STATERAMP SECURITY SNAPSHOT

CRITERIA & SCORING

VERSION:
1.0

DATE:
November 18, 2022

DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
11 / 15 / 2022	Original Publication	1.0	StateRAMP Standards & Technical Committee

This document will be reviewed at the discretion of the StateRAMP Board at a frequency no less than annually.

1. PURPOSE OF STATERAMP SECURITY SNAPSHOT

The purpose of the StateRAMP Security Snapshot is to provide a simple process for providers to begin their first step on the path to StateRAMP Ready or Authorized and to provide a score to Government to understand the current maturity of the cloud product's security program. The StateRAMP Security Snapshot provides a moment in time of a product's security maturity. StateRAMP recommends a valid Snapshot is not older than 12 months.

2. SECURITY SNAPSHOT CRITERIA & APPLICATION

The intent of the security snapshot criteria is to provide providers a first step toward achieving a verified StateRAMP Security status. The criteria are designed to provide a gap analysis, that goes beyond self-attestation to validate a product's current maturity in relation to meeting the Minimum Mandatory Requirements for StateRAMP Ready, including controls and select additional requirements that would have a significant impact on the state of the system. For example, these include if the IaaS provider is StateRAMP or FedRAMP authorized, or if the solution has already completed a FedRAMP audit but has not completed a Fast Track assessment with the StateRAMP PMO. Additional requirements include incorporation of other audit frameworks common to industry, such as SOC 2, a completed penetration test, and required annual security awareness training.

StateRAMP Security Snapshot provides a risk score that allows governments to reduce the burden of their resources by leveraging the shared service provided by the StateRAMP Program Management Office (PMO). The StateRAMP Security Snapshot can be utilized throughout the procurement process through contract expiration, as governments may utilize the Snapshot to determine the risk associated with products being considered for procurement. The Snapshot may also be used by Governments to assess progress of products once contracted.

3. SECURITY SNAPSHOT SCORING METHODOLOGY

Snapshot scores are derived from a combination of the impact they have on the providers ability to move forward with a StateRAMP assessment, their impact on security, and the insight and information the StateRAMP PMO can provide to the government procurement and security teams. Providers receive higher points for hosting in a StateRAMP Authorized IaaS as the StateRAMP PMO has direct insight into the state of security of the underlying IaaS solution. Additional, but reduced points can be awarded for leveraging a FedRAMP Authorized IaaS or the solution being FedRAMP Authorized; The rationale for reduced points is the lack of insight into continuous monitoring the StateRAMP PMO is able to provide to the government. Similarly, points can be earned for other regulatory compliance frameworks and

penetration tests at a reduced scoring level, as other audit frameworks and penetration tests do not always specify parameters for controls or include a full scope of the boundary required for a penetration test. Finally, due to the overall company impact, annual security awareness training is an additional requirement for increased points as it has a direct impact on the company's security posture. The remaining requirements for scoring at one point each include the StateRAMP minimum mandatory controls. To receive points for each individual criteria, artifacts must be captured by the StateRAMP PMO and verified that they meet the requirements of the criteria in its entirety.

See *Summary of Required Security Controls* on following pages.

Summary of Required Security Controls

ID	Security Maturity Status	Implemented (Yes or No) To be completed by the Program Management Office	Weighted Value
1	Is your product hosted in a StateRAMP Authorized IaaS?		10
2	Is your product hosted in a FedRAMP Authorized IaaS?		5
3	Is your product currently FedRAMP Authorized?		5
4	Has your product completed one of the following audits: SOC 2 Type 2, ISO 27001, CSA STAR, HITRUST within the past 12 months?		5
5	Has your product completed a penetration test within the past 12 months?		5
6	Do you require and provide annual Security Awareness Training for all employees?		5
7	Are modern cryptographic modules consistently used where cryptography is required?		1
8	Can the system support single sign on?		1
9	Does the SP scan for and consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days?		1
10	Does the SP and system utilize an audit and event monitoring solution that can support 90 days of online storage and 365 days of event/log data?		1
11	Does the system's external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances?		1
12	Does the system require multi-factor authentication (MFA) for administrative accounts and functions?		1
13	Does the system ensure secure separation of customer data?		1
14	Does the system have the capability to detect, contain, and eradicate malicious software?		1
15	Does the system protect audit information from unauthorized access, modification, and deletion?		1
16	Does the SP have the capability to recover the system, within a reasonable timeframe and/or		1

ID	Security Maturity Status	Implemented (Yes or No) To be completed by the Program Management Office	Weighted Value
	within contracted time frames, to a known and functional state following an outage, breach, DoS attack, or disaster?		
17	Does the SP maintain a current, complete, and accurate inventory of the information system software, hardware, and network components?		1
18	Does the SP employ automated mechanisms to detect inventory and configuration changes?		1
19	Does the SP follow a formal change control process that includes a security impact assessment?		1
20	Does the SP prevent unauthorized changes to the system?		1
21	Does the SP scan for configuration settings on systems in the environment?		1
22	Does the SP have an Incident Response Plan?		1
23	Does the SP have a Configuration Management Plan?		1
24	Does the SP have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34?		1
25	Does the SP conduct code analysis for internally developed code?		1
26	***IaaS Only*** Does the SP restrict physical system access to only authorized personnel?		1
27	***IaaS Only*** Does the SP monitor and log physical access to the information system, and maintain access records?		1
28	***IaaS Only*** Does the SP monitor and respond to physical intrusion alarms and surveillance equipment?		1
29	***IaaS Only*** Does the system have or use alternate telecommunications providers?		1
30	***IaaS Only*** Does the system have backup power generation or other redundancy?		1
31	***IaaS Only*** Does the SP have service level agreements (SLAs) in place with all telecommunications providers?		1