# FedRAMP Security Assessment Report (SAR) Template

FedRAMP

CSP Name

<Information System Name>

Sensitivity Level

Version 3.3

<Date>

Controlled Unclassified Information

# Prepared by

| Identification of Organization that Prepared this Document | | |
|---|---|---|
| | **Organization Name** | <Enter Company/Organization>. |
| | **Street Address** | <Enter Street Address> |
| | **Suite/Room/Building** | <Enter Suite/Room/Building> |
| | **City, State Zip** | <Enter Zip Code> |

# Prepared for

| Identification of Cloud Service Provider | | |
|---|---|---|
| | **Organization Name** | <Enter Company/Organization>. |
| | **Street Address** | <Enter Street Address> |
| | **Suite/Room/Building** | <Enter Suite/Room/Building> |
| | | |

# Record of Changes

| Date | Version | Page(s) | Description | Author |
|---|---|---|---|---|
| 6/6/2014 | | All | Major revision for SP800-53 Revision 4. Includes new template and formatting changes. | FedRAMP PMO |
| 10/21/2016 | 3.0 | All | Converted to standard document template; Clarity edits; Removed Acronyms and referenced F FedRAMP Master Acronyms and Glossary resource document; Instructions for the new Integrated Inventory Template Appendix C; Operational Requirements – False Positive Updates | FedRAMP PMO |

| Date | Version | Page(s) | Description | Author |
|---|---|---|---|---|
| 01/20/2017 | 3.1 | All | • "Prepared By" section: changed "Zip" to "ZIP" and corrected input field label.<br>• Corrected horizontal axis of table 3-6 from "Likelihood" to "Impact."<br>• Corrected references to the Security Assessment Summary Worksheet, and added it to the FedRAMP website.<br>• Corrected erroneous footers reading "Confidential Unclassified Information" to "Controlled Unclassified Information," and removed duplicate page numbers appearing in some footers in the middle of the footer text.<br>• Corrected typographical errors, capitalization, format.<br>• Added and clarified instruction boxes.<br>• Made all external links appear in the text for clarity.<br>• Corrected missing common input fields by including them as linked form fields.<br>• Removed Appendix K, which referred to an immature Table Creation Tool. | FedRAMP PMO |
| 2/22/2017 | 3.2 | Appendix A, Section 4 | Updated TOC to capture Appendix A RISK EXPOSURE TABLE | FedRAMP PMO |
| 3/9/2017 | 3.3 | Appendix H | Implementation Statement Differential changed back to "Yes" or "No" from "Low", "Moderate" or "High". This changed the verbiage throughout Appendix H.<br>Low, Moderate, and High Security Test Case Procedures Templates updated to reflect this change.<br>Updated Table of Contents to ensure pages numbers are current. | FedRAMP PMO |
| 6/6/2017 | 3.3 | Cover | Updated logo | FedRAMP PMO |
| 1/21/2022 | 3.3 | 1,3,36 | Updated outdated links | FedRAMP PMO |

# Revision History

| Date | Description | Version of SAR | Author |
|---|---|---|---|
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

### How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact *info@fedramp.gov*

For more information about the FedRAMP project, see www.fedramp.gov

# Table of Contents

# List of Tables

# 1. INTRODUCTION AND PURPOSE

This document consists of a *Security Assessment Report (SAR)* for <Information System Name> (Information System Abbreviation) as required by FedRAMP. This SAR contains the results of the comprehensive security test and evaluation of the Information System Abbreviation system. This assessment report and the results documented herein are provided in support of CSP Name Security Authorization program goals, efforts, and activities necessary to achieve compliance with FedRAMP security requirements. The SAR describes the risks associated with the vulnerabilities identified during the <Information System Name> security assessment and also serves as the risk summary report as referenced in National Institute of Standards and Technology (NIST) Special Publications (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 (SO), CSP Name, and the Authorizing Officials (AOs) with an assessment of the controls that safeguard the confidentiality, integrity, and availability of data hosted by the system as described in the Information System Abbreviation System Security Plan (SSP).

## 1.1. APPLICABLE LAWS AND REGULATIONS

The FedRAMP Laws and Regulations can be found on this page: https://www.fedramp.gov/documents-templates/ in the Document Phase SSP attachments.

Table 1-1 Information System Abbreviation Laws and Regulations includes additional laws and regulations specific to Information System Abbreviation. These will include law and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

*Include any additional Laws and Regulations specific to Information System Abbreviation in the table below.*

*Delete this instruction from your final version of this document.*

**Table 1-1 Information System Abbreviation Laws and Regulations**

| Identification Number | Title | Date | Link |
|---|---|---|---|
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

## 1.2. APPLICABLE STANDARDS AND GUIDANCE

The FedRAMP Standards and Guidance be found on this page: https://www.fedramp.gov/documents-templates/ with the SSP attachments.

Table 1-2 Information System Abbreviation Standards and Guidance includes any additional standards and guidance specific to Information System Abbreviation. These will include standards and guidance from Federal Information Processing Standards (FIPS) and NIST SP.

*Include any additional Standards and Guidance specific to Information System Abbreviation in the table below.*

*Delete this instruction from your final version of this document.*

***Table 1-2 Information System Abbreviation Standards and Guidance***

| Identification Number | Title | Date | Link |
|---|---|---|---|
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

## 1.3. PURPOSE

The purpose of this document is to provide the SO, CSP Name, and the AOs with a SAR for the Information System Abbreviation. A security assessment has been performed on the Information System Abbreviation to evaluate the system's implementation of, and compliance with, the FedRAMP baseline security controls. The implementation of security controls is described in the SSP, and required by FedRAMP to meet FISMA compliance mandate.

The FedRAMP program requires Cloud Service Providers (CSPs) to use a FedRAMP-accepted Independent Assessor (IA) Third Party Assessment Organization (3PAO) to perform independent security assessment testing and development of the SAR. Security testing for Information System Abbreviation was performed by Third Party Assessment Organization in accordance with the Information System Abbreviation Security Assessment Plan (SAP), dated Date.

## 1.4. SCOPE

This SAR applies to Information System Abbreviation which is managed and operated by CSP Name. The Information System Abbreviation that is being reported on in this document has a unique identifier which is noted in Table 1-3 Information System Unique Identifier, Name and Abbreviation.

***Table 1-3 Information System Unique Identifier, Name and Abbreviation***

| Unique Identifier | Information System Name | Information System Abbreviation |
|---|---|---|
| <Enter FedRAMP Application Number> | <Information System Name> | Information System Abbreviation |

*Instruction: 3PAOs must at the minimum review all the below listed documents. If other documents or files are reviewed, they must be attached in Appendix H and referred to as necessary.*

*Delete this instruction from your final version of this document.*

Documentation used by the Third Party Assessment Organization to perform the assessment of Information System Abbreviation includes the following:

- Information System Abbreviation *System Security Plan and Attachments*

  - *Information System Abbreviation Attachment 1: Information Security Policies and Procedures (covering all Control Families)*
  - *Information System Abbreviation Attachment 2: User Guide*
  - *Information System Abbreviation Attachment 3: E-Authentication Plan*
  - *Information System Abbreviation Attachment 4: Privacy Threshold Analysis/Privacy Impact Assessment*
  - *Information System Abbreviation Attachment 5: Rules of Behavior*
  - *Information System Abbreviation Attachment 6: Information System Contingency Plan and Test Results*
  - *Information System Abbreviation Attachment 7: Configuration Management Plan*
  - *Information System Abbreviation Attachment 8: Incident Response Plan*
  - *Information System Abbreviation Attachment 9: Control Implementation Summary Report and Worksheet*
  - *Information System Abbreviation Attachment 10: FIPS-199 Categorization*
  - *Information System Abbreviation Attachment 11: Separation of Duties Matrix*
  - *Information System Abbreviation Attachment 12: FedRAMP Laws and Regulations*
  - *Information System Abbreviation Attachment 13: FedRAMP Inventory Workbook*
- Information System Abbreviation *Business Impact Analysis*
- Information System Abbreviation *Security Assessment Plan*

The documentation listed above corresponds to the “CSP Security Package Documentation Checklist, dated MM/DD/YYYY, located on the FedRAMP website at the following URL: https://www.fedramp.gov/documents-templates/, under the “Document Phase”. Each system security assessment package must contain the required attachments, as listed.

The Information System Abbreviation is physically located at the facilities noted in Table 1-4 Site Names and Addresses.

***Table 1-4 Site Names and Addresses***

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

*Instruction: 3PAO must ensure that the site names match those found in the IT Contingency Plan (unless the site names found in the IT Contingency Plan were found to be in error in which case that must be noted.)*

*Delete this instruction from your final version of this document.*

# 2. SYSTEM OVERVIEW

## 2.1. SECURITY CATEGORIZATION

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

## 2.2. SYSTEM DESCRIPTION

*Instruction: 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 must 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.*

*Delete this instruction from your final version of this document.*

## 2.3. PURPOSE OF SYSTEM

*Instruction: 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.*

*Delete this instruction from your final version of this document.*

# 3. ASSESSMENT METHODOLOGY

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

3.1. Perform tests described in the SAP workbook and record the results
3.2. Identify vulnerabilities related to the CSP platform
3.3. Identify threats and determine which threats are associated with the cited vulnerabilities
3.4. Analyze risks based on vulnerabilities and associated threats
3.5. Recommend corrective actions
3.6. Document the results

## 3.1. PERFORM TESTS

Third Party Assessment Organization performed security tests on the Information System Abbreviation, which were concluded on <date>. The 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 identified in 7.Appendix B FedRAMP High, Moderate, or Low Security Test CASE Procedures . The findings of the security tests serve as inputs to this SAR. A separate penetration test was performed, with the results documented in a formal Penetration Test Report that is described as an attachment template in 7.Appendix J to this SAR.

### 3.1.1. Assessment Deviations

Third Party Assessment Organization performed security tests on the <Information System Name> and the tests concluded on <date>. The Table 3-1 List of Assessment Deviations below contains a list of deviations from the original plan for the assessment presented in the SAP.

*Table 3-1 List of Assessment Deviations*

| Deviation ID | Deviation Description | Justification |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |

## 3.2. IDENTIFICATION OF VULNERABILITIES

Vulnerabilities have been identified by Third Party Assessment Organization for the Information System Abbreviation through security control testing. The results of the security control testing are recorded in the Security Test procedures workbooks and the 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 Abbreviation are identified in the Information System Abbreviation SAR Risk Exposure Table.

## 3.3. 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. FedRAMP categorizes threats using a threat origination taxonomy of Purposeful (P), Unintentional (U), or Environmental (E) type threats as described in Table 3-2 Threat Categories and Type Identifiers.

*Table 3-2 Threat Categories and Type Identifiers*

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

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. FedRAMP takes threat types into consideration to help determine the likelihood that a vulnerability could be exploited. The threat table shown in Table 3-3 Potential Threats, is designed to offer typical threats to information systems and these threats have been considered for Information System Abbreviation.

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

*Delete this instruction from your final version of this document.*

*Table 3-3 Potential Threats*

| ID | Threat Name | Type Identifier | Description | Typical Impact to Data or System | | |
|---|---|---|---|---|---|---|
| | | | | Confidentiality | Integrity | Availability |
| T-1 | Alteration | U, P, E | Alteration of data, files, or records. | | Modification | |
| T-2 | 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 |
| T-3 | Bomb | P | An intentional explosion. | | Modification or Destruction | Denial of Service |
| T-4 | Communications Failure | U, E | Cut of fiber optic lines, trees falling on telephone lines. | | | Denial of Service |
| T-5 | Compromising Emanations | P | Eavesdropping can occur via electronic media directed against large scale electronic facilities that do not process classified National Security Information. | Disclosure | | |
| T-6 | 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 |
| T-7 | 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 | | |
| T-8 | 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 | |

| ID | Threat Name | Type Identifier | Description | Typical Impact to Data or System | | |
|---|---|---|---|---|---|---|
| | | | | Confidentiality | Integrity | Availability |
| T-9 | 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 |
| T-10 | 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 |
| T-11 | 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 |
| T-12 | 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 sun spots. | | | Denial of Service |
| T-13 | Espionage | P | The illegal covert act of copying, reproducing, recording, photographing or intercepting to obtain sensitive information. | Disclosure | Modification | |
| T-14 | Fire | E, P | Fire can be caused by arson, electrical problems, lightning, chemical agents, or other unrelated proximity fires. | | Destruction | Denial of Service |
| T-15 | 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 |
| T-16 | 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 |
| T-17 | Hardware or Equipment Failure | E | Hardware or equipment may fail due to a variety of reasons. | | | Denial of Service |

| ID | Threat Name | Type Identifier | Description | Typical Impact to Data or System | | |
|---|---|---|---|---|---|---|
| | | | | Confidentiality | Integrity | Availability |
| T-18 | 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 |
| T-19 | 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 |
| T-20 | Malicious Software | P | Software that damages a system such a virus, Trojan, or worm. | | Modification or Destruction | Denial of Service |
| T-21 | 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 |
| T-22 | 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 |
| T-23 | Procedural Error | U | An error in procedures could result in unintended consequences. | Disclosure | Modification or Destruction | Denial of Service |
| T-24 | Procedural Violations | P | Violations of standard procedures. | Disclosure | Modification or Destruction | Denial of Service |
| T-25 | Resource Exhaustion | U | An errant (buggy) process may create a situation that exhausts critical resources preventing access to services. | | | Denial of Service |
| T-26 | Sabotage | P | Underhand interference with work. | | Modification or Destruction | Denial of Service |
| T-27 | Scavenging | P | Searching through disposal containers (e.g., dumpsters) to acquire unauthorized data. | Disclosure | | |

| ID | Threat Name | Type Identifier | Description | Typical Impact to Data or System | | |
|---|---|---|---|---|---|---|
| | | | | Confidentiality | Integrity | Availability |
| T-28 | 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 |
| T-29 | 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 | | |
| T-30 | Software Tampering | P | Unauthorized modification of software (e.g., files, programs, database records) that alters the proper operational functions. | | Modification or Destruction | |
| T-31 | 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 |
| T-32 | Theft | P | An adversary could steal elements of the hardware. | | | Denial of Service |
| T-33 | 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 |
| T-34 | Transportation Accidents | E | Transportation accidents include train derailments, river barge accidents, trucking accidents, and airlines accidents. Local transportation accidents typically occur when airports, sea ports, 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 |
| T-35 | 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 |
| T-36 | Unauthorized Systems Access | P | An unauthorized user accesses a system or data. | Disclosure | Modification or Destruction | |

| ID | Threat Name | Type Identifier | Description | Typical Impact to Data or System | | |
|---|---|---|---|---|---|---|
| | | | | Confidentiality | Integrity | Availability |
| T-37 | 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 |

## 3.4. 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 FedRAMP 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 Likelihood Definitions.

*Table 3-4 Likelihood Definitions*

| Likelihood | 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. |

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 Impact Definitions. 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*.

*Table 3-5 Impact Definitions*

| 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. |

The combination of High likelihood and High impact creates the highest risk exposure. The risk exposure matrix shown in Table 3-6 Risk Exposure Ratings presents the same likelihood and impact severity ratings as those found in NIST SP 800-30 Risk Management Guide for Information Technology Systems. Analyzing the likelihood and impact of each vulnerability, based upon the potential threats yields a Risk Exposure Table as outlined in Section 4 of this SAR.

*Table 3-6 Risk Exposure Ratings*

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

Third Party Assessment Organization and CSP Name reviewed all identified weaknesses and assigned a risk to the weakness based on Table 3-6 Risk Exposure Ratings. All identified scan risks have been assigned the risk identified by the scanning tool.

### 3.5. RECOMMEND CORRECTIVE ACTIONS

Third Party Assessment Organization and CSP Name record and review all recommendations and corrective actions.

### 3.6. 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.

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. CSP Name will leverage the SAR to create a POA&M for Information System Abbreviation. The POA&M is a mitigation plan designed to address specific residual security weaknesses and includes information on costing, resources, and target dates.

## 4. RISK EXPOSURE TABLE

*For the most current template copy, the SAR Risk Exposure Table can be downloaded from the FedRAMP Template website: https://www.fedramp.gov/resources/templates-2016/ . Please see SAR Appendix A: Risk Exposure Table.*

*Delete this instruction from your final version of this document.*

The <Information System Name> SAR Risk Exposure Table describes all security weaknesses found during testing. The following elements for each security weakness are reported in this Table, as follows:

- Column A: Identifier
- Column B: Name
- Column C: Source of Discovery
- Column D: Description
- Column E: Affected internet protocol (IP) Address/Hostname/Database
- Column F: Applicable Threats
- Column G: Likelihood (before mitigating controls/factors)
- Column H: Impact (before mitigating controls/factors)
- Column I: Risk Exposure (before mitigating controls/factors)
- Column J: Risk Statement
- Column K: Mitigating Controls/Factors
- Column L: Likelihood (after mitigating controls/factors)
- Column M: Impact (after mitigating controls/factors)

- Column N: Risk Exposure (after mitigating controls/factors)
- Column O: Recommendation
- Column P: Justification or Proposed Remediation

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 identification (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 scan reports are attached in Appendices. Results of manual tests can be found in 7.Appendix G Manual Test Results. 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 7.Appendix B FedRAMP High, Moderate, or Low Security Test CASE Procedures . 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 CSP, the Information System Security Officer (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 Likelihood Definitions).

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

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

**Risk Statement:** Provide a risk statement that describes the risk to the business. (See examples in <System Name Acronym> SAR Risk Exposure Table). 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 Likelihood Definitions) after mitigating control/factors have been identified and considered.

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

**Risk Exposure (after mitigating controls/factors):** Moderate or Low (see Table 3-6 Risk Exposure Ratings) 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.> |

## 4.1. SECURITY ASSESSMENT SUMMARY

<Number> vulnerabilities (<Number> high, <Number> moderate, and <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 the SAR Risk Exposure Table with the Source of Discovery column containing each of the types of testing that identified the vulnerability.

The summary is contained in the file named <System Name Acronym> SAR Risk Exposure Table, included as an Appendix A to this SAR.

# 5. 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.

## 5.1. RISKS CORRECTED DURING TESTING

Risks discovered during the testing of Information System Abbreviation that have been corrected prior to authorization are listed in Table 5-1 Summary of Risks Corrected During Testing. Risks corrected during testing have been verified by Third Party Assessment Organization. The verification method used to determine the correction of each of the identified vulnerabilities is noted in the far right-hand column of the table as "Verification Statement".

***Table 5-1 Summary of Risks Corrected During Testing***

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

## 5.2. RISKS WITH MITIGATING FACTORS

Risks that have had their severity levels changed due to mitigating factors are summarized in Table 5-2 Summary of Risks with Mitigating Factors. The factors used to justify changing the initial risk exposure rating are noted in the far right-hand column of the table. See  this SAR Appendix A: <System Name Acronym> Risk Exposure Table for more information on these risks.

*Instruction: 3PAO must ensure that the content of this table is consistent with the same information documented in Appendix A: <System Name Acronym> Risk Exposure Table.*

*Delete this instruction from your final version of this document.*

*Table 5-2 Summary of Risks with Mitigating Factors*

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

## 5.3. RISKS REMAINING DUE TO OPERATIONAL REQUIREMENTS

Risks that reside in the <System Name> that cannot be corrected because of operational impact to the system are summarized in Table 5-3 Summary of Risks Remaining Due to Operational Requirements. An explanation of the operational impact and risks are included below as well as in the appropriate Security Assessment Test Cases and System Security Plan (SSP). Although these risks are not to be corrected, they are listed in this <System Name Acronym> SAR Appendix A: Risk Exposure Table, and tracked in the Plan of Action and Milestones (POA&M) as Operational Requirements.

*Instruction: 3PAO must ensure that the content of this table is consistent with the same information documented in <System Name Acronym> SAR Appendix A: Risk Exposure Table.*

*Delete this instruction from your final version of this document.*

Note: The justification that remediating a vulnerability will cause a break in functionality is not a sufficient rationale for permitting the risk to persist. There must also be full descriptions of the mitigating factors and compensating controls that address the ongoing risk to this specific system.

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

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

# 6. RISKS KNOWN FOR INTERCONNECTED SYSTEMS

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 Abbreviation is provided in Table 6-1 Risks from Interconnected Systems.

*Instruction: 3PAO must include any known risks with interconnected systems that they discovered. CSPs shall disclose any known risks with interconnected systems.*

*Delete this instruction from your final version of this document.*

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.

**Table 6-1 Risks from Interconnected Systems**

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

# 7. AUTHORIZATION RECOMMENDATION

A total of <Number> system risks were identified for Information System Abbreviation. Of the <Number> risks that were identified, there were <Number> High risks, <Number> Moderate risks, <Number> Low risks, and <Number> of operationally required risks. Priority levels were established based on the type of vulnerability identified.

*Instruction: In the space below this instruction, 3PAO must render a professional opinion of their analysis of risks for the information system based on the results from the security assessment. Any recommendations must be supported by findings, evidence, and artifacts. This recommendation will be fully reviewed by the AO.*

*Delete this instruction from your final version of this document.*

Table 7-1 Risk Mitigation Priorities indicates the priority of recommended risk mitigation actions for the Information System Abbreviation.

**Table 7-1 Risk Mitigation Priorities**

| Priority Number | Risk Level | Identifier | Vulnerability Description |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |

| Priority Number | Risk Level | Identifier | Vulnerability Description |
|---|---|---|---|
| 8 | | | |
| 9 | | | |
| 10 | | | |

Third Party Assessment Organization attests that the SAR from the <Information System Name> assessment testing provides a complete assessment of the applicable FedRAMP 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 <System Name Acronym> SAR Appendix A: Risk Exposure Table, and the continuous improvement of security related processes and controls, Third Party Assessment Organization recommends an authorization be granted for <Information System Name>.

# APPENDIX A. RISK EXPOSURE TABLE

As identified in Section 4, the Risk Exposure Table describes all security weaknesses found during testing. Each weakness is uniquely identified and described in this table that accompanies this SAR.

# APPENDIX B. FEDRAMP HIGH, MODERATE, OR LOW SECURITY TEST CASE PROCEDURES TEMPLATE

*Instruction: Provide the FedRAMP High, Moderate, or Low Security Test Case Procedures Template. The applicable template can be downloaded from the FedRAMP website. Ensure that results of all security control tests are recorded in the template.*

*Delete this instruction from your final version of this document.*

The <Information System Name> Security Test Case Procedures are captured in the FedRAMP Security Test Case Procedures Template that accompanies this SAR. The results of all security controls testing (interview, examine, test) are recorded in the template.

# APPENDIX C. INFRASTRUCTURE SCAN RESULTS

Infrastructure scans consist of scans of operating systems, networks, routers, firewalls, domain name servers (DNS), domain servers, network information security (NIS) masters, and other devices that keep the network running. Infrastructures scans can include both physical and virtual Host and devices. The <Scanner Name, Vendor, & Version #> was used to scan the Information System Abbreviation infrastructure. <Number> percent of the inventory was scanned. For the remaining inventory, the Third Party Assessment Organization technical assessor performed a manual review of configuration files to analyze for existing vulnerabilities. Any results were documented in the SAR table.

## C.1. Infrastructure Scans: Inventory of Items Scanned

*Instruction: This section should reference the system's Integrated Inventory Workbook, which should be maintained and updated monthly by the CSP.*

*Delete this instruction from your final version of this document.*

## C.2. Infrastructure Scans: Raw Scan Results for Fully Authenticated Scans

*Instruction: 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.*

*Delete this instruction from your final version of this document.*

The following Table C-1 Infrastructure Scans: Raw Scan Zip File Index shows the files that are included:

**Table C-1 Infrastructure Scans: Raw Scan Zip File Index**

| Title | File Name (includes extension) |
|---|---|
| | |
| | |
| | |
| | |

## C.3. Infrastructure Scans: False Positive [1]Reports

*Instruction: 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."*

*Delete this instruction from your final version of this document.*

The Table C-2 Infrastructure Scans: False Positive Reports below identifies false positives that were generated by the scanner.

***Table C-2 Infrastructure Scans: False Positive Reports***

| ID # | Page and IP Address | Scanner Severity Level | Finding | False Positive Explanation |
|---|---|---|---|---|
| 1-FP-IS | | | | |
| 2-FP-IS | | | | |
| 3-FP-IS | | | | |
| 4-FP-IS | | | | |
| 5-FP-IS | | | | |
| 6-FP-IS | | | | |
| 7-FP-IS | | | | |
| 8-FP-IS | | | | |
| 9-FP-IS | | | | |
| 10-FP-IS | | | | |

[1] A False Positive (FP) occurs when vulnerability is identified that does not actually exist on the system. For example, a vulnerability scanner may incorrectly identify a weakness that is not installed, or not completely identify a recent system update. Either the scanner is incorrect, or it has not found a completed system update.

# APPENDIX D. DATABASE SCAN RESULTS

The <Scanner Name, Vendor, & Version #> was used to scan the Information System Abbreviation databases. <Number> % percent of all databases were scanned.

## D.1. Database Scans: Inventory of Databases Scanned

*Instruction: Indicate the databases that were scanned. 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*

*Delete this instruction from your final version of this document.*

The database inventory scan results are found in Table D-1 Database Scans: Inventory of Databases Scanned below

***Table D-1 Database Scans: Inventory of Databases Scanned***

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

## D.2. Database Scans: Raw Scan Results

*Instruction: 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.*

*Delete this instruction from your final version of this document.*

The following Table E-2 Web Application Scans Raw Scan Zip File Index shows the files that are included:

***Table D-2 Database Scans: Raw Scan Zip File Index***

| Title | File Name (includes extension) |
|---|---|
| | |
| | |
| | |
| | |

## D.3. Database Scans: False Positive Reports

*Instruction: 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."*

*Delete this instruction from your final version of this document.*

The Table D-3 Database Scans: False Positive Reports below identifies false positives that were generated by the scanner.

***Table D-3 Database Scans: False Positive Reports***

| ID # | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
|---|---|---|---|---|
| 1-FP-DS | | | | |
| 2-FP-DS | | | | |
| 3-FP-DS | | | | |
| 4-FP-DS | | | | |
| 5-FP-DS | | | | |
| 6-FP-DS | | | | |
| 7-FP-DS | | | | |
| 8-FP-DS | | | | |
| 9-FP-DS | | | | |
| 10-FP-DS | | | | |

# APPENDIX E. WEB APPLICATION SCAN RESULTS

The <Scanner Name, Vendor, & Version #> was used to scan the <Information System Name> web applications. <Number> % of all web applications was scanned.

*Instruction: Indicate the web applications that were scanned. For "Function," indicate the function that the web-facing application plays for the system (e.g., control panel to build virtual machines). Add additional rows as necessary.*

*Delete this instruction from your final version of this document.*

## E.1. Web Applications Scans: Inventory of Web Applications Scanned

The web applications were scanned and the function the web-application plays for the system are indicated in the Table E-1 Web Application Scans: Inventory of Web Applications below.

***Table E-1 Web Application Scans: Inventory of Web Applications Scanned***

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

## E.2. Web Applications Scans: Raw Scan Results

*Instruction: 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.*

*Delete this instruction from your final version of this document.*

The following Table E-2 Web Application Scans Raw Scan Zip File Index shows the files that are included:

***Table E-2 Web Application Scans Raw Scan Zip File Index***

| Title | File Name (includes extension) |
|---|---|
| | |
| | |
| | |
| | |

## E.3. Web Applications Scans: False Positive Reports

*Instruction: 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."*

*Delete this instruction from your final version of this document.*

The following Table E-3 Web Application Scans: False Positive Reports identifies each false positive that was generated by the scanner.

*Table E-3 Web Application Scans: False Positive Reports*

| ID # | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
|---|---|---|---|---|
| 1-FP-WS | | | | |
| 2-FP-WS | | | | |
| 3-FP-WS | | | | |
| 4-FP-WS | | | | |
| 5-FP-WS | | | | |
| 6-FP-WS | | | | |
| 7-FP-WS | | | | |
| 8-FP-WS | | | | |
| 9-FP-WS | | | | |
| 10-FP-WS | | | | |

# APPENDIX F. ASSESSMENT RESULTS

Below is Table F-1 Assessment Results: Summary of System Security Risks from FedRAMP Testing.

*Table F-1 Assessment Results: Summary of System Security Risks from FedRAMP Testing*

| Risk Level | Assessment Test Cases | OS Scans | Web Scans | DB Scans | Source Code | Penetration Test | Total |
|---|---|---|---|---|---|---|---|
| High | | | | | | | |
| Moderate | | | | | | | |
| Low | | | | | | | |
| Operational Required | | | | | | | |
| Total | | | | | | | |

The products and methodology are represented in Table F-2 Assessment Results: Final Summary of System Security Risks

*Table F-2 Assessment Results: Final Summary of System Security Risks*

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

Table F-3 Assessment Results: Final Summary of Unauthenticated Scans identifies contents and methodology of the unauthenticated scans.

*Table F-3 Assessment Results: Final Summary of Unauthenticated Scans*

| Identifier | Product/Embedded Component Description | Assessment Methodology Description |
|---|---|---|
| 1-UAS | | |
| 2-UAS | | |
| 3-UAS | | |
| 4-UAS | | |

## F.1. Other Automated and Miscellaneous 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>.

### F.1.1. Other Automated and Miscellaneous Tool Results: Inventory of Items Scanned

*Instruction: 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.*

*Delete this instruction from your final version of this document.*

The other tools for the system are indicated in the Table F-4 Other Automated and Miscellaneous Tool Results: Inventory of Items Scanned below.

***Table F-4 Other Automated and Miscellaneous Tool Results: Inventory of Items Scanned***

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

### F.1.2. Other Automated and Miscellaneous Tool Results: Raw Scan Results

*Instruction: 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.*

*Delete this instruction from your final version of this document.*

The following Table F-5 Other Automated and Miscellaneous Tool Results: Raw Scan Result shows the files that are included:

***Table F-5 Other Automated and Miscellaneous Tool Results: Raw Scan Result***

| Title | File Name (includes extension) |
|---|---|
| | |
| | |
| | |
| | |

### F.1.3. Other Automated and Miscellaneous Tool Results: False Positive Reports

*Instruction: 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 Appendix F was not used.*

*Delete this instruction from your final version of this document.*

The Table F-6 Other Automated and Miscellaneous Tool: False Positive Reports below identifies false positives that were generated by other tools.

*Table F-6 Other Automated and Miscellaneous Tool: False Positive Reports*

| ID # | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
|---|---|---|---|---|
| 1-FP-OT | | | | |
| 2-FP-OT | | | | |
| 3-FP-OT | | | | |
| 4-FP-OT | | | | |
| 5-FP-OT | | | | |
| 6-FP-OT | | | | |
| 7-FP-OT | | | | |
| 8-FP-OT | | | | |
| 9-FP-OT | | | | |
| 10-FP-OT | | | | |

## F.2. Unauthenticated Scans

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

*Instruction: Indicate the Unauthenticated. For "Function," indicate the function that the web-facing application plays for the system (e.g., control panel to build virtual machines). Add additional rows as necessary.*

*Delete this instruction from your final version of this document.*

### F.2.1. Unauthenticated Scans: Inventory of Unauthenticated Scan Reports

*Instruction: 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 3PAO must obtain approval from the AO when submitting the SAP. If this table is not used, write "Not Applicable" in the first column.*

*Delete this instruction from your final version of this document.*

The unauthenticated scans for the system are indicated in the Table F-7 Unauthenticated Scans: Inventory of Unauthenticated Scan Reports below.

*Table F-7 Unauthenticated Scans: Inventory of Unauthenticated Scan Reports*

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

### F.2.2. Unauthenticated Scans: False Positive Reports

The Table D-3 Database Scans: False Positive Reports below identifies false positives that were generated by the scanner.

*Table F-8 Unauthenticated Scans: False Positive Reports*

| ID # | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
|---|---|---|---|---|
| 1-FP-US | | | | |
| 2-FP-US | | | | |
| 3-FP-US | | | | |
| 4-FP-US | | | | |
| 5-FP-US | | | | |
| 6-FP-US | | | | |
| 7-FP-US | | | | |
| 8-FP-US | | | | |
| 9-FP-US | | | | |
| 10-FP-US | | | | |

# APPENDIX G. MANUAL TEST RESULTS

*Instruction: The table that follows must record the test results for the manual tests that are described below. Each vulnerability found must be recorded as they are identified, as required in Section 4 of this document and in 7.Appendix A Risk Exposure Table, for this document. Put the test ID number for "Source of Discovery" in Section 4. For manual tests, if no vulnerability for a test was discovered, write "No."*

*Delete this instruction from your final version of this document.*

The test results for the manual tests that are described in Table G-1 Manual Test Results.

***Table G-1 Manual Test Results***

| Test ID | Test Name | Description | Finding |
|---|---|---|---|
| MT-1 | | | |
| MT-2 | | | |
| MT-3 | | | |
| MT-4 | | | |
| MT-5 | | | |

# APPENDIX H. DOCUMENTATION REVIEW FINDINGS

***Instruction: The table that follows must record the findings that result from the review of all documentation provided by the CSP (SSP and all attachments). These findings are documented in Appendix B, Security Test Procedure Workbook. Each test with an SSP Implementation Statement Differential Status of "No" must be recorded in*** **"Yes"** The SSP security control implementation statement is an accurate depiction and representation of the technical implementation within the environment and accurately describes the CSP's responsibility, the Customers responsibility, and/or the Shared responsibility between the CSP and the Customer.

**"No"** The SSP security control implementation statement is not an accurate depiction and representation of the technical implementation within the environment and does not accurately describe the CSP, Customer, or Shared responsibilities between the CSP and the Customer. The CSP has not properly documented exactly what is technically, operationally, or managerially taking place in the environment as the outcome of the 3PAO assessment was sufficiently varied from what is documented in the SSP.

*Table H-1 Documentation Review Findings, and <System Name Acronym> SAR Risk Exposure Table which is an appendix to this document. Create a unique ID as described in Section 4. The documentation deficiencies must be recorded as findings. For the <System Name Acronym> SAR Risk Exposure Table, put the name of the control in the "Name" field, put "Documentation Review" for "Source of Discovery," and complete the description of the inadequacy of the examined documentation based on the finding. Complete the rest of the information for <System Name Acronym> SAR Risk Exposure Table as described in Section 4 Risk Exposure Table .*

*Delete this instruction from your final version of this document.*

The following table documents the differences between the technical implementation and the written documentation describing the implementation, including the SSP and related documents. Consider this as the SSP Security Control Implementation Statement Differential: Does the SSP's security control / control objective implementation statement match the technical implementation within the CSP's environment? The impact level is determined as follows:

**"Yes"** The SSP security control implementation statement is an accurate depiction and representation of the technical implementation within the environment and accurately describes the CSP's responsibility, the Customers responsibility, and/or the Shared responsibility between the CSP and the Customer.

**"No"** The SSP security control implementation statement is not an accurate depiction and representation of the technical implementation within the environment and does not accurately describe the CSP, Customer, or Shared responsibilities between the CSP and the Customer. The CSP has not properly documented exactly what is technically, operationally, or managerially taking place in the environment as the outcome of the 3PAO assessment was sufficiently varied from what is documented in the SSP.

***Table H-1 Documentation Review Findings***

| Test ID | Name | Description of Differential | Impact Level of Differential: Yes or No |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# APPENDIX I. AUXILIARY DOCUMENTS

*Instruction: If any document (or files) other than those listed in Section 1.4 Scope, list them and in this section and provide them with this report. The list of the Attachments must include the title, version, and the exact file name, including the file extension.*

*Delete this instruction from your final version of this document.*

Documentation used by the 3PAO to perform the assessment of includes the following:

*SSP and Attachments*

- *Attachment 1: Information Security Policies and Procedures, title, version, and the exact file name, including the file extension*
- *Attachment 2: User Guide, title, version, and the exact file name, including the file extension*
- *Attachment 3: E-Authentication Plan, title, version, and the exact file name, including the file extension*
- *Attachment 4: PIA, title, version, and the exact file name, including the file extension*
- *Attachment 5: RoB, title, version, and the exact file name, including the file extension*
- *Attachment 6: ISCP, title, version, and the exact file name, including the file extension*
- *Attachment 7: CMP, title, version, and the exact file name, including the file extension*
- *Attachment 8: IRP, title, version, and the exact file name, including the file extension*
- *Attachment 9: CIS Workbook, title, version, and the exact file name, including the file extension*
- *Attachment 10: FIPS-199, title, version, and the exact file name, including the file extension*
- *Attachment 11: Separation of Duties Matrix, title, version, and the exact file name, including the file extension*
- *Attachment 12: FedRAMP Laws and Regulations, title, version, and the exact file name, including the file extension*
- *Attachment 13: Integrated Inventory Workbook, title, version, and the exact file name, including the file extension*

*Business Impact Analysis, title, version, and the exact file name, including the file extension*

*SAP, title, version, and the exact file name, including the file extension*

# APPENDIX J. PENETRATION TEST REPORT

The scope of this assessment was limited to the Information System Abbreviation solution, including <list components here> components. Third Party Assessment Organization conducted testing of CSP Name activities from the <location information here> via an attributable Internet connection. Provide IP addresses and uniform resource locators (URLs) for all of the in-scope systems at the beginning of the assessment.

*Table J-1 In-Scope Systems*

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

The attached file provides the full Information System Abbreviation Penetration Test Report.

# APPENDIX K. ACRONYMS AND GLOSSARY

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page under Program Overview Documents: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Master_Acronym_and_Glossary.pdf .

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.