mitrelogo-verysmall-white.png

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

For Internal <Sponsor> Use. This document was prepared for authorized distribution only. It has not been approved for public release.

©2023 The MITRE Corporation. All rights reserved.

<System Name> (<System Acronym>)

System Security Plan

<Document Number / Revision>

<Date>

<Case / Contract Number>

Prepared for:

<Sponsor Organization>

<Sponsor Info & Address>

Prepared by:

<Preparer Organization>

<Preparer Info & Address>

Based on ACT SSP Template version **1.1**

Table of Contents

[1. Introduction 1](#_Toc196813195)

[2. System Description and Authorization Boundary 1](#_Toc196813196)

[2.1 System Background and Purpose 1](#_Toc196813197)

[2.2 System Description 1](#_Toc196813198)

[2.3 System Identification and Security Level 2](#_Toc196813199)

[2.4 System Type Designation and Categorization/Classification 2](#_Toc196813200)

[2.5 System Operational Status 3](#_Toc196813201)

[2.6 Authorization Boundary Diagram and System Description 3](#_Toc196813202)

[2.7 Authorization Boundary Details 4](#_Toc196813203)

[2.7.1 Hardware Inventory 4](#_Toc196813204)

[2.7.2 Software Inventory 5](#_Toc196813205)

[2.7.3 Ports, Protocols, and Services (PPS) 5](#_Toc196813206)

[2.7.4 System Hardening 6](#_Toc196813207)

[2.7.5 System Interconnections 6](#_Toc196813208)

[2.7.6 User Roles and Access Privileges 7](#_Toc196813209)

[2.8 Responsible Parties 7](#_Toc196813210)

[2.8.1 Responsible Organizations 7](#_Toc196813211)

[2.8.2 Assignment of Security Responsibility 7](#_Toc196813212)

[2.8.3 Designated Contacts 8](#_Toc196813213)

[2.9 Rules of Behavior (RoB) 8](#_Toc196813214)

[2.10 Applicable Laws, Regulations, and Standards 8](#_Toc196813215)

[3. Security Controls Detail and Comment 9](#_Toc196813216)

List of Figures

[Figure 1. Authorization Boundary Diagram 3](#_Toc178242756)

List of Tables

[Table 1. System Identification 1](#_Toc178242757)

[Table 2. System Type Designation and Categorization/Classification 1](#_Toc178242758)

[Table 3. System Operational Status 2](#_Toc178242759)

[Table 4. Authorization Boundary Details 4](#_Toc178242760)

[Table 5. Hardware Inventory 5](#_Toc178242761)

[Table 6. Software Inventory 5](#_Toc178242762)

[Table 7. User Roles and Access Privileges 6](#_Toc178242763)

[Table 8. Responsible Organizations 6](#_Toc178242764)

[Table 9. ISSO/ISSM Contact Information 6](#_Toc178242765)

[Table 10. Business Owner Contact Information 7](#_Toc178242766)

[Table 11. System Developer/Maintainer Contact Information 7](#_Toc178242767)

Review Log

This section records the reviews that have been performed on this document.

| Date of Review | Version Reviewed | Name of Reviewer | Result of Review |
| --- | --- | --- | --- |
| <Date> | <Document Version> | <Name> | <Result> |

Change Log

This section summarizes the changes that have been made to this document.

| Date of Change | Document Version | Author | Summary of Changes |
| --- | --- | --- | --- |
| <Date> | <Version> |  | <Summary of Changes> |

# Introduction

This System Security Plan (SSP) documents the structured process for planning and executing DoD-compliant security protections, and is developed in accordance with the guidelines contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 (Guide for Developing Security Plans for Information Technology Systems), and applicable risk mitigation guidance and standards from other sources (see Section 2.9 below).

This SSP details the system’s current implementation of security controls based on the recommended security categorization and overlay, explaining the compliance, non-compliance, and non-applicability of each security controls.

# System Description and Authorization Boundary

This section describes the system’s purpose, components, and Authorization Boundary.

## System Background and Purpose

“Why does the system exist? What problem does the system solve? At a high level: what does the system do and how does it function?”

Using plain language, describe why the system was created, why it continues to operate, and what function(s) it performs. Include technical details as needed to “tell the story” of the system but aim for brevity and narrative vs. inclusion of large amounts of technical data.

[Provide a brief description (up to several paragraphs) of the assessed system’s background and purpose].

PN (as a United States partner nation) is investing in an Integrated Air and Missile Defense (PN IAMD) system to protect against air breathing threats (ABTs – e.g., military jets, shorter-range solid rockets) and ballistic missile threats (BMTs) out to at least 5000 kilometers. The ability for PN to defend its sovereignty, protect its national infrastructure, safeguard its citizens, and police its air, land, and sea trade routes is critical to PN and to the stability of the entire Persian Gulf region, one of the most geopolitically unstable areas in the world. The overall PN IAMD integrates a variety of sensing, weapons, and C3I (command, control, communication and intelligence) elements to meet its mission needs.

## System Description

“What are the system’s functions, architecture, technologies, interfaces, and deployment environment?”

Using plain language and at a high level, describe what the system does, the deployment architecture and involved technologies, what other systems or technologies it interfaces with, and the environment in which it is deployed. Include technical details as needed to “tell the story” of the system, but aim for brevity and narrative vs. inclusion of large amounts of technical data.

[Provide a brief description (up to several paragraphs) of the assessed system].

## System Identification and Security Level

Table 1. System Identification

|  |  |
| --- | --- |
| Official System Name | * Official System Name |
| System Acronym | * ABCD |
| System Purpose | * <Brief summary of the system’s purpose of the system – 1 to 2 sentences.> |
| System of Records (SOR) ID | * 12345 |
| Financial Management Investment Board (FMIB) Number | * 67890 |

## System Type Designation and Categorization/Classification

Table 2. System Type Designation and Categorization/Classification

|  |  |
| --- | --- |
| System Type | * Major Application (MA) * General Support System (GSS) * Cloud Service Provider (CSP) * Standalone (SUSA) * Multi-User Standalone (MUSA) * Closed Restricted Network (Local Area Network (LAN)) * Wide Area Network (WAN) * Interconnected System – Contractor-to-Contractor (C2C) * Interconnected System – Contractor-to-Government (C2G) * <Other System Type> |
| High Value Asset (HVA) | * Yes/No |
| FIPS 199 Security Category | * Overall: Low / Moderate / High * Confidentiality: Low / Moderate / High / Not Applicable * Integrity: Low / Moderate / High / Not Applicable * Availability: Low / Moderate / High / Not Applicable |
| FIPS 199 Security Category Rationale | * <Rationale – explain how the ratings for the Security Objectives and overall Security Category were determined> |
| Sensitivity Level (of System and/or Hosted Data) | * Public Trust (PT) * Confidential * Personally Identifiable Information (PII) * Protected Health Information (PHI) * Financial Data |
| Classification Level (of System and/or Hosted Data) | * Unclassified * Controlled Unclassified Information (CUI) * Secret * Top Secret * <Other Classification Level> |
| Classification Caveats | * None * FRD * RD * FGI * <Other> |
| Formal Access Approvals | * None * NATO * COMSEC * CNWDI * <Other> |
| System User / Development Personnel Minimum Clearance | * Confidential * Secret * Top Secret |
| System User / Development Personnel Minimum Access | * Interim * Final |
| System User / Development Personnel Citizenship | * US-only * Foreign Nationals: <Specify Nationalities> |

## System Operational Status

Table 3. System Operational Status

|  |  |
| --- | --- |
| Operational Status | * Under Development * New * Operational * Undergoing a Major Modification * <Other> |

## Authorization Boundary Diagram and System Description

Figure 1 provides the official diagram of the <System Acronym> Authorization Boundary:

A screenshot of a cell phone

Description automatically generated

Figure 1. Authorization Boundary Diagram

“How does the system work?”

Using plain language when possible, explain the environment, makeup, and functions of the system as shown in the Authorization Boundary Diagram(s). **It should be clear to the reader what is inside and what is outside the Authorization Boundary.**

Ensure that every component, function, and connection is covered, and clearly call out any component/function/connection that is not represented (or not represented accurately or adequately) in the Diagram(s). Do not provide large sets of low-level technical data (such as IP addresses, host names, etc.) unless they are required for understanding the Description narrative – technical data will be provided in the next section.

[Provide a detailed description of the environment, each component, each function, and each *internal* component connection shown in the Diagram(s).]

## Authorization Boundary Details

This section provides technical details about the system’s Authorization Boundary.

Table 4. Authorization Boundary Details

|  |  |
| --- | --- |
| Applications | * ABCD Main Application: Web Server 1, Web Server 2 * EFGH Supporting Application: Web Server 2 |
| Database Servers & Instances | * PRODDB01: Oracle 11i. * ABCD accounts payable database: Oracle 11i. * EFGH database: SQL Server 2013. * PRODDB04: SQL Server 2013 * ABCD accounts receivable database: Oracle 11i |
| Servers / Workstations & Operating Systems | * PRODDB01: Solaris 11.2 * PRODDB04: Windows Server 2013 R2 * PRODAPP01: Red Hat Enterprise Linux 6.6 |
| Any Mainframe-based Components Being Assessed? | * Yes / No |
| Network Devices / Infrastructure | * 192.168.1.25 (“Load Balancer”): SuperMax HyperBalance LB * 192.168.5.30 (“Switch”): Cisco 5620 Switch * 192.168.1.1 (“Firewall” at Internet/DMZ border): WatchGuard X45 * 192.168.5.1 (“Firewall at DMZ/Data Zone border): Sophos AV-FW Xtreme |
| Cloud Technologies | * Amazon Data Lake: Amazon S3 * Amazon Data Lake: AWS Lake Formation * Amazon Data Lake: Amazon Athena * Azure DevOps: Azure Pipelines * Azure DevOps: Azure Boards * [Other] |
| Cloud Services | * Amazon Data Lake * Amazon Virtual Private Cloud * Azure DevOps * Azure Data Factory * [Other] |
| Virtualization/Hypervisor Technologies | * Hyper-V Server 2019 * Red Hat Virtualization Hypervisor v4.4 * VirtualBox 7.0.10 * VMware ESX * [Other] |
| Other Technologies | * XYZ Tech |
| Interconnections (See Section 2.7.5 for details) | * System Name – Organization |
| Required Authentication Methods | * LDAP * RADIUS * TACACS / TACACS+ * Active Directory (AD) * Local Authentication * Resource Access Control Facility (RACF) |

### Hardware Inventory

Provide the full **hardware** inventory for every component inside the Authorization Boundary. Preferred method is to list the data here in a table, but if this will be too cumbersome then either embed a separate document here or reference/attach a separate document (provide the exact name, version, date, and location of the file). Any separate document that is referenced or attached must contain **at least** the information specified by the Hardware Inventory table below.

Note: do not embed documents unless both are true:  
1. The Sponsor’s IT systems allow embedded objects in documents.  
2. This SSP will not be converted to a format that does not support embedding (such as basic PDF).

[Provide hardware inventory here.]

Table 5. Hardware Inventory

| Manufacturer | Model | Version | IP/Hostname | Description |
| --- | --- | --- | --- | --- |
| SuperMax | HyperBalance | LB | 192.168.1.25 | Load balancer with built-in antivirus and graphic compression engine. |
| Dell | MegaBlade | XXL | PRODDB01 | Database server and local backup repository. |

### Software Inventory

Provide the full **software** inventory for every component inside the Authorization Boundary. Preferred method is to list the data here in table for bulleted list form, but if this will be too cumbersome then either embed a separate document here or reference one (provide the exact name, version, date, and location of the file). Any separate document that is referenced or attached must contain **at least** the information specified by the Software Inventory table below.

Note: do not embed documents unless both are true:  
1. The Sponsor’s IT systems allow embedded objects in documents.  
2. This SSP will not be converted to a format that does not support embedding (such as basic PDF).

[Provide software inventory here.]

Table 6. Software Inventory

| Manufacturer | Application | Version | IP/Hostname | Description |
| --- | --- | --- | --- | --- |
| Windows | Server | 2013 R2 | PRODDB01 | Operating system, STIG’d. |
| Oracle | Oracle | 11.1 | PRODDB01 | Relational database management system. |
| Backy | BackupMaster | 3000 | PRODDB01 | Local backup software – receives backups from other system components and stores in local filesystem as .rar files. |

### Ports, Protocols, and Services (PPS)

Detail all applications, protocols, and services (with their associated network ports) used within the Authorization Boundary.

The PPS list helps support:

* Acquisition and Development
* Certification/Authorization/Accreditation
* Enterprise, Organization, and/or System Designated Accrediting Authority (DAA)
* NetOps & Firewall Administrators
* Perimeter and boundary defense
* Connection approval processes

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Service Name | Port # | Protocol | Application Name | Network Environment | IP Address Range | Description | Network Boundaries |
| Web Server | 80 | HTTP | Apache | Public | 1.2.3.4, 1.2.5.6 | Provides browser-based access to statistical data. | Internet, DMZ |
| Web Server (Secure) | 443 | HTTPS (TLS) | Apache | Public | 1.2.3.4, 1.2.5.6 | Provides browser-based access to statistical data. | Internet, DMZ |

### System Hardening

Describe any specific manual or automated hardening steps or processes that the system requires.

Due to the mission critical nature of this network, hardening is required to protect data traversing it. System cybersecurity hardening uses the following tools and methods:

* Manual:
  + Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)
* Automated:
  + Security Content Automation Protocol Analysis (SCAP)
  + Tenable Nessus Vulnerability Scans (Nessus)

### System Interconnections

<System Acronym> has the following system interconnections[[1]](#footnote-2):

Table . System Interconnections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Interconnected (External) System | Owning Organization | Purpose of Interconnection | Ports/Protocols/Details | Memorandum of Understanding / Memorandum of Agreement |
|  |  |  |  |  |

### User Roles and Access Privileges

Table 8. User Roles and Access Privileges

| System | Application | Role | Privileges | Description |
| --- | --- | --- | --- | --- |
| PRODDB01 | BackupMaster | Administrator | Read, write, and execute for all application data | Administers access control and security functions for the application |
| PRODDB01 | BackupMaster | Supervisor | Read, write, and execute for all application data within their role | Validates or reviews all user application input |
| PRODDB01 | BackupMaster | User | Read all application data within their role | Reads and searches application data |

## Responsible Parties

This section enumerates the organizations and personnel responsible for the development, maintenance, and secure operation of the system.

### Responsible Organizations

Table 9. Responsible Organizations

|  |  |
| --- | --- |
| Authorizing Official | * <Sponsor> Chief Information Security Officer (CISO) |
| System Owner / Responsible Organization | * <Sponsor> / RX93 – Enterprise Information Technology Division Office |
| System Contractors & Roles | * ABC Contractor: Development * DEF Contractor: Maintenance * GHI Contractor: Hosting |

### Assignment of Security Responsibility

This section lists the personnel who have been assigned direct responsibility for the security of the system.

#### Information System Security Officer/Manager (ISSO/ISSM)

Table 10. ISSO/ISSM Contact Information

|  |  |
| --- | --- |
| Name | * John Smith |
| Title | * Division Director |
| Organization | * RX93 – Enterprise Information Technology Division Office |
| Street Address | * 123 Main St |
| Mailstop | * K481 |
| City, State, ZIP | * Anytown, AA 12345 |
| E-Mail | * email@email |
| Phone | * 555-555-5555 |

### Designated Contacts

This section lists personnel who have been designated as official contacts for the system.

#### Business/Mission Owner

Table 11. Business/Mission Owner Contact Information

|  |  |
| --- | --- |
| Name | * John Smith |
| Title | * Division Director |
| Organization | * RX93 – Enterprise Information Technology Division Office |
| Street Address | * 123 Main St |
| Mailstop | * K481 |
| City, State, ZIP | * Anytown, AA 12345 |
| E-Mail | * email@email |
| Phone | * 555-555-5555 |

#### System Developer/Maintainer

Table 12. System Developer/Maintainer Contact Information

|  |  |
| --- | --- |
| Name | * John Smith |
| Title | * Division Director |
| Organization | * RX93 – Enterprise Information Technology Division Office |
| Street Address | * 123 Main St |
| Mailstop | * K481 |
| City, State, ZIP | * Anytown, AA 12345 |
| E-Mail | * email@email |
| Phone | * 555-555-5555 |

## Rules of Behavior (RoB)

If the Sponsor has a documented Rules of Behavior (general and/or system-specific) then include it as an Appendix or attachment and reference it here. Document any additional system-specific Rules of Behavior here.

[Provide rules of behavior here.]

## Applicable Laws, Regulations, and Standards

[Provide list and details of applicable laws, regulations, and standards here.]

# Security Controls Detail and Comment

List the Security Controls that are in-scope for the system, along with compliance details. Clearly describe:

* Which parts of each control the system **complies** with (and how compliance is achieved).
* Which parts of each control the system **does not** comply with (and why compliance was not achieved).
* Which parts (or full controls) are not applicable (and why the control does not apply to this system).
* Which specific implementation details are **inherited** (and from which system).
* Which specific implementation details are **available for inheritance** by other systems (and whether or not system-specific actions will still need to be taken on those inherited implementation details by the inheriting system).

[Provide security control implementation details here – this will likely be many pages.]

1. Appendix Heading 1

Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text.

* 1. Appendix Heading 2

Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text. Body Text.

1. Per NIST SP 800-47 Rev. 1, a system interconnection is “a direct connection between two or more systems in different authorization boundaries for the purpose of exchanging information and/or allowing access to information, information services, and resources.” [↑](#footnote-ref-2)