STATERAMP PENETRATION TESTING REQUIREMENTS GUIDE

VERSION:

1.0

DATE:

June 2023

DOCUMENT REVISION HISTORY

Date	Description	Version	Governing Body
5/24/2023	Original Publication	1.0	Standards & Technical Committee
6/6/2023	Adopted	1.0	StateRAMP Board of Directors

How to contact us

For questions about StateRAMP, or for technical questions about this document including how to use it, contact *pmo@StateRAMP.org*. For more information about StateRAMP, see www.StateRAMP.org.

TABLE OF CONTENTS

1. PURPOSE

The purpose of this document is to provide guidance for Service Providers (SPs) who are planning to use a third-party assessment organization (3PAO) for conducting a StateRAMP penetration test. It also outlines the attack paths and reporting requirements associated with it.

A penetration test is a proactive and authorized exercise to evaluate the security of an Information Technology (IT) system. The primary objective of a penetration test is to identify security weaknesses and vulnerabilities in an information system. These might include service and application flaws, insecure configurations, improper role-based privilege assignments, and risky end-user behavior. Additionally, a penetration test can assess an organization's compliance with its security policies, its employees' security awareness, and its ability to detect and respond to security incidents.

Threat actors are constantly looking for ways to bypass initial system defenses. Penetration testing ensures that the depth of defense goes beyond early compromise and 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.

2. SCOPE

StateRAMP requires that penetration testing be conducted in compliance with the following guidance:

- *StateRAMP Vulnerability Scan Requirements Guide*
- *StateRAMP Minimum Mandates for Low Impact Level*
- *StateRAMP Minimum Mandates for Moderate and High Impact Levels*
- *StateRAMP Security Controls Baseline Summary*
- *StateRAMP Continuous Monitoring Guide*

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 and is outlined in Section 4.1. 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 the exploitation of the relevant devices and/or services.

The Penetration Test Plan must address all attack paths described in Section 4 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.

3. THREATS

SPs should consult with their 3PAO to derive the most efficient and effective risk profiling for their product.

3.1 THREAT MODELS

To ensure comprehensive penetration testing, a 3PAO should follow various threat models that align with the latest adversarial tactics and techniques. These models are integrated into each attack path to analyze, assess, mitigate, and accept real-world threats and risks under the supervision of an authorizing authority. At a minimum, 3PAOs should evaluate the risk and security of a system or product through the following threat models:

3.1.1 INTERNET-BASED (UNTRUSTED)

- Network threat actors
- Attacks on SP-managed users
- Email attacks against SP-managed users
- Application threat actors
- Physical based attacks

3.1.2 SP CORPORATE (UNTRUSTED AND TRUSTED)

- Breach of SP management systems
- Breach of SP-managed support systems and/or networks
- Breach of SP-managed enclaves of authorized systems
- Corporate insider threats
- Lost SP-managed systems
- Interconnected networks including international entities, and foreign adversaries internally pivoting to US enclaves
- Ransomware spread from SPs
- Unauthorized physical access to authorized systems

3.1.3 INTERNAL THREAT (UNTRUSTED AND TRUSTED)

- Weak permissions and access control
- Abuse of services of authorized systems
- Ransomware spread from government systems
- Multi-organization access to authorized systems
- Unauthorized physical access to authorized systems

If a 3PAO determines additional threat models are warranted to provide an adequate assessment, an SP must be willing to consider what the 3PAO recommends. If a 3PAO and SP cannot come to terms, and a

SLED Authorizing Body or the StateRAMP Approvals Committee (SAC) determines that this additional testing should be performed, this may extend an SP's time to StateRAMP authorization.

3.2 ATTACK MODELS

The applicability of attack models may vary depending on the authorized service architecture. Multiple ways of testing attack models may be used, and testers should be able to demonstrate their ability to exploit vulnerabilities or verify exploits if it's not possible to do so. The penetration test should not solely rely on automated scanning techniques; manual techniques should also be included.

In order to provide StateRAMP and the SLED Authorizing Body or the SAC with a clear understanding of the attack models used against an authorized system, a penetration testing methodology and report should be prepared for a 3PAO. The report should clearly outline the specific attack narratives used to identify and validate vulnerabilities found during testing. This ensures that the approach and attack models were properly met. Although not an exhaustive list, penetration testing should be able to attain all the following guidelines outlined in the MITRE ATTACK® knowledge base:

3.2.1 ENTERPRISE

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

3.2.2 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

It is important for StateRAMP to achieve its testing goals, but StateRAMP understands that this may not be feasible for every product. Therefore, Service Providers and 3PAOs are responsible for determining the tactics and techniques that are most likely to affect a particular system. StateRAMP relies heavily on the penetration testing expertise of the 3PAO to identify and test the most applicable tactics that a malicious actor may adopt. The 3PAO should explain the rationale for selecting the specific penetration testing tactics for the system. A Service Provider should also be aware that a SLED Authorizing Body or the SAC may request additional testing during the review if common tactics for a product are not tested. This may delay the StateRAMP authorization process.

4. ATTACK PATHS

Attack paths are potential ways of compromise that can lead to a loss or degradation of system confidentiality, integrity, or availability. StateRAMP has identified and developed several risk scenarios for 3PAOs. It is important for SPs and 3PAOs to agree on the attack paths and review them during penetration testing. If there is a specific attack path that cannot be performed, the deviation must be included in the Security Assessment Report (SAR) as a deviation from the Penetration Testing Guidance. SPs should understand that not conforming to the testing of a particular attack path may be seen as a high-risk finding in the SAR Risk Exposure Table (RET) by a 3PAO. If a SP believes that testing the attack path may have a significant negative impact on the production system, they are encouraged to submit a non-conformance justification to the StateRAMP PMO for why a 3PAO-recommended attack path cannot be tested. It is important for both SPs and 3PAOs to be aware that any deviations or non-conformance to established guidance may result in longer time for StateRAMP authorization due to the time required for the StateRAMP PMO and the Authorizing Body to understand and agree to the deviation or non-conformance.

4.1 MANDATORY ATTACK PATHS

Techniques to test each system may vary depending on the service offering. 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

4.1.1 ATTACK PATH 1: EXTERNAL TO CORPORATE

To execute an External to Corporate attack, attackers leverage social engineering or phishing attacks on the system administrators or managing personnel of a Service Provider (SP) who can influence the system administrators. If sampling is performed, it must be documented in the Rules of Engagement (ROE) and approved by the StateRAMP PMO before the test execution. The attacker's IP address and email domains will be permitted on all perimeter security devices, such as firewalls, web application firewalls, SPAM filters, and intrusion protection systems.

4.1.1.1 Email Phishing Campaign

Conducting a phishing test involves a coordinated assessment between the 3PAO and an SP. The primary objective of this test is to assess user compliance, not email security. Users are the ultimate defense against phishing attacks and should be regularly tested. Emails used in the test should be allowed on all security systems and be presented to the user without any flags, modifications, or alterations.

3PAOs must coordinate with the SP’s security teams to ensure that the testing process is not manipulated in any way. All SP users with access to management, authorized systems, applications, or support systems are in-scope for this attack. Additionally, system administrators with privileged access to SP management endpoints should also be considered in-scope.

In the event that SP personnel are victimized by the phishing test, the landing pages should immediately identify the 3PAO as an authorized party using user phishing programs for testing purposes. 3PAOs will provide or approve email templates and landing pages used in testing.

3PAOs must either perform the attack themselves or independently evaluate the effectiveness of a third-party phishing campaign.

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 the user
- Username and password capture
- Ability to track user submission

It is important to note that SP security systems, such as sandboxing and link clicking, may generate false positives, but they must still be included in the overall count due to SP requirements. To ensure privacy and security, 3PAOs must not retain credentials and must destroy them after testing. StateRAMP mandates that 3PAOs report roles and metrics only, not specific names. Additionally, SPs should require password changes after each test. Any data, whether real or not, submitted to the application is considered a test failure.

To measure failures and their severity, a system based on the most current Common Vulnerability Scoring System (CVSS) and 3PAO expertise can be used. The number of clicks and credential submissions should be reported, along with the 3PAO's justification for the scoring.

4.1.1.2 Non-Credentialed-Based Phishing Attack

Determining whether a user can execute untrusted PowerShell or Bash scripts is crucial in preventing attacks. These scripts may obtain the local username and hostname of the machine and transmit the payload to a server associated with the attacker. Such attacks demonstrate the possibility of remote code execution.

While it is not necessary for the 3PAO to capture credentials, it is important to keep track of certain details such as when and under what circumstances the script was executed, as well as the role assigned to the user who executed it. It is not the aim of the phishing attack to harvest credentials. Whether successful or not, the 3PAO can provide evidence of script or macro execution as an alternative to credentials.

4.1.2 ATTACK PATH 2: EXTERNAL TO SP TARGET SYSTEM

The External to SP Target System attack path is a simulation and testing process designed to identify vulnerabilities in the system. It tests potential attacks from external threat actors and untrusted Internet-based sources. It also identifies internal threats, such as weak permissions and access controls, abuse of system services, and inadequate customer separation measures. This includes improper network segmentation and poor implementation of security controls.

4.1.2.1 Internal Threats

Insider threats are a complex and ever-evolving risk that affect both public and private domains of all critical infrastructure sectors, according to CISA. These threats can be either intentional or unintentional. CISA has provided clear definitions for both types of threats, which are summarized below for easy understanding.

Unintentional Threat (Negligence, Accidental)
Computing devices face major threats from human beings themselves. This is because humans can often be impatient, careless, tired, make mistakes, and procrastinate.

Negligence is a lack of reasonable care or due diligence. Many insider threats occur due to the actions of individuals who are aware of the need for physical and logical security but disregard basic security principles. For example, some individuals may choose to ignore a security update just because it's inconvenient.

Accidental threats are typically made by mistake, but they can also stem from a negligent event. These threats arise when individuals unknowingly introduce a threat to an organization. Usually, this happens because the person does not have a thorough understanding of security principles and applications. For instance, they may be unaware of privacy data and send an unencrypted attachment via email that includes a list of employee Social Security Numbers. Or they may unknowingly forward an email thread with sensitive company data to a business competitor. Such individuals may also forward email attachments or jokes to others without realizing that it contains malware.

Intentional Threats
Intentional threats refer to harmful actions that are committed purposefully against a person or an organization. These actions are usually carried out by malcontents or disgruntled employees who are unhappy with their situation. Dissidents often cause disruptions as a way of rebelling against the status quo, while disgruntled employees may cause issues because they feel they have been treated unfairly.

These individuals may try to damage equipment or cause other types of disruptions and violence. In some cases, they may also attempt to steal proprietary data or intellectual property in the hopes of advancing their own careers.

Other Threats
Insider threats can come from collusion with third-party actors, direct or indirect threats. To minimize these threats, 3PAOs and SPs should consider each type of insider threat when testing the product.

4.1.2.2 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 be conducted from the public internet, targeting the exterior IPs or URLs that are used to host or manage authorized systems. This includes out-of-band, break glass, VPNs, or site-to-site connection interfaces that are non-authenticated. 3PAOs should consider the impact of exploiting corporate shared services and systems on SLED data and metadata. These systems typically reside on SP "corporate networks," and the interconnections should be assessed due to their impact on the accredited system.

PaaS
Testing should originate from the public internet attacking IPs or URLs used to host and manage authorized systems, including within the application or relevant 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.

4.1.3 ATTACK PATH 3: TENANT TO SP MANAGEMENT SYSTEM

The Tenant to SP Management System attack path is a testing method used to simulate and identify vulnerabilities and threats that can arise from both trusted and untrusted sources within the network. These threats can be caused by network threat actors, application threat actors, and abuse of authorized system services.

This attack path is conducted by performing a comprehensive application test that attempts to access the SP management systems. It aims to identify potential security breaches caused by system design flaws, misconfiguration, misuse of intended function, low-code, or no-code software deployment, and/or unauthorized access through command line interface (CLI) to the SP management zone.

4.1.3.1 Privileged and Unprivileged Users

In order to identify potential security vulnerabilities, Service Providers (SPs) will grant privileged-level accounts to applications within the production environment. This will help to detect scenarios where attackers may attempt to gain access from unauthenticated to authenticated to privileged levels. Any attacks on the Tenant to SP Management System will be conducted using the highest level of permissions available to customer users of the information system. The objective is to identify any opportunities that privileged customer accounts may have to compromise the underlying system architecture.

While cloud providers may evaluate a tenant within the development/test environment, this environment may differ from the production deployment and may not be an accurate representation for the 3PAO penetration test paths. Thus, an SP’s production environment must be resilient enough 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.

4.1.4 ATTACK PATH 4: TENANT-TO-TENANT

This attack path is designed to simulate and test vulnerabilities arising from both untrusted and trusted internal threats. These threats can arise from various issues, such as ransomware spread from SLED and multi-organization access to the authorized system.

To perform this attack path, a full application test is conducted, which attempts to use provisional access of one tenant to compromise another tenant. The testing environment should be set up to cover all aspects of the service provided, including authentication, data access, user permissions, and sessions. Access to the cloud service offering should mirror the methods used by system customers.

In order to test the Tenant-to-Tenant attack path, 3PAOs should be provisioned with two full production customer tenants.

4.1.5 ATTACK PATH 5: MOBILE APPLICATION TO TARGET SYSTEM

The Mobile Application to Target System attack path simulates a mobile application user trying to access an SP target system or management system. This path is tested on a representative mobile device and does not directly impact the SP's target system or infrastructure. The information obtained from this test can be used to inform testing of other attack paths. If a mobile application is not part of an SP's product, then this attack path can be marked as out-of-scope.

4.1.6 ATTACK PATH 6: CLIENT-SIDE APPLICATION AND/OR AGENTS TO TARGET SYSTEM

When an SP offers client-side components, such as software applications, servers, appliances, browser extensions, thick clients, and agents installed locally within a customer's environment, the components must be included in the SP's authorization boundary. If these components are essential for the customer's use of the SP's product, they should be tested as part of the SP's system boundary security assessment. If the SP provides optional-use, client-side components, these may be included in the SP's tested authorization boundary if agreed upon between the SP and the customer.

SPs should include controls in their System Security Plan (SSP), and testers in their testing, that are out of a customer's ability to remediate, such as encryption and software development. Shared responsibilities should be clearly called out in the SSP and assessed by a tester.

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

When scoping the system boundaries for the assessment, the legal ramifications of performing penetration testing activities on third-party environments must be considered. 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. SPs are responsible for obtaining permissions for any third-party assets that are required to be in-scope.

5. SCOPING THE PENETRATION TEST

The authorization boundaries of a proposed cloud service will be initially determined based on the SSP and attachments. The authorization boundary should be clearly depicted in the SSP in both the system description and the Authorization Boundary Diagram. 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 is required to be in-scope and is an SP’s responsibility.

Service models intending to use StateRAMP Authorized services lower in the “cloud stack” can leverage those services' StateRAMP compliance and security features. 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, an 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 include StateRAMP Authorized security features for the lower layers, then penetration testing of the lower layers is required, and an SP needs to obtain all the authorizations required for a 3PAO to perform penetration testing for the lower layers.

When conducting penetration testing, it may be necessary to negotiate and come to an agreement with third parties such as internet service providers (ISPs), managed security service providers (MSSPs), facility leaseholders, hosting services, or other organizations that may be impacted by the testing. In such cases, the SP is responsible for coordinating and obtaining approval from the third parties before beginning the 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. The use of production-to-development instances to meet multi-tenancy may be used if a 3PAO validates attack paths and models are effectively tested.

6. RULES OF ENGAGEMENT (ROE)

The Rules of Engagement (ROE) for penetration testing outlines the target systems, scope, constraints, and proper notifications and disclosures required for the successful execution of a penetration test.

Third Party Assessment Organizations (3PAOs) develop the ROE based on the parameters provided by an SP. To ensure compliance, the ROE must be developed in accordance with NIST Special Publication (SP) 800-115, Appendix C. Additionally, the ROE must include informing appropriate personnel such as the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Information System Security Officer (ISSO) of any critical high-impact vulnerabilities as soon as they are discovered, in line with NIST SP 800-115, Section 7, *Security Assessment Execution*. StateRAMP requires that the ROE must contain this clause and include the SLED AO or the StateRAMP Approvals Committee (SAC), in addition to the CIO, CISO, and ISSO. For more information on the ROE, refer to Section 6, Rules of Engagement, of the StateRAMP *Security Assessment Plan Template*. 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 an SP’s users’ failures to follow documented CSO policies and procedures.
    - Can be evaluated against the effectiveness of an 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 must be included in the documentation. The time to authorization will be extended if additional testing is required to be done based on a review by the SLED Authorizing Body or the SAC 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 an 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.

7. 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 an SP's organizational policy. 3PAOs should provide the report to an 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:

7.1 SCOPE OF TARGET SYSTEM

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

7.2 ATTACK PATHS ASSESSED DURING THE PENETRATION TEST

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

7.3 TIMELINE FOR ASSESSMENT ACTIVITY

Document when penetration testing activity was performed.

7.4 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.

7.5 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.

7.6 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 an SP.

8. 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.

9. 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, and maintained by the SP to administer services of the system. This includes networks, laptops, mobile phones, and 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.

10. 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/

11. APPENDIX C: RULES OF ENGAGEMENT / TEST PLAN TEMPLATE

11.1 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 an ROE and TP based on the parameters and system information provided by an SP.

The ROE and TP document must be developed in accordance with NIST SP 800-115, Appendix B. 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

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

11.2 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.

11.3 ASSUMPTIONS AND LIMITATIONS

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

11.4 TESTING SCHEDULE

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

11.5 TESTING METHODOLOGY

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

11.6 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)

11.7 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.

11.8 EVIDENCE HANDLING PROCEDURES

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