Security Assessment Plan Template



Version X.X

Month xx, xxxx



Prepared by

| Identification of Third-Party Assessment Organization that Prepared this Document | | |
| --- | --- | --- |
| <**insert logo**> | Organization Name |  |
| Street Address |  |
| Suite/Room/Building |  |
| City, State Zip |  |

Prepared for

| Identification of Cloud Service Provider | | |
| --- | --- | --- |
| <**insert logo**> | Organization Name |  |
| Street Address |  |
| Suite/Room/Building |  |
| City, State Zip |  |

Template Revision History

| **Date** | **Page(s)** | **Description** | **Author** |
| --- | --- | --- | --- |
| 06/06/2014 |  | Major revision for SP800-53 Revision 4. Includes new template and formatting changes. | FedRAMP PMO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Template Revision History 3](#_Toc389750719)

[About this document 7](#_Toc389750720)

[Who should use this document? 7](#_Toc389750721)

[How this document is organized 7](#_Toc389750722)

[How to contact us 7](#_Toc389750723)

[1. Introduction 8](#_Toc389750724)

[1.1. Applicable Laws and Regulations 8](#_Toc389750725)

[1.2. Applicable Standards and Guidance 8](#_Toc389750726)

[1.3. Fedramp Requirements and Guidance 9](#_Toc389750727)

[1.4. Overview 10](#_Toc389750728)

[1.5. Purpose 10](#_Toc389750729)

[2. Scope 11](#_Toc389750730)

[2.1. System Name/Title 11](#_Toc389750731)

[2.2. IP Addresses Slated for Testing 12](#_Toc389750732)

[2.3. Web Applications Slated for Testing 12](#_Toc389750733)

[2.4. Databases Slated for Testing 13](#_Toc389750734)

[2.5. Roles Slated for Testing 13](#_Toc389750735)

[3. Assumptions 14](#_Toc389750736)

[4. Methodology 14](#_Toc389750737)

[5. Test Plan 15](#_Toc389750738)

[5.1. Security Assessment Team 15](#_Toc389750739)

[5.2. CSP Testing Points of Contact 16](#_Toc389750740)

[5.3. Testing Performed Using Automated Tools 16](#_Toc389750741)

[5.4. Testing Performed Through Manual Methods 17](#_Toc389750742)

[5.5. Schedule 17](#_Toc389750743)

[6. Rules of Engagement 18](#_Toc389750744)

[6.1.1. Security testing May Include 19](#_Toc389750745)

[6.1.2. Security Testing Will Not Include 19](#_Toc389750746)

[6.2. End of Testing 20](#_Toc389750747)

[6.3. Communication of Test Results 20](#_Toc389750748)

[6.4. Limitation of Liability 20](#_Toc389750749)

[6.5. Signatures 20](#_Toc389750750)

[Appendix A – Acronyms 22](#_Toc389750751)

[Appendix B – Test Case Procedures 23](#_Toc389750752)

[Appendix C – Penetration Testing Plan and Methodology 24](#_Toc389750753)

[Appendix D – Attachments 25](#_Toc389750754)

List of Tables

[Table 2-1 – Information System Name and Title 11](#_Toc389642793)

[Table 2-2 – Location of Components 11](#_Toc389642794)

[Table 2-3 – Components Slated for Testing 12](#_Toc389642795)

[Table 2-4 – Application URLs Slated for Testing 13](#_Toc389642796)

[Table 2-5 – Databases Slated for Testing 13](#_Toc389642797)

[Table 2-6 – Role Based Testing 14](#_Toc389642798)

[Table 5-1 – Security Testing Team 16](#_Toc389642799)

[Table 5-2 – CSP Points of Contact 16](#_Toc389642800)

[Table 5-3 – Tools Used for Security Testing 17](#_Toc389642801)

[Table 5-4 – Testing Performed Through Manual Methods 17](#_Toc389642802)

[Table 5-5 – Testing Schedule 18](#_Toc389642803)

[Table 6-1 – Individuals at CSP Receiving Test Results 20](#_Toc389642804)

4

# About this document

This document has been developed to provide guidance on how to complete security assessments for FedRAMP authorizations.

## Who should use this document?

This document is intended to be used by independent assessors when testing Cloud Service Provider (CSP) security controls.

## How this document is organized

This document is divided into six primary sections and four appendices:

|  |  |
| --- | --- |
| Section 1 | Describes an overview of the testing process. |
| Section 2 | Describes the scope of the security testing. |
| Section 3 | Describes assumptions related to the security testing. |
| Section 4 | Describes the security testing methodology. |
| Section 5 | Describes the test plan and schedule. |
| Section 6 | Describes the Rules of Engagement and signatures for security testing. |
| Appendix A | Table of Acronyms. |
| Appendix B | Test Case Scenarios |
| Appendix C | Penetration Testing Plan and Methodology |
| Appendix D | Attachments |

## How to contact us

Questions about FedRAMP or this document may be directed to [*info@fedramp.gov*](mailto:info@fedramp.gov)*.*

For more information about FedRAMP, visit the website at <http://www.fedramp.gov>.

1. Introduction
   1. 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]
  1. Applicable Standards and Guidance
* A NIST Definition of Cloud Computing [NIST SP 800-145]
* Computer Security Incident Handling Guide [NIST SP 800—61, Revision 1]
* 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]
* Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Guide to Understanding FedRAMP ]
* Guide for Developing 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 [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 201-1]
* Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]
* Risk Management Guide for Information Technology Systems [NIST SP 800-30]
* 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]
  1. Overview

Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for Cloud Service Providers (CSP). Testing security controls is an integral part of the FedRAMP security authorization requirements. Providing a plan for security control ensures that the process runs smoothly.

The <Information System Name> will be assessed by an Independent Assessor (3PAO). The use of an independent assessment team reduces the potential for conflicts of interest that could occur in verifying the implementation status and effectiveness of the security controls. NIST SP 800-39, Managing Information Security Risk states:

Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision.

* 1. Purpose

This document consists of a test plan to test the security controls for the <Information System Name>. It has been completed by <3PAO> for the benefit of <CSP>. NIST SP 800-39, Managing Information Security Risk states:

*Instruction: A goal of the kick-off meeting is to obtain the necessary information to populate this plan. The IA must obtain the requisite information on the CSP system at the kick-off meeting so that this plan can be completed. After this plan has been completed, the IA must meet again with the CSP, present the Draft Security Assessment Plan, and make any necessary changes before finalizing the plan. Both the Draft plan and Final plan must be submitted to the Authorizing Official (AO) for review.*

The information system owner and common control provider rely on the security expertise and the technical judgment of the assessor to: (i) assess the security controls employed within and inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and address identified vulnerabilities.

1. Scope
   1. System Name/Title

This <Information System Nam**e**>that is undergoing testing as described in this Security Assessment Plan is named in Table 2-1.

*Instruction: Name the system that that is slated for testing and include the geographic location of all components that will be tested. Put in a brief description of the system components that is a direct copy/paste from the description in the System Security Plan.*

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

Table 2-1 – Information System Name and Title

The physical locations of all the different components that will be tested are described in Table 2-2.

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

Table 2-2 – Location of Components

* 1. IP Addresses Slated for Testing

IP addresses, and network ranges, of the system that will be tested are noted in Table 2-3.

*Instruction: List the IP address of all systems that will be tested. You will need to obtain this information from the System Security Plan and the CSP. Note that the IP addresses found in the System Security Plan must be consistent with the boundary. If additional IP addresses are discovered that were not included in the System Security Plan, advise the CSP to update the inventory and boundary information in the SSP and obtain new approval on the SSP from the ISSO before moving forward. IP addresses can be listed by network ranges and CIDR blocks. If the network is a large network (Class B or larger), test a subset of the IP addresses. All scans must be fully authenticated. Add additional rows to the table as necessary.*

*CSPs must ensure that the inventory is current before testing, and that the inventory and components to be tested are in agreement.*

*In lieu of filling out this table, CSPs may embed a separate file or refer to Appendix D, as long as all required information is included. In addition, CSPs may use any unique identifier (e.g. MAC address or hostname), instead of the IP address.*

| No. | IP Address(s) or Ranges | Hostname | Software & Version | Function |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 2-3 – Components Slated for Testing

* 1. Web Applications Slated for Testing

Activities employed to perform role testing on web applications may include capturing POST and GET requests for each function. The various web based applications that make up the system, and the logins and their associated roles that will be used for testing are noted by URL in Table 2-4.

*Instruction: Insert any URLs and the associated login IDs that will be used for testing. Only list the login URL. Do not list every URL that is inside the login in the below table. In the Function column, indicate the purpose that the web-facing application plays for the system (e.g. control panel to build virtual machines).*

*In lieu of filling out this table, CSPs may embed a separate file or refer to Appendix D, as long as all required information is included. In addition, CSPs may use any unique identifier (e.g. MAC address or hostname), instead of the IP address.*

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

Table 2-4 – Application URLs Slated for Testing

* 1. Databases Slated for Testing

Databases that are slated for testing include those listed in Table 2-5.

*Instruction: Insert the hostnames, IP address, and any relevant additional information on the databases that will be tested. All scans must be fully authenticated. Add additional rows as necessary.*

*In lieu of filling out this table, CSPs may embed a separate file or refer to Appendix D, as long as all required information is included. In addition, CSPs may use any unique identifier (e.g. MAC address or hostname), instead of the IP address.*

|  |  |  |  |
| --- | --- | --- | --- |
| Database Name | Hostname | IP Address | Additional Info |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 2-5 – Databases Slated for Testing

* 1. Roles Slated for Testing

Role testing will be performed to test the authorizations restrictions for each role. <**3PAO**> will access the system while logged in as different user types and attempt to perform restricted functions as unprivileged users. Functions and roles that will be tested are noted in Table 2-6. Roles slated for testing correspond to those roles listed in Table 9-1 of the <**Information System Name**> System Security Plan.

| Role Name | Test User ID | Associated Functions |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Table 2-6 – Role Based Testing

1. Assumptions

The following assumptions were used when developing this Security Assessment Plan:

*Instruction: The assumptions listed are default assumptions. IA must edit these assumptions as necessary for each unique engagement.*

* <**CSP**> resources, including documentation and individuals with knowledge of the <**CSP**> systems and infrastructure and their contact information, will be available to <**3PAO**> staff during the time necessary to complete assessments.
* The <**CSP**> will provide login account information / credentials necessary for <**3PAO**> to use its testing devices to perform authenticated scans of devices and applications.
* The <**CSP**> will permit <**3PAO**> to connect its testing laptops to the <**CSP**> networks defined within the scope of this assessment.
* The <**CSP** > will permit communication from <**3PAO**> testing appliances to an internet hosted vulnerability management service to permit the analysis of vulnerability data.
* Security controls that have been identified as “Not Applicable” (e.g. AC-18 wireless access) in the System Security Plan will be verified as such and further testing will not be performed on these security controls
* Significant upgrades or changes to the infrastructure and components of the system undergoing testing will not be performed during the security assessment period.
* For onsite control assessment, <**CSP**> personnel will be available should the <**3PAO**> staff determine that either after hours work, or weekend work, is necessary to support the security assessment.

1. Methodology

<**3PAO**> will perform an assessment of the <**Information System Name**> security controls using the methodology described in NIST SP 800-53A. <**3PAO**> will use FedRAMP supplied test procedures to evaluate the security controls. Contained in Excel worksheets, these test procedures contain the test objectives and associated test cases to determine if a control is effectively implemented and operating as intended. The results of the testing shall be recorded in the worksheets (provided in Appendix B) along with information that notes whether the control (or control enhancement) is satisfied or not.

*Instruction: FedRAMP provides a documented methodology to describe the process for testing the security controls. IAs may edit this section to add additional information.*

<**3PAO**> data gathering activities will consist of the following:

* Request <**CSP**> to provide FedRAMP required documentation
* Request any follow-up documentation, files, or information needed that is not provided in FedRAMP required documentation
* Travel to the CSP sites as necessary to inspect systems and meet with CSP staff
* Obtain information through the use of security testing tools

Security controls will be verified using one or more of the following assessment methods:

* Examine: the IA will review, analyze, inspect, or observe one or more assessment artifacts as specified in the attached test cases;
* Interview: the IA will conduct discussions with individuals within the organization to facilitate assessor understanding, achieve clarification, or obtain evidence;
* Technical Tests: the IA will perform technical tests, including penetration testing, on system components using automated and manual methods.

<**3PAO**> <**will or will not**> use sampling when performing this assessment.

Penetration testing methodology is attached in Appendix C.

*Instruction: If sampling methodology is used, attach the sampling methodology in Appendix D.*

1. Test Plan
   1. Security Assessment Team

The security assessment team consists of individuals from <**3PAO**> which are located at <**Address of 3PAO**>. Information about <**3PAO**> can be found at the following URL: <**insert URL**>.

*Instruction: List the members of the risk assessment team and the role each member will play. Include team members contact information.*

Security control assessors play a unique role in testing system security controls. NIST 800-39, *Managing Information Security Risk* states:

*The security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).*

The members of the IA security testing team are found in Table 5-1.

| Name | Role | Contact Information |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Table 5-1 – Security Testing Team

* 1. CSP Testing Points of Contact

The CSP points of contact that the testing team will use are found in Table 5-2.

*Instruction: The IA must obtain at least three points of contact from the CSP to use for testing communications. One of the contacts must be available 24 x 7 and must include an operations center (e.g. NOC, SOC).*

| Name | Role | Contact Information |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Table 5-2 – CSP Points of Contact

* 1. Testing Performed Using Automated Tools

<**3PAO** > plans to use the following tools noted in Table 5-3 to perform testing of the <**Information System Name**>.

*Instruction: Describe what tools will be used for testing security controls. Include all product names and names of open source tools and include version numbers. If open source tools are used, name the organization (or individuals) who developed the tools. Additionally, describe the function and purpose of the tool (e.g. file integrity checking, web application scanning). For scanners, indicate what the scanner’s capability is, e.g. database scanning, web application scanning, infrastructure scanning, code scanning/analysis). For more information see the Guide to Understanding FedRAMP.*

| Tool Name | Vendor/Organization Name & Version | Purpose of Tool |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table 5-3 – Tools Used for Security Testing

* 1. Testing Performed Through Manual Methods

*Instruction: Describe what technical tests will be performed through manual methods without the use of automated tools. The results of all manual tests must be recorded in the SAR. Examples are listed in the first four rows. Delete the examples, and put in the real tests. Add additional rows as necessary. Identifiers must be in the format MT-1, MT-2 which would indicate “Manual Test 1” and “Manual Test 2” etc.*

*Penetration tests must be included in this section.*

| Test ID | Test Name | Description |
| --- | --- | --- |
| MT-1 | Forceful Browsing | We will login as a customer and try to see if we can gain access to the Network Administrator and Database Administrator privileges and authorizations by navigating to different views and manually forcing the browser to various URLs. |
| MT-2 | SQL Injection | We will perform some manual SQL injection attacks using fake names and 0 OR '1'='1' statements. |
| MT-3 | CAPTCHA | We will test the CAPTCHA function on the web form manually. |
| MT-4 | OCSP | We will manually test to see if OCSP is validating certificates. |
|  |  |  |

Table 5-4 – Testing Performed Through Manual Methods

* 1. Schedule

The security assessment testing schedule can be found in Table 5-5.

*Instruction: Insert the security assessment testing schedule. This schedule must be presented to the CSP by the IA at the kick-off meeting. The ISSO must be invited to the meeting that presents the schedule to the CSP. After being presented to the CSP at the kick-off meeting, the IA must make any necessary updates to the schedule and this document and send an updated version of the CSP, copying the ISSO.*

| Task Name | Start Date | Finish Date |
| --- | --- | --- |
| Kick-off Meeting |  |  |
| Prepare Test Plan |  |  |
| Meeting to Review Test Plan |  |  |
| Test Plan Update |  |  |
| Review CSP Documentation |  |  |
| Conduct Interviews of CSP Staff |  |  |
| Perform Testing |  |  |
| Vulnerability Analysis and Threat Assessment |  |  |
| Risk Exposure Table Development |  |  |
| Complete Draft SAR |  |  |
| Draft SAR Delivered to SAP |  |  |
| Issue Resolution Meeting |  |  |
| Complete Final Version of SAR |  |  |
| Send Final Version of SAR to CSP and ISSO |  |  |

Table 5-5 – Testing Schedule

1. Rules of Engagement

A Rules of Engagement (ROE) is a document designed to describe proper notifications and disclosures between the owner of a tested systems and an independent assessor. In particular, a ROE includes information about targets of automated scans and IP address origination information of automated scans (and other testing tools). Together with the information provided in preceding sections of this document, this document shall serve as a Rules of Engagement once signed.

Disclosures

*Instruction: FedRAMP provides a Rules of Engagement template. IAs must edit this ROE as necessary. The final version of the ROE must be signed by both the IA and CSP.*

Any testing will be performed according to terms and conditions designed to minimize risk exposure that could occur during security testing. All scans will originate from the following IP address(es): <**IP addresses**>.

*Instruction: Edit and modify the disclosures as necessary.* *If testing is to be conducted from an internal location, identify at least one network port with access to all subnets/segments to be tested. The purpose of identifying the IP addresses from where the security testing will be performed is so that when IAs are performing scans, the CSP will understand that the rapid and high volume network traffic is not an attack and is part of the testing.*

* + 1. Security testing May Include

Security testing may include the following activities:

*Instruction: IA must edit the bullets in this default list to make it consistent with each unique system tested.*

* Port scans and other network service interaction and queries
* Network sniffing, traffic monitoring, traffic analysis, and host discovery
* Attempted logins or other use of systems, with any account name/password
* Attempted SQL injection and other forms of input parameter testing
* Use of exploit code for leveraging discovered vulnerabilities
* Password cracking via capture and scanning of authentication databases
* Spoofing or deceiving servers regarding network traffic
* Altering running system configuration except where denial of service would result
* Adding user accounts
  + 1. Security Testing Will Not Include

Security testing will not include any of the following activities:

*Instruction: IA must edit the bullets in this default list to make it consistent with each unique system tested.*

* Changes to assigned user passwords
* Modification of user files or system files
* Telephone modem probes and scans (active and passive)
* Intentional viewing of <**CSP**> staff email, Internet caches, and/or personnel cookie files
* Denial of Service attacks
* Exploits that will introduce new weaknesses to the system
* Intentional introduction of malicious code (viruses, Trojans, worms, etc.)
  1. End of Testing

<3PAO> will notify <Name of Person> at <CSP> when security testing has been completed.

* 1. Communication of Test Results

Email and reports on all security testing will be encrypted according to <**CSP**> requirements. Security testing results will be sent and disclosed to the individuals at <**CSP**> noted in Table 6-1 within <**number**> days after security testing has been completed.

| Name | Role | Contact Information |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Table 6-1 – Individuals at CSP Receiving Test Results

* 1. Limitation of Liability

<**3PAO**>, and its stated partners, shall not be held liable to <**CSP**> for any and all liabilities, claims, or damages arising out of or relating to the security vulnerability testing portion of this Agreement, howsoever caused and regardless of the legal theory asserted, including breach of contract or warranty, tort, strict liability, statutory liability, or otherwise.

*Instruction: Insert any Limitations of Liability associated with the security testing below. Edit the provided default Limitation of Liability as needed.*

<**CSP**> acknowledges that there are limitations inherent in the methodologies implemented, and the assessment of security and vulnerability relating to information technology is an uncertain process based on past experiences, currently available information, and the anticipation of reasonable threats at the time of the analysis. There is no assurance that an analysis of this nature will identify all vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate all exposure.

* 1. Signatures

The following individuals at the IA and CSP have been identified as having the authority to agree to security testing of <**Information System Name**>.

ACCEPTANCE AND SIGNATURE

I have read the above Security Assessment Plan and Rules of Engagement and I acknowledge and agree to the tests and terms set forth in the plan.

IA Representative: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (printed)

IA Representative: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature) \_\_\_\_\_\_\_\_\_\_\_ (date)

CSP Representative: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (printed)

CSP Representative: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (signature) \_\_\_\_\_\_\_\_\_\_\_ (date)

Appendix A – Acronyms

|  |  |
| --- | --- |
| **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 |
| FedRAMP | Federal Risk and Authorization Management Program |
| FIPS PUB | Federal Information Processing Standard Publication |
| FISMA | Federal Information Security Management Act |
| GSS | General Support System |
| IaaS | Infrastructure as a Service (Model) |
| IATO | Interim Authorization to Operate |
| ID | Identification |
| IA | Independent Assessor (3PAO) |
| IT | Information Technology |
| LAN | Local Area Network |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PIA | Privacy Impact Assessment |
| 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 |

Appendix B – Test Case Procedures

Results of the attached security test case procedures shall be recorded directly in each respective workbook.

NOTE: The Test Case Procedures are currently in text format on FedRAMP.gov and will be available in workbook format by October 1, 2014.

Appendix C – Penetration Testing Plan and Methodology

*Instruction: CSPs may embed a file containing the plan or include the plan in this section.*

Appendix D – Attachments

*Instruction: If applicable, attachments must include penetration testing rules of engagement, penetration testing methodology, and the sampling methodology used in testing.*