step one of the BIA process - Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), identify the specific mission/business processes that depend on or support the information system.

Mission / Business Process	Description
Cybersecurity Operations Simulation	Simulated ISSO/ISSE workflows including monitoring, assessment, and documentation
Security Testing & Validation	Execution of vulnerability scanning, STIG checks, and functional security testing
Documentation & Artifact Development	Development of RMF artifacts, policies, and procedures
Training & Skills Maintenance	Hands-on cybersecurity skill development

If criticality of mission/business processes has not been determined outside of the BIA, the following subsections will help to determine criticality of mission/business processes that depend on or support the information system.

3.1.1 Identify Outage Impacts and Estimated Downtime

This section identifies and characterizes the types of impact categories that a system disruption is likely to create in addition to those identified by the FIPS 199 impact level, as well as the estimated downtime that the organization can tolerate for a given process. Impact categories should be created and values assigned to these categories to measure the level or type of impact a disruption may cause. An example of cost as an impact category is provided. Organizations could consider other categories like harm to individuals and ability to perform mission. The template should be revised to reflect what is appropriate for the organization.

Outage Impacts

Impact categories and values should be created in order to characterize levels of severity to the organization that would result for that particular impact category if the mission/business process could not be performed. These impact categories and values are samples and should be revised to reflect what is appropriate for the organization.

The following impact categories represent important areas for consideration in the event of a disruption /impact.

> ***Example impact category = Cost***
>
> - ***Severe*** *- temp staffing, overtime, fees are greater than $1 million*
> - ***Moderate*** *– fines, penalties, liabilities potential $550k*

Impact Category: Operational Effectiveness

Impact values for assessing category impact:

- **Severe**: Loss of ability to perform cybersecurity testing or documentation activities for extended periods
- **Moderate**: Delays in testing or documentation with limited workarounds
- **Minimal:** Short-term inconvenience with no long-term effect

Impact Category: Data Integrity

- **Severe:** Loss or corruption of system baselines or documentation
- **Moderate:** Partial data loss recoverable from backups
- **Minimal:** No data loss

The table below summarizes the impact on each mission/business process if *PCOS* were unavailable, based on the following criteria:

Mission / Business Process (PCOS Homelab)	Operational Effectiveness	Data Integrity	Overall Impact
Cybersecurity Operations Simulation	Moderate	Moderate	Moderate
Security Testing & Validation	Moderate	Minimal	Moderate
Documentation & Artifact Development	Moderate	Moderate	Moderate
Training & Skills Maintenance	Minimal	Minimal	Minimal

Estimated Downtime

Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the downtime factors for consideration as a result of a disruptive event.

- **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important

because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.

- **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.
- **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

The table below identifies the MTD, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on *the PCOS. Values for MTDs and RPOs are expected to be specific time frames, identified in hourly increments (i.e., 8 hours, 36 hours, 97 hours, etc.).*

Mission / Business Process	MTD	RTO	RPO
Cybersecurity Operations Simulation	7 days	72 hours	24 hours
Security Testing & Validation	14 days	5 days	48 hours
Documentation & Artifact Development	7 days	72 hours	24 hours
Training & Skills Maintenance	30 days	14 days	N/A

Drivers: *Downtime tolerances are driven by non-production status, absence of real-world mission deadlines, and availability of manual documentation workarounds.*

Alternate Means: *Documentation tasks may be performed offline. Testing activities require system restoration.*

3.2 Identify Resource Requirements

The following table identifies the resources that compose the *PCOS* including hardware, software, and other resources such as data files. ***(Condensed Version, please review the official PCOS Hardware Baseline, Software Baseline, and Diagrams by clicking here.)***

System Resource / Component	Platform / OS	Description
Firewall (AREA51)	pfSense	Network boundary enforcement
Switch (USLINK)	Managed Switch	Internal network connectivity
Domain Controller (COMMAND)	Windows Server 2022	Identity and authentication
Security Server (UNION)	Windows/Linux	SIEM, vulnerability scanning
Hypervisors (STAR/EAGLE)	Windows/Linux	Virtualized workloads
NAS (LIBERTY)	NAS OS	Centralized storage and backups
Monitoring Node (DRONE)	Linux	Metrics and performance monitoring

It is assumed that all identified resources support the mission/business processes identified in Section 3.1 unless otherwise stated.

Note: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. ***(No BIA attachments, review here)***

3.3 Identify Recovery Priorities for System Resources

The table below lists the order of recovery for *the PCOS's* resources. The table also identifies the expected time for recovering the resource following a "worst case" (complete rebuild/repair or replacement) disruption.

- **Recovery Time Objective (RTO)** - RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

Priority	System Resource / Component	RTO
1	**Firewall (AREA51)**	24 hours
2	**Switch (USLINK)**	24 hours
3	**Domain Controller (COMMAND)**	48 hours
4	Security Server (UNION)	72 hours

Priority	System Resource / Component	RTO
5	Hypervisors (STAR/EAGLE)	72 hours
6	NAS (LIBERTY)	96 hours
7	Monitoring Node (DRONE)	7 days

Note: *Priorities are listed in descending order, with priority 1 being the highest.*

A system resource can be software, data files, servers, or other hardware and should be identified individually or as a logical group.

Identify any alternate strategies in place to meet expected RTOs. This includes backup or spare equipment and vendor support contracts.

Alternate Strategies

- Manual rebuild using documented baselines
- Vendor support and reinstall media
- Local backups stored on NAS

BIA Scope Disclaimer (Specific to the PCOS and Final Purpose):

This Business Impact Analysis represents a best-effort assessment for a non-production, representative cybersecurity lab environment and is intended to simulate enterprise contingency planning practices within realistic time and resource constraints.