**Security Assessment Report**

**SYS Name**

**(SYS Acronym)**

**Agency**

**Office/Branch**

**[Publish Date]**

Prepared by:

[Assessor]

Table of Contents

[1. Executive Summary 1](#_Toc386726013)

[1.1. Overview 1](#_Toc386726014)

[1.2. Scope 1](#_Toc386726015)

[1.3. Assessment Summary 1](#_Toc386726016)

[1.3.1. Deficiencies 2](#_Toc386726017)

[1.3.2. Remediations 2](#_Toc386726018)

[1.4. Assumptions, Constraints, and Deviations 2](#_Toc386726019)

[2. Appendices Descriptions 2](#_Toc386726020)

[3. Assessor Statement 4](#_Toc386726021)

Appendix A – Vulnerability Assessment – Issue Resolution

Appendix B – Risk Tables

Appendix C – Assessment Cases

Appendix D – Technical Test Report

# Executive Summary

## Overview

[Assessor] conducted a Security Assessment of the SYS Name (SYS Acronym),Choose an item., [GSS Application etc.]) for the ORG. The Security Assessment was conducted from [Assessment Start Date] through [SAR Delivery Date] in accordance with the methodology defined in the corresponding Security Assessment Plan (SAP).

The results of the assessment were reviewed with ISSO Name, Information System Security Officer (ISSO) who has the responsibility of communicating the results to the Authorization Official (AO). All items identified as false positive and verified as corrected and retested were documented and not forwarded to the risk assessment phase.

A risk assessment was performed for all unresolved vulnerabilities. The level of risk assigned to a vulnerability was based on the current state of the control at the time of assessment, information provided, and known temporal threats and mitigations. Risk ratings are based solely on base risk ratings and should be tailored to include Tiers 1 and 2 of NIST SP 800-30 rev 1, system specific environmental factors, as well as unique business requirements.

## Scope

The assessment was based on scope as defined in the Security Assessment Plan (SAP). Deviations from the SAP are identified in section 1.4.

## Assessment Summary

Include a summary of the system’s deficiencies and remediation’s. Cover significant issues identified and address all components of the system. This should not be a narrative on all issues that were identified. **(Include elements such as total # of controls, # of added controls, # of failures, and final # of vulnerabilities). DO NOT INCLUDE AN OVERALL POSTURE STATEMENT SUCH AS “THE OVERALL POSTURE OF THE SYSTEM IS CONSIDERED STRONG”.**

**EXAMPLE:**

The assessment included (730) technical, operational, and managerial controls. During the original control selection which is included in the Security Assessment Plan (SAP), (30) controls were added based on (observed failures, the request of the CISO, AO, ISSO). A total of 375 controls did not meet all or part of the requirement for one or more of the system components (Application or Infrastructure). Of the 375 controls, 75 failures were identified as High, 150 Medium, and 150 Low. The 375 individual control failures were summarized into 30 individual vulnerabilities, of which 20 were High, 5 Medium, and 5 Low.

Prior to the completion of the assessment (drafting of the SAR), 280 controls were remediated by the customer, and reassessed to ensure the remediation efforts fully satisfied the control requirements.

**List the deficiencies and remediation efforts by technology and component:**

## Deficiencies

**Auditing**

1. Application - Multiple deficiencies in regards to auditing were identified to include:

* The application does not record all the required elements in the log file to include time and date.
* No reviews of system logs key events are being performed.
* The system does not record Failed logins.

## Remediations

**Auditing**

1. Infrastructure – auditing features were enabled on dedicated network devices and external facing Linux Web Servers.

## Assumptions, Constraints, and Deviations

(Revise as needed)

The following assumptions and constraints apply to the development of this SAR:

* The authorization boundary described in the SSP is accurate and complete.
* The system is presently in the Choose an item. phase of its System Development Life Cycle (SDLC).
* All key stakeholders of the system were involved with the risk assessment process.
* Remediation activities were verified to reduce or eliminate system risk prior to the creation of the final SAR.
* Remaining vulnerabilities are tracked in the system’s Plan of Action & Milestones (POA&Ms).
* **List any controls not identified in the SAP**
* **Identify Security Plan changes after the SAP**
* **List any other changes that were not included in the SAP**

# Appendices Descriptions

Reference the appendices below for detailed assessment information:

* Appendix A: Issue Resolution (VA - IR) contains a detailed listing of vulnerabilities identified to include a description, threat-source, existing controls, likelihood, impact, risk level, and recommendation.
* Appendix B: Risk Tables
* Appendix C: Assessment Cases include examinations, interviews, and tests performed on selected security controls as outlined in the Security Assessment Plan (SAP) Control Selection Table (CST).
* Appendix D: Technical Test Report

Assessor Statement

[Assessor] has completed a Security Assessment of the SYS Acronym in accordance with: OMB Circular A-130; FISMA; and NIST Special Publications 800-37, Rev. 1; 800-53, Rev. 4; and Fiscal Service policies.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| NAME, Title  [Role]  [ORG] |  | Date |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| NAME, Title  [Role]  [ORG] |  | Date |

**Appendix A**

**Vulnerability assessment – Issue Resolution (VA - IR)**

**SYS Name**

**(SYS Acronym)**

**Agency**

**Office/Branch**

**[Publish Date]**

Prepared by:

[Assessor]

**Appendix B Risk Tables**

## Likelihood Determination

For each un-resolved vulnerability the probability of exploitation, compromise or failure is determined using the criteria presented in NIST SP 800-30 rev 1. Tables B1-B3 provide the details for determining the Likelihood Rating.

Table B1: Likelihood of failure or change (Initiation / occurrence)

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualitative**  **Values** | **Semi-Quantitative**  **Values** | | **Description** |
| Very High | 96-100 | 10 | Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**. |
| High | 80-95 | 8 | Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**. |
| Moderate | 21-79 | 5 | Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**. |
| Low | 5-20 | 2 | Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**. |
| Very Low | 0-4 | 0 | Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**. |

Table B2: Likelihood of compromise (adverse effects)

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualitative**  **Values** | **Semi-Quantitative**  **Values** | | **Description** |
| Very High | 96-100 | 10 | If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts. |
| High | 80-95 | 8 | If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts. |
| Moderate | 21-79 | 5 | If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts. |
| Low | 5-20 | 2 | If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts. |
| Very Low | 0-4 | 0 | If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts. |

Table B3: ASSESSMENT SCALE – OVERALL LIKELIHOOD

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood of Threat Event Initiation or Occurrence** | **Likelihood Threat Events Result in Adverse Impacts** | | | | |
| **Very Low** | **Low** | **Moderate** | **High** | **Very High** |
| **Very High** | Low | Moderate | High | Very High | Very High |
| **High** | Low | Moderate | Moderate | High | Very High |
| **Moderate** | Low | Low | Moderate | Moderate | High |
| **Low** | Very Low | Low | Low | Moderate | Moderate |
| **Very Low** | Very Low | Very Low | Low | Low | Low |

**Appendix B Rational Tables**

## Impact Determination

For each un-resolved vulnerability, the impact of exploitation, compromise or failure is determined using the criteria presented in Table B4. The mission can be adversely impacted when a threat event occurs, compromising data integrity, availability, and confidentiality.

Table B4: IMPACT OF THREAT EVENTS

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualitative**  **Values** | **Semi-Quantitative**  **Values** | | **Description** |
| Very High | 96-100 | 10 | The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| High | 80-95 | 8 | The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to  organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries. |
| Moderate | 21-79 | 5 | The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions,  but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to  individuals that does not involve loss of life or serious life-threatening injuries. |
| Low | 5-20 | 2 | The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. |
| Very Low | 0-4 | 0 | The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. |

## Risk Ranking

Unresolved vulnerabilities are assigned a risk level using the Risk-Level Matrix in Table B5. The risk level determination is calculated using the overall Likelihood and Impact information.

Table B5: LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood (Threat Event Occurs and Results in Adverse Impact)** | **Level of Impact** | | | | |
| **Very Low** | **Low** | **Moderate** | **High** | **Very High** |
| **Very High** | Very Low | Low | Moderate | High | Very High |
| **High** | Very Low | Low | Moderate | High | Very High |
| **Moderate** | Very Low | Low | Moderate | Moderate | High |
| **Low** | Very Low | Low | Low | Low | Moderate |
| **Very Low** | Very Low | Very Low | Very Low | Low | Low |

**Appendix C**

**Assessment Cases**

**SYS Name**

**(SYS Acronym)**

**Agency**

**Office/Branch**

**[Publish Date]**

Prepared by:

[Assessor]

**Appendix D**

**Technical Assessment Report**

**SYS Name**

**(SYS Acronym)**

**Agency**

**Office/Branch**

**[Publish Date]**

Prepared by:

[Assessor]