STATERAMP PENETRATION REQUIREMENTS GUIDE

VERSION:
1.0

DATE:
May 2023

DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
11/22/2022	Policy Draft Submission	1.0	StateRAMP PMO

About This Document

The purpose of this document is to give requirements for Service Providers (SPs) planning to leverage a third-party assessment organization (3PAO) to conduct a StateRAMP penetration test, as well as the associated attack paths and overall reporting requirements.

A penetration test is a proactive and approved exercise to break through the security of an Information Technology (IT) system. The main objective of a penetration test is to identify vulnerable security weaknesses in an information system. These vulnerabilities may include service and application flaws, insecure configurations, improper role-based privilege assignments, and risky end-user behavior. A penetration test may also assess an organization's security policy compliance, its employees' security awareness, and the organization's ability to identify and respond to security incidents. Threat actors work diligently to bypass initial system defenses. Penetration testing ensures that the depth of defense goes beyond early compromise and/or considers whether IT security best practices such as patch management and secure coding practices are being followed.

Zero Trust Protection mechanisms should be defined as part of the system boundary and are better addressed and included in the SSP front matter discussions.

The term authorization refers to an SP's approval status with StateRAMP which could either be "Ready", "Approved" or "Authorized"..

The term third-party assessment organization (3PAO) refers to a StateRAMP recognized 3PAO. The use of a StateRAMP recognized 3PAO is required for systems with a StateRAMP ; however, for systems

with a StateRAMP this may refer to any assessment organization designated by the agency AO.

Who Should Use This Document?

The following **individuals should review this document:**

- Service Providers (SPs) when preparing to perform a penetration test on their cloud system
- Third Party Assessment Organizations (3PAOs) when planning, executing, and reporting on StateRAMP penetration testing activities
- AOs when developing and evaluating penetration test plans.

How to Contact Us

Questions about StateRAMP or this document should be directed to https://stateramp.org/contact/

For more information about StateRAMP, visit https://stateramp.org/

TABLE OF CONTENTS

Scope of Testing

- The State Risk and Authorization Management Program (StateRAMP) requires that penetration testing be conducted in compliance with the following guidance:
    - **STATERAMP VULNERABILITY SCAN REQUIREMENTS GUIDE**
    - **STATERAMP READY MINIMUM MANDATORY REQUIREMENTS FOR LOW IMPACT LEVEL**
    - **STATERAMP READY MINIMUM MANDATORY REQUIREMENTS FOR MODERATE AND HIGH IMPACT LEVELS**
    - **STATERAMP SECURITY CONTROLS BASELINE SUMMARY**
    - **STATERAMP CONTINUOUS MONITORING GUIDE**
- StateRAMP also requires that an SP's productan third-party assessment and penetration test must be classified as a SaaS, PaaS, and/or IaaS (see definitions in Table 2). In some scenarios, it may be appropriate to apply multiple cloud service models to a cloud service.

Table 2: Cloud Service Classification

Cloud Service Model	NIST Description (Current Revision)
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin-client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment

Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly limited control of select networking components (e.g., host firewalls).

- In the final Penetration Test Plan, all components, associated services, and access paths (internal/external) within the defined test boundary of the SP's system must be scoped and assessed. A set of attack paths will be required, regardless of classification (SaaS, IaaS, PaaS, or hybrid) and is outlined in Section 3.1. SPs will work, in coordination with their 3PAO, to identify and scope-in other attack paths prescribed in this guidance. Any deviations from the mandatory or scoped-in attack paths must be approved by an Authorizing Official (AO). The Rules of Engagement (ROE) must identify and define the appropriate testing method(s) and techniques associated with exploitation of the relevant devices and/or services.
- The Penetration Test Plan must address all attack paths described in Section 3 or explain why a particular attack path was deemed out of scope or not applicable. 3PAOs may include additional attack paths they believe are appropriate based on the cloud service offering being assessed. See Appendix D: Rules of Engagement (ROE)/Test Plan Template for more information regarding test plans.

Threats

- SPs should consult with their 3PAO to derive the most efficient and effective risk profiling for their cloud service offering (CSO).

2.0. Threat Models

Penetration testing conducted by a 3PAO should follow multiple threat models developed to align with current adversarial tactics and techniques. These threat models are built into each attack path to ensure real-world threats and risks are analyzed, assessed, mitigated, and accepted by an authorizing authority. 3PAOs should **assess the risk and security of a SP minimally through the following threat models:**

- **Internet based (Untrusted)**
  - *Network threat actor*
  - *Attack on SP managed user*

- *Email attack against SP managed user*
- *Application threat actor*
- *Physical based attack*

- **SP Corporate (Untrusted and Trusted)**
  - *Breach of SP management systems*
  - *Breach of SP managed support system and/or networks*
  - *Breach of SP managed enclave of authorized systems*
  - *Corporate insider threat*
  - *Lost SP managed system*
  - *Interconnected networks including international entities, foreign adversaries internally pivoting to US CSO enclave*
  - *Ransomware spread from SP*
  - *Unauthorized physical access to authorized system*
- **Internal Threat (Untrusted and Trusted)**
  - *Weak permissions and access control*
  - *Abuse of services of authorized system*
  - *Ransomware spread from government system*
  - *Multi organization access to authorized system*
  - *Unauthorized physical access to authorized system*

If a 3PAO determines additional threat models are warranted to provide an adequate assessment, a SP must be willing to consider what the 3PAO recommends. If a 3PAO and SP cannot come to terms, and an AO determines that this additional testing should be performed, this may extend a SP's time to StateRAMP authorization.

2.1. Attack Models

Depending on the authorized service architecture (IaaS, PaaS, SaaS, hybrid), all or some attack models may be applicable. Additionally, attack models may be tested in different or multiple ways, and testers are required to demonstrate the ability to exploit vulnerabilities or verify exploits when not feasible. The penetration test should not be strictly limited to automated scanning techniques, but the usage of manual techniques should be incorporated as well.

A 3PAO's penetration testing methodology and report should provide an AO with a clear picture of attack models leveraged against the authorized system. The report should outline the specific attack narratives of verification and validation of vulnerabilities identified during testing. This requirement will ensure that the

approach and attack models were properly met. While not a comprehensive list, the **goal of penetration testing should be to attain all the following, per the MITRE ATTACK®[1] knowledge base:**

- Enterprise
    - Reconnaissance
    - Resource Development
    - Initial Access
    - Execution
    - Persistence
    - Privilege Escalation
    - Defense Evasion
    - Credential Access
    - Discovery
    - Lateral Movement
    - Collection
    - Command and Control
    - Exfiltration
    - Impact
- Mobile
    - Initial Access
    - Execution
    - Persistence
    - Privilege Escalation
    - Defense Evasion
    - Credential Access
    - Discovery
    - Lateral Movement
    - Collection
    - Command and Control
    - Exfiltration
    - Impact
    - Network Effects
    - Remote Service Effects

StateRAMP realizes that the goal of testing to attain all the above is not feasible for every CSO. It is up to SPs and 3PAOs to determine the tactics and techniques that most assuredly could affect the particular

[1] https://attack.mitre.org/matrices/enterprise/cloud/

system. StateRAMP relies extensively on a 3PAO's penetration testing expertise to identify and test the most applicable tactics that would be adopted by a malicious actor. 3PAOs should explain the rationale for choosing the specific penetration testing tactics for the system. A SP should be aware that an AO may ask for additional testing during the review if common tactics for a CSO are not tested. This can delay the time for StateRAMP authorization.

3.0. Attack Paths

Attack paths are defined as potential ways of compromise that may lead to a loss or degradation of system confidentiality, integrity, or availability. StateRAMP has identified and developed several risk scenarios for 3PAOs to review and address during penetration testing. SPs and 3PAOs should agree on the attack paths. If a specific attack path cannot be performed, the deviation must be included in the Security Assessment Report (SAR) as a deviation from the Penetration Testing Guidance. SPs must understand that a 3PAO might see non-conformance to testing a particular attack path as a High Risk finding in the SAR Risk Exposure Table (RET). If a SP feels strongly that testing the attack path may result in a significant negative impact to the production system, then the SP is encouraged to submit a non-conformance justification for why a 3PAO-recommended attack path cannot be tested, to an AO. SPs and 3PAOs must both be aware that any deviations or non-conformance to established guidance may result in a longer time to StateRAMP authorization due to the time required for an AO to understand and agree to the deviation or non-conformance.

3.1 Mandatory Attack Paths

Techniques to test each system may vary depending on the service offering (IaaS, PaaS, SaaS, and Hybrid). Due to system commonalities, the following are **mandatory attack paths for all authorized systems:**

- **External to Corporate**
- **External to SP Target System**
- **Tenant to SP Management System**
- **Tenant to Tenant**
- **Mobile Application to Target System**
- **Client-side Application and/or Agents to Target System**

3.1.1 Attack Path 1: External to Corporate

The External to Corporate attack path requires the execution of a social engineering (phishing) attack against a SP's system administrators, and managing personnel who may influence system

administrators. If sampling is performed, it must be documented in the ROE and approved by an AO prior to test execution. An attackers' originating IPs and email domains will be allowed on all perimeter security devices such as firewalls, web application firewalls, SPAM filters, and intrusion protection systems.

Email Phish Campaign

A phishing test is a coordinated assessment between a 3PAO and SP. The intent is to test user compliance, not email security. Users are the last line of defense and should be tested. Emails should be allow-listed on all security systems and be presented to the user unflagged, unmodified, and unaltered in any way.

3PAOs must coordinate with SP security teams to ensure testing is not manipulated in any way. SP users that are in-scope for this attack path are all users with access to SP management, authorized systems, applications, or support systems. Additionally, any system administrators with privileged level access to SP management endpoints should be considered in-scope of this assessment.

Landing pages for SP personnel who are victims of the phishing attack should immediately identify that the 3PAOs are authorized to coordinate with SPs to utilize established user phishing programs to facilitate testing. 3PAOs will provide or approve email templates and landing pages used in testing. 3PAOs must either perform this attack path themselves, or independently evaluate the effectiveness of a third-party phishing campaign.

email was a phish and provide supplemental information on how to identify phishing attacks in the future.

The email campaign will consist of the following:

- Email with username in body
- Link to landing page
- Ability to capture emails opened (hidden pixel)
- Landing page
- Ability to tie landing page visits by user
- Username and password capture
- Ability to track user submission

False positives created by SP security systems, e.g., sandboxing and link clicking, are to be included in totals due to requirements of SPs to bypass these protections. 3PAOs should not keep credentials and must destroy them after the test due to privacy and security risks. StateRAMP requires that the 3PAO report back roles and/or metrics but not specific names. SPs should also require all passwords changed post-test. Any data submitted to the application, real or not, is to be considered a failure of the test.

System of measurement for failures and severity can be based on the most current Common Vulnerability Scoring System (CVSS) and the 3PAO expertise. For instance, the number of clicks and credential submissions should be reported along with the 3PAO justification for the scoring.

Non-Credentialed-Based Phishing Attack

Determine if a user can run an untrusted PowerShell or Bash script. In this type of attack, the scripts could gather the local username and hostname of the machine and send the payload back to a 3PAO server.
This shows that remote code execution is possible. 3PAOs are not required to capture credentials but should track items such as when the script was run, under what circumstances was it run, and the role allowed to run it. Credential harvesting is not the goal of the phishing attack. If successful or not successful, a 3PAO can provide evidence of a macro or script execution in lieu of credentials.

3.1.2. **Attack Path 2:** External to SP Target System

The External to SP Target System attack path simulates and tests vulnerabilities from external threat actors and untrusted Internet-based attacks; internal threats such as weak permissions/access controls and abuse of system services; and poor customer separation measures (e.g., improper network segmentation and poor implementation of security controls).

Internal Threats

CISA states that "Insider threats present a complex and dynamic risk affecting the public and private domains of all critical infrastructure sectors."[2] Insider threats are unintentional or intentional. CISA defines the unintentional and intentional threats very clearly. These threats are synopsized here for ease of use.

Unintentional Threat (Negligence, Accidental)

Human beings are one of the biggest threat paths to any computing device. Human beings are at times impatient, careless, tired, make mistakes, and procrastinate.

Negligence is the failure to exercise reasonable care or due diligence. Most insider threats are the result of actions by people who understand the reason for physical and logical security. These people think security is for the lesser population and deliberately choose to ignore basic security principles. For instance, these people may choose to ignore a security update because it is inconvenient.

Accidental threats are mostly carried out mistakenly but can be the result of a negligent event. We look at accidental threats as caused by those people who mistakenly introduce a threat to an organization. Mainly, this accidental threat happens because a person does not understand security principles and applications. For instance, this type of person may not understand privacy data and could send a list of employee Social Security Numbers as an unencrypted attachment to an external email. Or this might be because a person unknowingly forwards an email thread with sensitive company data to a business competitor. This type of person may love to forward email attachments or jokes to others and not realize that the attachment contains malware.

Intentional Threats

Intentional threats are purposefully harmful to another person or an organization. These threats are the result of malcontents or disgruntled employees. Dissidents cause issues because they seek to disrupt life in general because of some internal rebellion. Disgruntled employees may cause issues because they feel they were treated unfairly.

[2] https://www.cisa.gov/defining-insider-threats

These types of people may try to sabotage equipment, or inflict other types of disruptions and violence. Other people may steal proprietary data or intellectual property in the false hope of advancing their career.

Other Threats

Additional threats include collusion, third-party actors, and direct and indirect threats. 3PAOs and SPs are urged to consider each type of insider threat and determine how to best test the CSO to minimize these threats.

Poor Separation Measures and Defense In Depth

Applications and systems currently exposed to the public internet should be tested and risk-assigned based on the footprint provided as part of the external boundary of the information system. Application, API, and services testing should be done in sessions or a "less than ideal scenario" where all external endpoints are known to an attacker. Additionally, all passive or active blocking security devices, such as web application firewalls and or software-based security controls, will be bypassed to facilitate testing. "Attack Path 2" may be tested along with "Attack Path 3" and "Attack Path 4", if all attack scenarios are covered, and user/management experiences do not differ. 3PAOs are also required to elevate risk ratings higher for compromise scenarios originating from public access.

- **IaaS** – Testing should originate from public internet attacking exterior IPs or URLs used to host or manage authorized systems. This should include out-of-band, break glass, VPNs, or site-to-site connection interfaces (non-authenticated). 3PAOs should take into consideration corporate shared services and systems and the direct or indirect impact exploitation of these may have on Federal Government data and metadata. These systems usually reside on SP "corporate networks" and the interconnections should be assessed due to their impact on the accredited system.
- **PaaS** – Testing should originate from public internet attacking exterior IPs or URLs used to host and manage authorized systems and within the application or applicable database.
- **SaaS** – Testing should originate from public internet attacking exterior IPs or URLs used to host and manage authorized systems and within the application or applicable database.

3.1.3. **Attack Path 3:** Tenant to SP Management System

This Tenant to SP Management System attack path simulates and tests vulnerabilities, untrusted internal threats, and trusted internal threats that emanate from network threat actors, application threat actors, and abuse of services of the authorized system.

This attack path is performed by conducting a full application test attempting to access SP management systems due to misconfiguration, flaw in system design, abuse of intended function, low-code or no-code software deployment, and/or command line interface (CLI) that allows access to the SP management zone.

Privileged and Unprivileged Users

SPs will provide privileged level accounts to applications within the production environment to facilitate and identify scenarios where the attacker may go from unauthenticated access to authenticated access to privileged level access. All Tenant to SP Management System attacks is to be conducted using the highest level of permissions available to customer users of the information system. The intent is to identify any opportunity that privileged customer accounts would have to compromise the underlying system architecture.

While cloud providers may prefer to evaluate a tenant within the development/test environments, these are rarely identical to the production deployment, and will not be used as a valid representation for the 3PAO penetration test paths. A SP's production environment should be sufficiently resilient to sustain a 3PAO penetration test.

- **IaaS** – Testing should originate from hosted Virtual Private Cloud (VPC) service, server, or platform. Agents, APIs, and applications that allow for communications between tenant space and infrastructure or platform layers are in scope to ensure host compromise is limited to VPC or platform.
- **PaaS** – Testing should originate from the platform provided and attempt to gain access to lower-level PaaS management systems or IaaS level systems. Due to inherent PaaS customizations and modifications (based on the Service Level Agreement [SLA]), the probability that the PaaS implementation may affect the security of underlying IaaS is high. Automated code deployment tools or CLIs to deploy SaaS solutions are considered in-scope and are required to be tested.
- **SaaS** – Testing should originate from an application, API, or CLI if provided as a tool that is presented as part of an authorized system.

3.1.4. **Attack Path 4:** Tenant-to-Tenant

This attack path simulates and tests vulnerabilities from untrusted internal threats and trusted internal threats that emanate from issues such as ransomware spread from state government and multi organization access to the authorized system.

This attack path is performed by conducting a full application test which attempts to use provisional access of one tenant to compromise another tenant. Environments are required to be set up to test all aspects of the service provided, to include authentication, data access, user permissions, and sessions. Access to the cloud service offering should mirror the methods used by system customers. 3PAOs should be provisioned with two full production customer tenants for performing the Tenant-to-Tenant attack path.

3.1.5. **Attack Path 5:** Mobile Application to Target System

The Mobile Application to Target System attack path consists of emulating a mobile application user attempting to access a SP target system or SP management system. This attack path is tested on a representative mobile device and does not directly impact a SP target system or infrastructure.
Information derived from this activity can be used to inform testing of other attack paths. If a mobile application is not part of a SP's CSO, then this attack path can be marked as out-of-scope.

3.1.6 **Attack Path 6:** Client-side Application and/or Agents to Target System

For this attack path, if a SP provides client-side components (i.e., components installed locally within a customer environment), those components must be included in the SP's authorization boundary and tested as part of a SP's system boundary security assessment if the components are essential for their customer's use of their CSO. Such client-side applications or components may include (though not exclusively) software applications, servers, appliances, browser extensions, thick clients, and agents. If a SP provides optional-use, client-side components, such components may be included in the SP's tested authorization boundary, if agreed upon between the SP and customer.

SPs should include in their SSP, and 3PAOs in their testing, any controls out of a customer's ability to remediate such as encryption and software development. It is recognized that many of these controls will have a significant customer responsibility. These shared responsibilities should be clearly called out in the SSP and assessed by a 3PAO.

StateRAMP encourages inclusion of optional-use components within a SP's tested boundary as it reduces the burden on customers for component assessment, authorization, and continuous monitoring.

When scoping the system boundaries for the assessment, it is important to consider the legal ramifications of performing penetration testing activities on third-party environments. All testing activities must be limited to the in-scope test boundary for the system to ensure adherence to all agreements and to limit legal liability. Penetration testing should not be performed on assets for which permission has not been explicitly documented. Obtaining permissions for any third-party assets are required to be in-scope and are a SP's responsibility.

4.0. Scoping the Penetration Test

The authorization boundaries of a proposed cloud service will be initially determined based on the SSP and attachments. It should clearly defined in an SSP the authorization boundaries of the cloud system reflected in a diagram and in words. During penetration test scoping discussions, individual system components will be reviewed and deemed as "in-scope" or "out-of-scope" for the penetration test. The aggregate of the agreed upon and authorized in-scope components will comprise the system boundary for the penetration test.

When scoping the system boundaries for an assessment, it is important to consider the legal ramifications of performing penetration testing activities on third-party environments. All testing activities must be limited to the in-scope test boundary for the system to ensure adherence to all agreements and to limit legal liability. Penetration testing should not be performed on assets for which permission has not been explicitly documented. Obtaining permissions for any third-party assets are required to be in-scope and is a SP's responsibility.

Service models intending to use StateRAMP Authorized services lower in the "cloud stack" can leverage the StateRAMP compliance and security features of those services. As a result, attack paths already addressed by other StateRAMP Authorized services lower in the "cloud stack" are not required to be re-evaluated. For example, if a PaaS and SaaS leverage another layer (i.e., IaaS) that is StateRAMP Authorized, then penetration testing of the lower layer is not required. However, a SP must determine the authorization system boundaries and provide justification for any controls they intend to claim as inherited from the supporting service. If the PaaS and/or SaaS are including StateRAMP Authorized security features for the lower layers, then penetration testing of the lower layers is required, and a SP needs to obtain all the authorizations required for a 3PAO to perform penetration testing for the lower layers.

Penetration testing may require:

- Negotiation and agreement with third parties such as internet service providers (ISPs), managed security service providers (MSSPs), facility leaseholders, hosting services, and/or other organizations involved in, or affected by, the test. In such scenarios, a SP is responsible for coordination and obtaining approvals from third parties prior to the commencement of testing.
- When a cloud system has multiple tenants, SPs must build a temporary tenant environment if another tenant environment suitable for testing does not exist. Use of production to development instances to meet multi-tenancy may be used if a 3PAO validates attack paths and models are effectively tested.

5.0 Rules of Engagement (ROE)

The penetration test plan must include:

- A description of the approach, constraints, and methodologies for each planned attack.
- A detailed test schedule that specifies the start and end date/times and content of each test period and the overall penetration test beginning and end dates.
- Technical points of contact (POC) with a backup for each subsystem and/or application that may be included in the penetration test.

The penetration test ROE describes the target systems, scope, constraints, and proper notifications and disclosures of the penetration test. 3PAOs develop a ROE based on the parameters provided by a SP. The

ROE must be developed in accordance with NIST Special Publication (SP) 800-115, Appendix C, and be approved by an AO prior to testing. Additionally, NIST SP 800-115, Section 7, Security Assessment Execution states, "appropriate personnel such as the CIO, CISO, and ISSO are informed of any critical high-impact vulnerabilities as soon as they are discovered." StateRAMP requires that the ROE must contain this clause and include the AO, in addition to the CIO, CISO, and ISSO. See Section 6, Rules of Engagement, of the StateRAMP Security Assessment Plan Template for more information on the ROE. 3PAOs must include a copy of the ROE in the StateRAMP Security Assessment Plan submitted to StateRAMP.

The ROE should also include:

- Local computer incident response team or capability and their requirements for exercising the penetration test
- Physical penetration constraints
- Acceptable social engineering pretext(s) to be fully worked out prior to the ROE being signed. Note:
    - Social engineering tests are based upon a 3PAO's expertise in challenging a SP's users' failures to follow documented CSO policies and procedures
    - Can be evaluated against the effectiveness of a SP's security awareness and training program
    - There is no "one size fits all" social engineering testing. 3PAOs should consider the threats, at the time of testing, and incorporate these methods, as applicable, into their penetration testing methodology.

A summary and reference to any third-party agreements, including POCs for third parties that may be affected by the penetration test and must be included in the documentation. The time to authorization will be extended if the additional testing is required to be done based on an AOs review and prior to StateRAMP authorizing the package. 3PAOs are required to fully document, in the Penetration Testing Report section 6.0, the rationale behind a SP not agreeing to a social engineering test. Also, SPs are encouraged to report to StateRAMP any proposed 3PAO penetration testing exercises that seem too severe given the nature of the CSO being offered.

6.0. Reporting

Penetration test assessment activities and results must be organized and compiled into a comprehensive penetration test report to be included in the SAR. There is no template provided for the penetration test report.

The penetration test report should include appropriate confidentiality and sensitivity markings in compliance with a SP's organizational policy. 3PAOs should provide the report to a SP via a secure means in compliance with the SP organization's policies. Any information included in the report that could contain sensitive data (screenshots, tables, figures) must be sanitized, or masked, using techniques that render the sensitive data permanently unrecoverable by recipients of the report. 3PAOs must not include passwords (including those in encrypted form) in the final report or must mask them to ensure recipients of the report cannot recreate or guess the password.

The report is required to address the following sections, but not necessarily in this order:

6.1. Scope of Target System

Outline the target system that was assessed and if any deviations were made from the ROE/TP document.

6.2. Attack Paths Assessed During the Penetration Test

Describe the attack path(s) tested and the threat model(s) followed for executing the penetration test.

6.3. Timeline for Assessment Activity

Document when penetration testing activity was performed.

6.4. Actual Tests Performed and Results

Document the actual tests performed to address the penetration test requirements outlined in this document and document the results of each test.

6.5. Findings and Evidence

Findings should include a description of the issue, the impact on the target system, a recommendation to the SP, a risk rating, and relevant evidence to provide context for each finding.

6.6. Access Paths

Access paths are the chain of attack paths, exploitations, and post-exploitations that lead to a degradation of system integrity, confidentiality, or availability. 3PAOs must describe the access path and the penetration test impact if multiple vulnerabilities could be coupled to form a sophisticated attack against a SP.

7.0. Testing Schedule Requirements

For each initial security authorization, a penetration test must be completed by a 3PAO as a part of the assessment process described in the SAP. This initial penetration test must be performed no more than 6 months prior to the submission of the SAR. Once within the continuous monitoring phase of the StateRAMP process, additional penetration testing activities must be performed **at least every 12 months**, unless otherwise approved by an authorizing body with documented rationale.

Appendix A: Definitions

The following is a **list of definitions for this document:**

- **Attack Path** – A prescribed attack scenario based on attack models and real-world threats.
- **Service Provider (SP)** – The entity responsible for the deployment, maintenance, and security of the authorized system.
- **Cloud Service Offering (CSO)** – The service, platform or capability that is being offered and accredited by the government customer.
- **Corporate** – An internal SP network accessed outside the authorization boundary. This corporate boundary includes all resources owned, operated, maintained by the SP to administer services of the system. This includes networks, laptops, mobile phones, systems that touch any part of the authorized system.
- **SP Management System** – The backend applications, systems, services, hardware, infrastructure, or out of band management that facilitates administrative access to the cloud service. The management system is the support infrastructure only accessible to SP personnel and authorized individuals.
- **Insider Threat** – An individual that is an employee, contractor, government employee or third party with access to a corporate or authorized system with malicious intent.
- **Microservices** – The capabilities provided or used to provide services.
- **Penetration Test** – A combination of automated and manual testing of technical security controls.
- **Target** – The intended product being offered to the government customer.
- **Tenant** – A customer instance of a cloud service.

Appendix B: References

The publications referenced in this document are **available at the following URLs:**

- StateRAMP Documents and Templates: https://stateramp.org/templates-resources/
- NIST Special Publication (SP) 800-115 Technical Guide to Information Security Testing and Assessment: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
- NIST SP 800-53 Current Revision Security and Privacy Controls for Federal Information Systems and Organizations: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST SP 800-145 The NIST Definition of Cloud Computing: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- MITRE ATTGCK® Matrix for Enterprise: https://attack.mitre.org/matrices/enterprise/cloud/

Appendix C: Rules of Engagement / Test Plan Template

Rules of Engagement / Test Plan

The Penetration Test Rules of Engagement (ROE) and Test Plan (TP) documents describe the target systems, scope, constraints, and proper notifications and disclosures of the Penetration Test. 3PAOs are required to develop a ROE and TP based on the parameters and system information provided by a SP.

The ROE and TP document must be developed in accordance with NIST SP 800-115, Appendix B, and be approved by an AO prior to testing. 3PAOs must include a copy of the ROE in the StateRAMP Security Assessment Plan submitted to StateRAMP.

Penetration test planning **must include or account for the following considerations:**

- Penetration
    - Network penetration
    - Wireless network penetration
    - Physical penetration
    - Social engineering penetration
- Affected IP ranges and domains
- Acceptable social engineering pretexts
- Targeted organization's capabilities and technology

- Investigative tools
- Specific testing periods (start and end date/times)
- SP reporting requirements (format, content, media, encryption) The

Penetration Test Plan **must describe:**

- Target locations
- Categories of information such as open-source intelligence, human intelligence
- Type of information such as physical, relationship, logical, electronic, metadata
- Gathering techniques such as active, passive, on- and off-location
- Pervasiveness
- Constraints that do not exploit business relationships (customer, supplier, joint venture, or teaming partners). The CSO control baseline provides the means to thoroughly test these relationships, especially supply chain controls

3PAOa must justify omitting any attack paths described in Section 3 above in the ROE/TP and the Penetration Test Report.

System Scope

Provide a description of the boundaries and scope of the cloud service system, along with any identified supporting services or systems. System scope should account for all Internet Protocol (IP) addresses, Uniform Resource Identifiers (URLs), devices, components, software, and hardware.

Assumptions and Limitations

Provide a description of the assumptions, dependencies, and limitations identified that may have an impact on penetration testing activities or results. Include references to local and federal legal constraints that may be relevant to testing or results. Assumptions also include any assumed agreement, or access to third party software, systems, or facilities.

Testing Schedule

Provide a schedule that describes testing phases, initiation/completion dates, and allows for tracking of penetration test deliverables.

Testing Methodology

The methodology section will address relevant penetration testing activities as described in Section 5, above.

Relevant Personnel

Provide a list of key personnel involved in the management and execution of the penetration test. The list should include, at a minimum:

- System Owner (SP)
- Trusted Agent (SP)
- Penetration Test Team Lead (3PAO)
- Penetration Test Team Member(s) (3PAO)
- Escalation Points of Contact (SP and 3PAO)

Incident Response Procedures

Provide a description of the chain of communications and procedures to be followed should an event requiring incident response intervention be initiated during penetration testing.

Evidence Handling Procedures

Provide a description of procedures for transmission and storage of penetration test evidence collected during the assessment.