

template

StateRAMP Security Assessment Report

(SAR)

Service Provider Name

Information System Name

**VERSION:**

X.X

**DATE:**

YYYYMMDD

TABLE OF CONTENTS

[1. About this document 4](#_Toc69972980)

[1.1 Who should use this document? 4](#_Toc69972981)

[1.2 How this document is organized 4](#_Toc69972982)

[1.3 How to contact us 4](#_Toc69972983)

[2. Introduction 5](#_Toc69972984)

[2.1 Applicable Laws and Regulations 5](#_Toc69972985)

[2.2 Applicable Standards And Guidance 5](#_Toc69972986)

[2.3 Purpose 6](#_Toc69972987)

[2.4 Inclusion of Previous Assessment Results 6](#_Toc69972988)

[2.5 Scope 7](#_Toc69972989)

[3. System Overview 8](#_Toc69972990)

[3.1 Security Categorization 8](#_Toc69972991)

[3.2 System Description 8](#_Toc69972992)

[3.3 Purpose of System 8](#_Toc69972993)

[4. Assessment Methodology 9](#_Toc69972994)

[4.1 Perform Tests 9](#_Toc69972995)

[4.2 Assessment Deviations 9](#_Toc69972996)

[4.3 Identification of Vulnerabilities 9](#_Toc69972997)

[4.4 Consideration of Threats 10](#_Toc69972998)

[4.5 Perform Risk Analysis 17](#_Toc69972999)

[4.6 Document Results 18](#_Toc69973000)

[5. Security Assessment Results 18](#_Toc69973001)

[5.1 Security Assessment Summary 20](#_Toc69973002)

[6. Non-Conforming Controls 21](#_Toc69973003)

[6.1 Risks Corrected During Testing 21](#_Toc69973004)

[6.2 Risks With Mitigating Factors 21](#_Toc69973005)

[6.3 Risks Remaining Due to Operational Requirements 22](#_Toc69973006)

[7. Risks Known For Interconnected Systems 23](#_Toc69973007)

[8. Continued Authorization Recommendation 24](#_Toc69973008)

[9. Appendix 25](#_Toc69973009)

[9.1 Appendix A: Acronyms and Glossary 25](#_Toc69973010)

[9.2 Appendix B: Security Test Case ProcedureS template 26](#_Toc69973011)

[9.3 Appendix C: Infrastructure Scan Results 27](#_Toc69973012)

[9.3.1 INFRASTRUCTURE SCANS: INVENTORY OF ITEMS SCANNED 27](#_Toc69973013)

[9.3.2 Infrastructure Scans: Raw Scan Results 28](#_Toc69973014)

[9.3.3 Infrastructure Scans: False Positive Reports 28](#_Toc69973015)

[9.4 Appendix D: Database Scan Results 29](#_Toc69973016)

[9.4.1 Database Scans: Raw Scan Results 29](#_Toc69973017)

[9.4.2 Database Scans: Inventory of Databases Scanned 29](#_Toc69973018)

[9.4.3 Database Scans: False Positive Reports 30](#_Toc69973019)

[9.5 Appendix E: Web Application Scan Results 32](#_Toc69973020)

[9.5.1 Web Applications Scans: Raw Scan Results 32](#_Toc69973021)

[9.5.2 Web Applications Scans: False Positive Reports 33](#_Toc69973022)

[9.6 Appendix F: Assessments Results 34](#_Toc69973023)

[9.7 Other Automated & Misc. Tool Results 37](#_Toc69973024)

[9.7.1 Tools Used 37](#_Toc69973025)

[9.7.2 Inventory of Items Scanned 37](#_Toc69973026)

[9.7.3 Scan Results 38](#_Toc69973027)

[9.7.4 False Positive Reports 38](#_Toc69973028)

[9.8 Unauthenticated Scans 39](#_Toc69973029)

[9.8.1 All Scan Results 39](#_Toc69973030)

[9.8.2 False Positive Reports 39](#_Toc69973031)

[9.9 Appendix G: Manual Test Results 40](#_Toc69973032)

[9.10 Appendix H: Auxilary Documents 41](#_Toc69973033)

[9.11 Appendix I: Penetration Test Report 42](#_Toc69973034)

List of Tables

No table of figures entries found.

This document describes the State Risk and Authorization Management Program (StateRAMP) Annual Security Assessment Report (SAR) for <Service Provider>. The primary purpose of this document is to provide a Security Assessment Report for <Information System Name> for the purpose of making risk-based decisions. The StateRAMP website can be found at [www.stateramp.org](http://www.stateramp.org) and information included in this document is consistent with the program described on the website.

The assessment took place between <date> and <date>. The assessment was conducted in accordance with the approved Security Assessment Plan (SAP), dated <date>. The deviations from the approved SAP were <summary info here> as detailed in table 3-1, List of Assessment Deviations. All assessment activities documented to occur in the SAP <did / did not > take place as described.

The table below represents the aggregate risk identified from the StateRAMP assessment. High risks are <number>% of total risks for the system. Moderate risks are <number>% of total risks for the system. Low risks are <number>% of total risks for the system. There <are/ are not> risks identified that are required for continued operation of the system.

Table – Executive Summary of Risks

| Risk Category | Total | % of Total Risks |
| --- | --- | --- |
| High |  | XX%  |
| Moderate |  | XX%  |
| Low |  | XX%  |
| Operationally Required |  | XX%  |
| **Total Risks[[1]](#footnote-2)** |  | 100% |

# About this document

This document template is developed for Third-Party Independent Assessors (3PAOs) to report security assessment findings for a service provider. 3PAOs must edit this template to create a Security Assessment Report (SAR).

## Who should use this document?

This document is intended to be used by 3PAOs to record vulnerabilities and risks to service provider systems. U.S. government authorization officials may use the completed version of this document to make risk-based decisions.

## How this document is organized

This document is divided into eight sections and eight appendices.

|  |  |
| --- | --- |
| Section 1 | Provides information on the scope of the assessment. |
| Section 2 | Describes the system and its purpose. |
| Section 3 | Describes the assessment methodology. |
| Section 4 | Describes the security assessment results. |
| Section 5 | Describes acceptable non-conforming controls. |
| Section 6 | Provides risks known for interconnected systems. |
| Section 7 | Provides a re-authorization recommendation. |
| Section 8 | Provides additional references and resources. |
| Appendix A | Acronyms and Glossary |
| Appendix B  | Security test procedure workbooks that were used during the testing. |
| Appendix C | Provide reports and files from automated testing tools. |
| Appendix D | Provide reports and files from automated testing tools. |
| Appendix E | Provide reports and files from automated testing tools. |
| Appendix F | Provide reports and files from automated testing tools. |
| Appendix G | Provides results of manual tests. |
| Appendix H | Describes auxiliary documents reviewed |
| Appendix I | Provides penetration testing results |

## How to contact us

Questions about StateRAMP or this document may be directed to pmo@stateramp.org.For more information about StateRAMP, visit the website at [www.stateramp.org](http://www.stateramp.org).

# Introduction

This document consists of a *Security Assessment Report (SAR)* for <Information System Name> as required by StateRAMP. This SAR contains the results of the comprehensive security test and evaluation of the <Information System Name> system. This assessment report, and the results documented herein, is provided in support of <SP name> Security Authorization program goals, efforts, and activities necessary to achieve compliance with StateRAMP security requirements. The SAR describes the risks associated with the vulnerabilities identified during <SP name> security assessment and also serves as the risk summary report as referenced in *NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems*.

All assessment results have been analyzed to provide both the information system owner, <SP name>, and the authorizing officials, with an assessment of the controls that safeguard the confidentiality, integrity, and availability of data hosted by the system as described in the <system name> System Security Plan.

## Applicable Laws and Regulations

* Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
* E-Authentication Guidance for Federal Agencies [OMB M-04-04]
* Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
* Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
* Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
* Homeland Security Presidential Directive-7, Critical Infrastructure Identification,
* Prioritization and Protection [HSPD-7]
* Internal Control Systems [OMB Circular A-123]
* Management of Federal Information Resources [OMB Circular A-130]
* Management’s Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
* Privacy Act of 1974 as amended [5 USC 552a]
* Protection of Sensitive Agency Information [OMB M-06-16]
* Records Management by Federal Agencies [44 USC 31]
* Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
* Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

## Applicable Standards And Guidance

* A NIST Definition of Cloud Computing [NIST SP 800-145]
* Computer Security Incident Handling Guide [NIST SP 800-61, Revision 2]
* Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
* Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
* Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A, Revision 1]
* Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
* Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
* Guide for Mapping Types of Information and Information Systems to Security Categories [NIST SP 800-60, Revision 1]
* Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
* Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
* Managing Information Security Risk: Organization, Mission, and Information System View [NIST SP 800-39]
* Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
* Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-2]
* Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]
* Guide for Conducting Risk Assessments [NIST SP 800-30, Revision 1]
* Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
* Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
* Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
* Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

##  Purpose

The purpose of this document is to provide the system owner, <SP name>, and the StateRAMP Authorizing Official (AO) with a *Security Assessment Report* (SAR) for the <system name> annual assessment. A security assessment has been performed <system name> to evaluate the system’s implementation of, and compliance with, the StateRAMP baseline security controls. The implementation of security controls is described in the System Security Plan and required by StateRAMP to meet *Federal Information Security Management Act* (FISMA) compliance mandate.

StateRAMP requires service providers to use StateRAMP Accepted Third Party Assessment Organizations to perform independent security assessment testing and development of the SAR. Security testing for <system name> annual assessment was performed by <3PAO>. <3PAO>also performed the assessment completed for the Provisional ATO granted on <date>**.**

**Note:** delete the statement regarding previous assessments if a different IA was used.

## Inclusion of Previous Assessment Results

A subset of security controls listed in Section 2.5 below were assessed, as the remaining security controls were previously assessed under the security assessment performed as part of the JAB provisional authorization determination or agency ATO. The subset of controls is selected every year in accordance with guidance provided in the StateRAMP Continuous Monitoring Strategy and Guide, which includes a table summarizing the frequencies required for each continuous monitoring activity.

## Scope

This SAR applies to the <Information System Name> annual assessment, which included a security control assessment of the following controls, as identified and approved by the AO:

| Family | Control |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 1-1 – Identified Security Controls to be assessed during the Annual Assessment

The <**system** **name**>has a unique identifier which is noted in Table 1-2.

|  |  |  |
| --- | --- | --- |
| Unique Identifier | Information System Name | Information System Abbreviation |
|  |  |  |

Table 1-2 – Information System Unique Identifier, Name, and Information System Abbreviation

Documentation used by the 3PAO to perform the assessment of <system name> includes the following:

* <system name> *System Security Plan*
* <system name> *Contingency Plan & Test Results*
* <system name> *Incident Response Plan & Test Results*
* <system name> *Configuration Management Plan*
* <system name> *Security Assessment Plan*
* <system name> *Vulnerability Scan Reports*
* <system name> *Awareness and Training Reports*

The <system name> is physically located at the facilities noted in Table 1-3.

|  |  |  |
| --- | --- | --- |
| Data Center Site Name | Address | Description of Components |
|  |  |  |
|  |  |  |

Table 1-3 – Site Names and Addresses

# System Overview

## Security Categorization

The <Information System Name> is categorized as a <Low/Moderate> impact system. The <Information System Name> categorization was determined in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

## System Description

In the sections below, insert a general description of the information system. Use a description that is consistent with the description found in the System Security Plan (SSP). The description should only differ from the description in the SSP if additional information is going to be included that is not available in the SSP or if the description in the SSP is not accurate.

## Purpose of System

In the sections below, insert the purpose of the information system. Ensure that the purpose is consistent with the one in the System Security Plan.

# Assessment Methodology

The assessment methodology used to conduct the security assessment for the <Information System Name> system is summarized in the following steps:

1. Perform tests described in the Security Assessment Plan workbook and record the results
2. Identify vulnerabilities related to the service provider’s platform
3. Identify threats and determine which threats are associated with the cited vulnerabilities
4. Analyze risks based on vulnerabilities and associated threats
5. Recommend corrective actions
6. Document the results

## Perform Tests

<3PAO> performed security tests on the <Information System Name> which were concluded on <date>. The Security Assessment Plan (SAP) separately documents the schedule of testing, which <was/was not> adjusted to provide an opportunity for correcting identified weaknesses and re-validation of those corrections. The results of the tests are recorded in the Security Test Procedures workbooks which are attached in Appendix B. The findings of the security tests serve as inputs to this Security Assessment Report. A separate penetration test was performed, with the results documented in a formal Penetration Testing Report that is embedded as an attachment in appendix <Appendix Number> to this SAR.

## Assessment Deviations

<3PAO> performed security tests on the <system name> and the tests concluded on <date>. The table below contains a list of deviations from the original plan for the assessment presented in the SAP.

| Deviation ID | Deviation Description | Justification |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Table 3-1 – List of Assessment Deviations

## Identification of Vulnerabilities

Vulnerabilities have been identified by <3PAO> for the <Information System Name> through security control testing. The results of the security control testing are recorded in the Security Test procedures workbooks and the Security Assessment Plan (SAP).

A vulnerability is an inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact on the protection of the confidentiality, integrity, or availability of the system (application and associated data). A vulnerability may be due to a design flaw or error in configuration which makes the network, or a host on the network, susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in multiple areas of the system or facilities, such as in firewalls, application servers, web servers, operating systems, or fire suppression systems.

Whether or not a vulnerability has the potential to be exploited by a threat depends on a number of variables including (but not limited to):

* The strength of the security controls in place
* The ease at which a human actor could purposefully launch an attack
* The probability of an environmental event or disruption in a given local area

An environmental disruption is usually unique to a geographic location. Depending on the level of the risk exposure, the successful exploitation of a vulnerability can vary from disclosure of information about the host to a complete compromise of the host. Risk exposure to organizational operations can affect the business mission, functions, and/or reputation of the organization.

The vulnerabilities that were identified through security control testing (including penetration testing) for the <Information System Name> are identified in Table 4-1.

## Consideration of Threats

 A threat is an adversarial force or phenomenon that could impact the availability, integrity, or confidentiality of an information system and its networks including the facility that houses the hardware and software. A threat agent is an element that provides the delivery mechanism for a threat. An entity that initiates the launch of a threat agent is referred to as a threat actor.

A threat actor might purposefully launch a threat agent (e.g., a terrorist igniting a bomb). However, a threat actor could also be a trusted employee that acts as an agent by making an unintentional human error (e.g., a trusted staff clicks on a phishing email that downloads malware). Threat agents may also be environmental in nature with no purposeful intent (e.g., a hurricane). Threat agents working alone, or in concert, exploit vulnerabilities to create incidents. StateRAMP categorizes threats using a threat origination taxonomy of P, U, or E type threats as described in Table 3-2.

| Threat Origination Category | Type Identifier |
| --- | --- |
| Threats launched purposefully | P |
| Threats created by unintentional human or machine error  | U |
| Threats caused by environmental agents or disruptions | E |

Table 3-2 – Threat Categories and Type Identifiers

Purposeful threats are launched by threat actors for a variety of reasons and the reasons may never be fully known. Threat actors could be motivated by curiosity, monetary gain, political gain, social activism, revenge, or many other driving forces. It is possible that some threats could have more than one threat origination category.

Some threat types are more likely to occur than others. StateRAMP takes threat types into consideration to help determine the likelihood that a vulnerability could be exploited. The threat table shown in Table 3-3 is designed to offer typical threats to information systems and these threats have been considered for <Information System Name>.

A list of potential threats is found in Table 3-3. Assign threat types to vulnerabilities, then determine the likelihood that a vulnerability could be exploited by the corresponding threat. This table does not include all threat types and the IA may add additional threat types, or modify the listed threats, as needed.

| ID | Threat Name | Type Identifier | Description | Typical Impact to Data or System |
| --- | --- | --- | --- | --- |
| Confidentiality | Integrity | Availability |
|  | Alteration | U, P, E | Alteration of data, files, or records.  |  | Modification |  |
|  | Audit Compromise | P | An unauthorized user gains access to the audit trail and could cause audit records to be deleted or modified, or prevents future audit records from being recorded, thus masking a security relevant event. |  | Modification or Destruction | Unavailable Accurate Records |
|  | Bomb | P | An intentional explosion. |  | Modification or Destruction | Denial of Service |
|  | Communications Failure | U, E | Cut of fiber optic lines, trees falling on telephone lines. |  |  | Denial of Service |
|  | Compromising Emanations | P | Eavesdropping can occur via electronic media directed against large scale electronic facilities that do not process classified National Security Information. | Disclosure |  |  |
|  | Cyber Brute Force | P | Unauthorized user could gain access to the information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.  | Disclosure | Modification or Destruction | Denial of Service |
|  | Data Disclosure Attack | P | An attacker uses techniques that could result in the disclosure of sensitive information by exploiting weaknesses in the design or configuration. | Disclosure |  |  |
|  | Data Entry Error | U | Human inattention, lack of knowledge, and failure to cross-check system activities could contribute to errors becoming integrated and ingrained in automated systems. |  | Modification |  |
|  | Denial of Service Attack | P | An adversary uses techniques to attack a single target rendering it unable to respond and could cause denial of service for users of the targeted information systems.  |  |  | Denial of Service |
|  | Distributed Denial of Service Attack | P | An adversary uses multiple compromised information systems to attack a single target and could cause denial of service for users of the targeted information systems.  |  |  | Denial of Service |
|  | Earthquake | E | Seismic activity can damage the information system or its facility. Refer to the following document for earthquake probability maps <http://pubs.usgs.gov/of/2008/1128/pdf/OF08-1128_v1.1.pdf> . |  | Destruction | Denial of Service |
|  | Electromagnetic Interference | E, P | Disruption of electronic and wire transmissions could be caused by high frequency (HF), very high frequency (VHF), and ultra-high frequency (UHF) communications devices (jamming) or sunspots.  |  |  | Denial of Service |
|  | Espionage | P | The illegal covert act of copying, reproducing, recording, photographing, or intercepting to obtain sensitive information. | Disclosure | Modification |  |
|  | Fire | E, P | Fire can be caused by arson, electrical problems, lightning, chemical agents, or other unrelated proximity fires. |  | Destruction | Denial of Service |
|  | Floods | E | Water damage caused by flood hazards can be caused by proximity to local flood plains. Flood maps and base flood elevation must be considered. |  | Destruction | Denial of Service |
|  | Fraud | P | Intentional deception regarding data or information about an information system could compromise the confidentiality, integrity, or availability of an information system.  | Disclosure | Modification or Destruction | Denial of Service |
|  | Hardware or Equipment Failure | E | Hardware or equipment may fail due to a variety of reasons.  |  |  | Denial of Service |
|  | Hardware Tampering | P | An unauthorized modification to hardware that alters the proper functioning of equipment in a manner that degrades the security functionality the asset provides. |  | Modification | Denial of Service |
|  | Hurricane | E | A category 1, 2, 3, 4, or 5 land falling hurricane could impact the facilities that house the information systems.  |  | Destruction | Denial of Service |
|  | Malicious Software | P | Software that damages a system such a virus, Trojan, or worm.  |  | Modification or Destruction | Denial of Service |
|  | Phishing Attack | P | Adversary attempts to acquire sensitive information such as usernames, passwords, or SSNs, by pretending to be communications from a legitimate/trustworthy source. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to Web sites that appear to be legitimate sites, while actually stealing the entered information.  | Disclosure | Modification or Destruction | Denial of Service |
|  | Power Interruptions | E | Power interruptions may be due to any number of reasons such as electrical grid failures, generator failures, uninterruptable power supply failures (e.g., spike, surge, brownout, or blackout).  |  |  | Denial of Service |
|  | Procedural Error | U | An error in procedures could result in unintended consequences.  | Disclosure | Modification or Destruction | Denial of Service |
|  | Procedural Violations | P | Violations of standard procedures.  | Disclosure | Modification or Destruction | Denial of Service |
|  | Resource Exhaustion | U | An errant (buggy) process may create a situation that exhausts critical resources preventing access to services.  |  |  | Denial of Service |
|  | Sabotage | P | Underhand interference with work. |  | Modification or Destruction | Denial of Service |
|  | Scavenging | P | Searching through disposal containers (e.g., dumpsters) to acquire unauthorized data.  | Disclosure |  |  |
|  | Severe Weather  | E | Naturally occurring forces of nature could disrupt the operation of an information system by freezing, sleet, hail, heat, lightning, thunderstorms, tornados, or snowfall.  |  | Destruction | Denial of Service |
|  | Social Engineering | P | An attacker manipulates people into performing actions or divulging confidential information, as well as possible access to computer systems or facilities. | Disclosure |  |  |
|  | Software Tampering | P | Unauthorized modification of software (e.g., files, programs, database records) that alters the proper operational functions.  |  | Modification or Destruction |  |
|  | Terrorist | P | An individual performing a deliberate violent act could use a variety of agents to damage the information system, its facility, and/or its operations.  |  | Modification or Destruction | Denial of Service |
|  | Theft | P | An adversary could steal elements of the hardware.  |  |  | Denial of Service |
|  | Time and State | P | An attacker exploits weaknesses in timing or state of functions to perform actions that would otherwise be prevented (e.g. race conditions, manipulation user state).  | Disclosure | Modification | Denial of Service |
|  | Transportation Accidents | E | Transportation accidents include train derailments, river barge accidents, trucking accidents, and airlines accidents. Local transportation accidents typically occur when airports, seaports, railroad tracks, and major trucking routes occur in close proximity to systems facilities. Likelihood of HAZMAT cargo must be determined when considering the probability of local transportation accidents. |  | Destruction | Denial of Service |
|  | Unauthorized Facility Access | P | An unauthorized individual accesses a facility which may result in comprises of confidentiality, integrity, or availability.  | Disclosure | Modification or Destruction | Denial of Service |
|  | Unauthorized Systems Access | P | An unauthorized user accesses a system or data.  | Disclosure | Modification or Destruction |  |
|  | Volcanic Activity | E | A crack, perforation, or vent in the earth’s crust followed by molten lava, steam, gases, and ash forcefully ejected into the atmosphere. For a list of volcanoes in the U.S. see: <http://volcanoes.usgs.gov/about/volcanoes/volcanolist.php> . |  | Destruction | Denial of Service |

Table 3-3 – Potential Threats

## Perform Risk Analysis

The goal of determining risk exposure is to facilitate decision making on how to respond to real and perceived risks. The outcome of performing risk analysis yields risk exposure metrics that can be used to make risk-based decisions.

The StateRAMP risk analysis process is based on qualitative risk analysis. In qualitative risk analysis the impact of exploiting a threat is measured in relative terms. When a system is easy to exploit, it has a High likelihood that a threat could exploit the vulnerability. Likelihood definitions for the exploitation of vulnerabilities are found in Table 3-4.

| Impact | Description |
| --- | --- |
| Low | There is little to no chance that a threat could exploit a vulnerability and cause loss to the system or its data.  |
| Moderate | There is a moderate chance that a threat could exploit a vulnerability and cause loss to the system or its data. |
| High | There is a high chance that a threat could exploit a vulnerability and cause loss to the system or its data. |

Table 3-4 – Likelihood Definitions

Impact refers to the magnitude of potential harm that could be caused to the system (or its data) by successful exploitation. Definitions for the impact resulting from the exploitation of a vulnerability are described in Table 3-5. Since exploitation has not yet occurred, these values are perceived values. If the exploitation of a vulnerability can cause significant loss to a system (or its data) then the impact of the exploit is considered to be High.

| Impact | Description |
| --- | --- |
| Low | If vulnerabilities are exploited by threats, little to no loss to the system, networks, or data would occur. |
| Moderate | If vulnerabilities are exploited by threats, moderate loss to the system, networks, and data would occur.  |
| High | If vulnerabilities are exploited by threats, significant loss to the system, networks, and data would occur.  |

Table 3-5 – Impact Definitions

The combination of High likelihood and High impact creates the highest risk exposure. The risk exposure matrix shown in Table 3-6 presents the same likelihood and impact severity ratings as those found in *NIST SP 800-30 Risk Management Guide for Information Technology Systems*.

| Likelihood | Impact |
| --- | --- |
| Low | Moderate | High |
| High | Low | Moderate | High |
| Moderate | Low | Moderate | Moderate |
| Low | Low | Low | Low |

Table 3-6 – Risk Exposure Ratings

<3PAO and SP names> reviewed all identified weaknesses and assigned a risk to the weakness based on table 3-6. All identified scan risks have been assigned the risk identified by the scanning tool.

## Document Results

Documenting the results of security control testing creates a record of the security posture for the system at a given moment in time. The record can be reviewed for risk-based decision making and to create plans of action to mitigate risks.

The Federal Information Security Management Act (FISMA) requires that a Plan of Action and Milestones (POA&M) (using the format guidance prescribed by OMB) be developed and utilized as the primary mechanism for tracking all system security weaknesses and issues. <Service provider> will leverage the SAR to create a Plan of Action and Milestones (POA&M) for <Information System Name>. The POA&M is a mitigation plan designed to address specific residual security weaknesses and includes information on costing, resources, and target dates

# Security Assessment Results

This section describes all security weaknesses found during testing. The following elements for each security weakness are reported.

* Identifier
* Name
* Source of Discovery
* Description
* Affected IP Address/Hostname/Database
* Applicable Threats
* Likelihood (before mitigating controls/factors)
* Impact (before mitigating controls/factors)
* Risk Exposure (before mitigating controls/factors)
* Risk Statement
* Mitigating Controls/Factors
* Likelihood (after mitigating controls/factors)
* Impact (after mitigating controls/factors)
* Risk Exposure (after mitigating controls/factors)
* Recommendation

The reader of the SAR must anticipate that the security weakness elements are described as indicated below.

**Identifier:** All weaknesses are assigned a vulnerability ID in the form of V#-Security Control ID. For example, the first vulnerability listed would be reported as V1-AC-2(2) if the vulnerability is for control ID AC-2(2). If there are multiple vulnerabilities for the same security control ID, the first part of the vulnerability ID must be incremented, for example V1-AC-2(2), V2-AC-2(2).

**Name:** A short name unique for each vulnerability.

**Source of Discovery**: The source of discovery refers to the method that was used to discover the vulnerability (e.g., web application scanner, manual testing, security test procedure workbook, interview, document review). References must be made to scan reports, security test case procedures numbers, staff that were interviewed, manual test results, and document names. All scans and reports are attached in Appendices C, D, E, and F. Results of manual tests can be found in Appendix G. If the source of discovery is from one of the security test procedure workbooks, a reference must point to the Workbook name, the sheet number, the row number, the column number. Workbook tests results are found in Appendix B. If the source of discovery is from an interview, the date of the interview and the people who were present at the interview are named. If the source of discovery is from a document, the document must be named.

**Description:** All security weaknesses must be described well enough such that they could be reproduced by the SP, the ISSO, or the AO. If a test was performed manually, the exact manual procedure and any relevant screenshots must be detailed. If a test was performed using a tool or scanner, a description of the reported scan results for that vulnerability must be included along with the vulnerability identifier (e.g., CVE, CVSS, and Nessus Plugin ID etc.) and screenshots of the particular vulnerability being described. If the tool or scanner reports a severity level, that level must be reported in this section. Any relevant login information and role information must be included for vulnerabilities discovered with scanners or automated tools. If any security weaknesses affect a database transaction, a discussion of atomicity violations must be included.

**Affected IP Address/Hostname(s)/Database:** For each reported vulnerability, all affected IP addresses/hostnames/databases must be included. If multiple hosts/databases have the same vulnerability, list all affected hosts/databases.

**Applicable Threats:** The applicable threats describe the unique threats that have the ability to exploit the security vulnerability. (Use threat numbers from Table 3-3.)

**Likelihood (before mitigating controls/factors):** **High, Moderate, or Low** (see Table 3-4).

**Impact (before mitigating controls/factors): High, Moderate, or Low** (see Table 3-5).

**Risk Exposure (before mitigating controls/factors): High, Moderate, or Low** (see Table 3-6).

**Risk Statement:** Provide a risk statement that describes the risk to the business. (See examples in Table 4-1). Also indicate whether the affected machine(s) is/are internally or externally facing.

**Mitigating Controls/Factors:** Describe any applicable mitigating controls/factors that could downgrade the likelihood or risk exposure. Also indicate whether the affected machine(s) is/are internally or externally facing. Include a full description of any mitigating factors and/or compensating controls if the risk is an operational requirement>

**Likelihood (after mitigating controls/factors):** Moderate or Low (see Table 3-4) after mitigating control/factors have been identified and considered.

**Impact (after mitigating controls/factors):** Moderate or Low (see Table 3-5) after mitigating control/factors have been identified and considered.

**Risk Exposure (after mitigating controls/factors):** Moderate or Low (see Table 3-6) after mitigating controls/factors have been identified and considered.

**Recommendation:** The recommendation describes how the vulnerability must be resolved. Indicate if there are multiple ways that the vulnerability could be resolved or recommendation for acceptance of operational requirement.

**Justification or Proposed Remediation:** <Rationale for recommendation of risk adjustment><Rationale for operational requirement>.

## Security Assessment Summary

<Number> vulnerabilities (<number> moderate, <number> low) discovered as part of the penetration testing were also identified in the operating system or web application vulnerability scanning. These vulnerabilities have been combined in table 4-1 with the Source of Discovery column containing each of the types of testing that identified the vulnerability.

The summary is contained in the following embedded file:



Table 4-1 – Risk Exposure

# Non-Conforming Controls

In some cases, the initial risk exposure to the system has been adjusted due to either corrections that occurred during testing or to other mitigating factors.

## Risks Corrected During Testing

Risks discovered during the testing of <Information System Name> that have been corrected prior to authorization are listed in Table 5-1. Risks corrected during testing have been verified by <3PAO>. The verification method used to determine correction of is noted in the far right-hand column of the table.

| Identifier | Description | Source of Discovery | Initial Risk Exposure | Remediation Description | Date of Remediation | Verification Statement/Testing Procedures |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Table 5-1. Summary of Risks Corrected During Testing

## Risks With Mitigating Factors

Risks that have had their severity levels changed due to mitigating factors are summarized in Table 5-2. The factors used to justify changing the initial risk exposure rating are noted in the far right-hand column of the table. See Table 4-1 for more information on these risks.

IA should ensure that the content of this table is consistent with the same information documented in Table 4-1

| Identifier | Description | Source of Discovery | Initial Risk Exposure | Current Risk Exposure | Description of Mitigating Factors |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table 5-2 – Summary of Risks with Mitigating Factors

## Risks Remaining Due to Operational Requirements

Risks that reside in the <System Name> that cannot be corrected due to operational constraints are summarized in Table 5-3. An explanation of the operational constraints and risks are included below as well as in the appropriate Security Assessment Test Cases and System Security Plan (SSP). Because these risks will not be corrected, they are not tracked in the Plan of Actions and Milestones (POA&M). See Table 4-1 for more information on these risks.

3PAOs should ensure that the content of this table is consistent with the same information documented in Table 4-1. Note: The justification that remediating vulnerability will cause a break in functionality is not a sufficient rationale for permitting the risk to persist. There must also be mitigating factors and/or compensating controls.

| Identifier | Description | Source of Discovery | Current Risk Exposure | Operational Requirements Rationale |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

Table 5-3 – Summary of Risks Remaining Due to Operational Requirements

# Risks Known For Interconnected Systems

3PAO should include any known risks with interconnected systems that they discovered. Service providers shall disclose any known risks with interconnected systems.

In order to determine this information, it may be necessary to consult other Security Assessment Reports, Interconnection Agreements, Service Level Agreements, Memorandums of Understanding, and US-CERT advisories.

Inherent relationships between the system and other interconnected systems may impact the overall system security posture. A summary of the risks known for systems that connect to <Information System Name> is provided in Table 6-1.

| System | Authorization Date/Status | Date of POA&M | Control Family Identifiers |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 6-1 – Risks from Interconnected System

# Continued Authorization Recommendation

A total of <number> system risks were identified for <Information System Name>. Of the <number> risks that were identified, there were <number> High risks, <number> Moderate risks, <number> Low risks, and <number> of operationally required risks. The <number> of operational risks <is/are not> denoted in the Table 7-1 as mitigation activities are not going to be performed on this risk. Priority levels were established based on the type of vulnerability identified. <Other information as may be required>.

Table 7-1 indicates the priority of recommended risk mitigation actions for the <**system name**>

| Priority Number | Risk Level | Identifier | Vulnerability Description |
| --- | --- | --- | --- |
| 1 |  |  |  |
| 2 |  |  |  |

Table 7-1 – Risk Mitigation Priorities

<3PAO> attests that the SAR from the <system name> annual assessment testing provides a complete assessment of the applicable StateRAMP controls as stipulated in the SAP. Evidence to validate the successful implementation of the various security controls has been collected and validated. Based on the remaining risk as noted in Table 4-1, and the continuous improvement of security related processes and controls, <3PAO> recommends a continued authorization be granted for the <system name>.

# Appendix

## Appendix A: Acronyms and Glossary

|  |  |
| --- | --- |
| Acronym | Definition |
| 3PAO | Third Party Assessor Organization |
| AO | Authorizing Official |
| API | Application Programming Interface |
| ATO | Authorization to Operate |
| C&A | Certification & Accreditation |
| COTS | Commercial Off the Shelf |
| AO | Authorizing Official |
| StateRAMP | Federal Risk and Authorization Management Program |
| GSS | General Support System |
| IaaS | Infrastructure as a Service (Model) |
| ID | Identification |
| IA | Independent Assessor (3PAO) |
| IT | Information Technology |
| LAN | Local Area Network |
| NIST | National Institute of Standards and Technology |
| POA&M | Plan of Action and Milestones |
| POC | Point of Contact |
| RA | Risk Assessment |
| Rev. | Revision |
| SA | Security Assessment |
| SAR | Security Assessment Report |
| SDLC | System Development Life Cycle |
| SP | Special Publication |
| SSP | System Security Plan |

|  |  |
| --- | --- |
| Term | Definition |
| Threat | An adversarial force or phenomenon that could impact the availability, integrity, or confidentiality of an information system and its networks including the facility that houses the hardware and software. |
| Threat Actor | An entity that initiates the launch of a threat agent is referred to as a threat actor. |
| Threat Agent | An element that provides the delivery mechanism for a threat.  |
| Vulnerability | An inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact in the protection of the confidentiality, integrity, or availability of the system (application and associated data). |

## Appendix B: Security Test Case ProcedureS template

Provide the StateRAMP Security Test Case Procedures Template. Ensure that results of all tests are recorded in the template.

## Appendix C: Infrastructure Scan Results

Infrastructure scans consist of scans of operating systems, networks, routers, firewalls, DNS servers, domain servers, NIS masters, and other devices that keep the network running. Infrastructures scans can include both physical and virtual host and devices. The <tool name, version> vulnerability scanner was used to scan the <system name> network/OS components. <number>% percent of the inventory was scanned. For the remaining inventory, the 3PAO technical assessor performed a manual review of configuration files to analyze for existing vulnerabilities. Any results were documented in the SAR table.

Documents may be attached as an embedded file or if the file is not embedded and is sent to StateRAMP by other means, provide the title, version, and exact file name, including the file extension.

### INFRASTRUCTURE SCANS: INVENTORY OF ITEMS SCANNED

| IP Address(s) or Ranges | Hostname | Software & Version | Function | Comments |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table C-1 – Inventory of Items Scanned

### Infrastructure Scans: Raw Scan Results

Provide all fully authenticated infrastructure scans results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.

The following raw scan results files are included:

* <List files here include Title, Filename (including extension)>

Use the summary table to identify false positives that were generated by the scanner. For each false positive reported, add an explanation as to why that finding is a false positive. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “IS” in the identifier number refers to “Infrastructure Scan.”

### Infrastructure Scans: False Positive Reports

| ID # | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-IS |  |  |  |  |
| 2-FP-IS |  |  |  |  |
| 3-FP-IS |  |  |  |  |
| 4-FP-IS |  |  |  |  |

Table C-2 – Infrastructure Scans: False Positive Reports

## Appendix D: Database Scan Results

The <tool name, version> vulnerability scanner was used to scan the <system name> databases. <number>% percent of all databases were scanned.

### Database Scans: Raw Scan Results

Provide all database scans results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.

The following raw scan results files are included:

* <List files here include Title, Filename (including extension)>

### Database Scans: Inventory of Databases Scanned

Scan 100% of all databases that make up the candidate system unless otherwise approved. Indicate what was scanned in the table that follows. For “Function,” indicate the function that the database plays for the system (e.g., database image for end-user development, database for authentication records). Add additional rows as necessary.

| IP Address | Hostname | Software & Version | Function | Comment |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table D-1 – Inventory of Databases Scanned

### Database Scans: False Positive Reports

Use the summary table to identify false positives that were generated by the scanner. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. For each false positive reported, add an explanation as to why that finding is a false positive. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “DS” in the identifier number refers to “Database Scan.”

| ID # | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-DS |  |  |  |  |
| 2-FP-DS |  |  |  |  |
| 3-FP-DS |  |  |  |  |

Table D-2 – Database Scans: False Positive Reports

## Appendix E: Web Application Scan Results

The <tool name, version> vulnerability scanner was used to scan the <system name> web applications. <number>% of all web applications were scanned.

|  |  |  |  |
| --- | --- | --- | --- |
| Login URL | IP Address of Login Host | Function | Comments |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table E-1 – Inventory of Web Applications Scanned

### Web Applications Scans: Raw Scan Results

Provide all web application scans results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.

The following raw scan results files are included:

* <List files here include Title, Filename (including extension)>

### Web Applications Scans: False Positive Reports

Use the summary table to identify false positives that were generated by the scanner. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. For each false positive reported, add an explanation as to why that finding is a false positive. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “WS” in the identifier number refers to “Web Application Scan.”

| ID # | Scanner Severity Level | Page & IP Address | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-WS |  |  |  |  |
| 2-FP-WS |  |  |  |  |
| 3-FP-WS |  |  |  |  |
| 4-FP-WS |  |  |  |  |

Table E-2 – Web Application Scans: False Positive Reports

## Appendix F: Assessments Results

| Risk Level | Assessment Test Cases | OS Scans | Web Scans | DB Scans | Penetration Test | Total |
| --- | --- | --- | --- | --- | --- | --- |
| High | <#> | <#> | <#> | <#> | <#> | <#> |
| Moderate | <#> | <#> | <#> | <#> | <#> | <#> |
| Low | <#> | <#> | <#> | <#> | <#> | <#> |
| Operational Required | -<#> | -<#> | -<#> | -<#> | -<#> | -<#> |
| **Total** | <#> | <#> | <#> | <#> | <#> | <#> |

Table F-1 – Summary of System Security Risks from StateRAMP Testing

| Risk Level | Risks from StateRAMP Testing | Total Risks |
| --- | --- | --- |
| High | <#> | <#>(<#>% of Grand Total) |
| Moderate | <#> | <#> (<#>% of Grand Total) |
| Low | <#> | <#> (<#>% of Grand Total) |
| Operational Required | -<#> | -<#> |
| **Total** | <#> | <#> |

Table F-2 – Final Summary of System Security Risks

Use the following tables in Appendix F as applicable to the system and assessment results.

Table F-3, Open POA&Ms, shows the number of POA&Ms with Ongoing status as of <date>. The third column shows POA&Ms identified as closed in the <date> POA&M that not had been validated by the AO or by <3PAO>. The Duplicate Open POA&M Entries column shows POA&M items where the same vulnerability, typically from scanning was open under different vulnerability IDs and can be consolidated. Adding the POA&Ms with ongoing status column to the POA&Ms closed but not validated and subtracting the duplicate open POA&M results in the numbers in the Open POA&Ms column (as of <date>).

| Severity | POA&Ms with Ongoing Status as of <date> | POA&Ms Closed (as of <date>) but not Validated by AO or 3PAO | Duplicate Open POA&M Entries | Open POA&Ms (as of <date>) |
| --- | --- | --- | --- | --- |
| High |  |  |  |  |
| Moderate |  |  |  |  |
| Low |  |  |  |  |
| Total |  |  |  |  |

Table F-3 – Open POA&Ms

Table F-4, Summary of Existing POA&Ms, shows the number of Open POA&Ms as of <date> from Table F-3. Some of these POA&Ms can be closed as a result of testing performed by <3PAO> during this annual assessment the number of open POA&Ms minus the number of POA&Ms closed through testing results in the total number of remaining POA&Ms that need to be carried forward through continuous monitoring for the <system name>.

| Severity | Open POA&Ms (as of <date>) | POA&Ms Closed Through Testing | Total Remaining POA&Ms from <date> Submission |
| --- | --- | --- | --- |
| High |  |  |  |
| Moderate |  |  |  |
| Low |  |  |  |
| Total |  |  |  |

Table F-4 – Summary of Existing POA&Ms

Table F-5 Summary of Vulnerabilities to be Carried Forward contains the total remaining POA&Ms from the <date> submission from table F-3 in the first column. The number of findings identified in this annual assessment is contained in the Annual Assessment Findings column. The next column shows the number of SAR findings that are duplicates of existing POA&Ms. The difference of these columns yields the number of unique findings from the annual assessment. Adding the number of unique findings to the total remaining POA&Ms from the <date> submission results in the number of total remaining vulnerabilities to be addressed by <service provider> from both the POA&M and this annual assessment.

| Severity | Total Remaining POA&Ms from <date> Submission | Annual Assessment Findings | Duplicates with Existing POA&Ms | Unique Findings from the Annual Assessment | Total Remaining Vulnerabilities |
| --- | --- | --- | --- | --- | --- |
| High |  |  |  |  |  |
| Moderate |  |  |  |  |  |
| Low |  |  |  |  |  |
| Total |  |  |  |  |  |

Table F-5 – Summary of Vulnerabilities to be Carried Forward

| Identifier | Product/Embedded Component Description | Assessment Methodology Description |
| --- | --- | --- |
| UN0001 |  |  |

Table F-6 – Summary of Unauthenticated Scans

No additional automated tools were used during the <system name> annual assessment.

## Other Automated & Misc. Tool Results

### Tools Used

The <Scanner Name, Vendor, & Version #> was used to scan the <Information System Name>.

The <Scanner Name, Vendor, & Version #> was used to scan the <Information System Name>.

### Inventory of Items Scanned

Provide any additional tests performed using automated tools in this Appendix. Bundle all output from automated tools into one zip file. This Appendix may not be needed if no other automated tools were used. If that is the case, write “Not Applicable” in the first column.

|  |  |  |  |
| --- | --- | --- | --- |
| IP Address | Function | Finding | False Positive Explanation |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table F-7 – Other Automated & Misc. Tool Results

### Scan Results

Provide the results from all other automated tools. Bundle all reports generated by automated tools into one zip file. Do not insert files that require a license to read the file.

The following raw scan results files are included:

* <List files here include Title, Filename (including extension)>

### False Positive Reports

Use the summary table to identify false positives that were generated by tools. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. For each false positive reported, add an explanation as to why that finding is a false positive. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “OT” in the identifier number refers to “Other Tools.” Write “Not Applicable” in the first column if you are not using Appendix F.

| ID # | IP Address | Tool/Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-OT |  |  |  |  |
| 2-FP-OT |  |  |  |  |
| 3-FP-OT |  |  |  |  |
| 4-FP-OT |  |  |  |  |

Table F-8 – Other Automated & Misc. Tool Results: False Positive Reports

## Unauthenticated Scans

### All Scan Results

Provide the results from any unauthenticated scans. Bundle all reports generated by automated tools into one zip file. Do not insert files that require a license to read the file. In order to use this table, the IA must obtain approval from the AO when submitting the SAP. If this table is not used, write “Not Applicable” in the first column.

| IP Address | Hostname | Software & Version | Function | Comment |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table F-9 – Unauthenticated Scans

### False Positive Reports

Use the summary table to identify false positives that were generated by unauthenticated scans. For each false positive reported, add an explanation as to why that finding is a false positive. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “US” in the identifier number refers to “Unauthenticated Scan.” If Table F.4.1 was not used, do not use this table and write “Not Applicable” in the first column.

| ID # | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-US |  |  |  |  |
| 2-FP-US |  |  |  |  |
| 3-FP-US |  |  |  |  |
| 4-FP-US |  |  |  |  |

Table F-10 – Infrastructure Scans: False Positive Reports

## Appendix G: Manual Test Results

| Test ID | Test Name | Description | Finding |
| --- | --- | --- | --- |
| MT-1 |  |  |  |
| MT-2 |  |  |  |
| MT-3 |  |  |  |

Table G-1 – Manual Test Results

## Appendix H: Auxilary Documents

The <system name> SAR auxiliary documents are listed below. All evidence collected as part of the assessment has been posted in OMB MAX within the associated evidence zip files.

|  |
| --- |
| * <system name> System Security Plan
* <system name> Contingency Plan
* <system name> Contingency Plan Test Results
* <system name> Incident Response Plan
* <system name> Incident Response Test Results
* <system name> Configuration Management Plan
* <system name> Vulnerability Scan Reports
* <system name> Awareness and Training Reports
 |

## Appendix I: Penetration Test Report

The scope of this assessment was limited to the <system name> solution, including <list components here> components. <3PAO> conducted testing activities from the <location information here> via an attributable Internet connection. <Service provider name> provided IP addresses and URLs for all of the in-scope systems at the beginning of the assessment.

|  |  |
| --- | --- |
| Application | IP/URL |
|  |  |
|  |  |
|  |  |
|  |  |

Table I-1 – In-Scope Systems

The file below provides the full <system name> Penetration Test Report.

1. Total is the sum of High, Moderate and Low with Operationally Required represented as a subset of this total. [↑](#footnote-ref-2)