GETTING STARTED WITH STATERAMP

A Guide for State Governments

VERSION:
1.2
DATE:
April 2021

TABLE OF CONTENTS

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
October 2020	Initial Draft	1.0	StateRAMP Staff
November 2020	Revisions to language	1.1	StateRAMP Staff
April 2021	Updates to membership information	1.2	StateRAMP Staff

1. WHAT IS STATERAMP

StateRAMP brings state and local governments together to develop standards for cloud security, educate on best practices, and recognize a common method for verifying the cloud security of service providers who use or offer cloud solutions that process, store, and/or transmit government data including personally identifiable information (PII), personal health information (PHI), and payment card industry (PCI) information. StateRAMP is organized under the Indiana Nonprofit Corporations Act as a domestic nonprofit organization.

StateRAMP's purpose is (1) to help state and local government protect citizen data; (2) save taxpayer and service provider dollars with a "verify once, serve many" model; (3) to lessen the burdens on Government; and (4) promote education and best practices in cybersecurity among those it serves in industry and the government communities. StateRAMP's security verification model is based on the National Institute of Standards and Technology (NIST) publication 800-53 Rev. 4—the same publication the Federal Government used to develop FedRAMP, a similar cybersecurity program for federal entities.

While the NIST 800-53 Rev. 4 standards and requirements have been adopted outright as the security framework for several state governments, StateRAMP has partnered with government officials, industry experts, and cybersecurity professionals to develop a widely acceptable set of standards, controls, policies, and procedures which specifically meet the cybersecurity needs of state and local governments.

StateRAMP is here to serve governments by providing a simplified and standardized approach for validating the cybersecurity of the service providers who offer IaaS, PaaS, or SaaS solutions that may process, transmit, and/or store any government data including PII, PCI, and PHI. When partnering with StateRAMP, governments receive education, consultation, and ongoing support through all phases of the implementation, contract award, and continuous monitoring phases of the procurement cycle. Participating governments have access to StateRAMP's secure repository to view service provider security packages, security statuses, and monthly and annual reporting tailored to the government's specific cybersecurity needs.

2. GETTING STARTED

To get started, review the Implementation Checklist provided in the Appendix, or download a copy from the StateRAMP website. Partnering with the StateRAMP Project Management Office (PMO) and completing the milestones outlined in the Implementation Checklist is the quickest way for governments to trust but verify cloud security. This Getting Started Guide is intended to provide further details and best practice recommendations for completing each item in the Implementation Checklist.

For questions about how to adopt StateRAMP's best practices or to speak with a member of the StateRAMP PMO, please email info@stateramp.org.

3. COMPLETING THE IMPLEMENTATION CHECKLIST

Use the following sections to complete all tasks and milestones included in the StateRAMP Implementation Checklist.

3.1 COMMUNICATING WITH STATERAMP

StateRAMP is government's partner from Request for Proposal (RFP) development through continuous monitoring after the contract has been awarded to a service provider. If you need to contact StateRAMP for any reason, please use the information listed below and a member of the StateRAMP team will respond to your inquiry within 1-2 business days.

StateRAMP Office Hours:
Monday-Friday 8:00 a.m. to 5:00 p.m. EST

Contact Information:
info@stateramp.org

3.2 IDENTIFY GOVERNMENT STAKEHOLDERS

To ensure a successful StateRAMP implementation, it is important to make sure all appropriate stakeholders have been notified and engaged. In addition to delegating a primary point of contact for all StateRAMP activities, it may be necessary to involve the following individuals in your organization:

- Chief Information Officer
- Chief Procurement Officer
- Chief Information Security Officer
- Chief Privacy Officer
- Chief Risk Officer
- Chief Technology Officer

The stakeholders identified should participate in StateRAMP discussions, planning, and implementation as well as the development and adoption of internal policies and procedures related to cybersecurity and the procurement of cloud solutions.

3.3 BECOME A STATERAMP MEMBER

State and local governments interested in requiring or accepting StateRAMP-verified third party IaaS, PaaS, and/or SaaS solutions should first become a StateRAMP Member. There are two membership classes available for governments: Government Individual membership and Certified Government membership. Government Individual members are any SLED (state, local, education, tribal/territorial) government official or employee with responsibility for information security, information technology, privacy, and/or procurement. Certified Government members are an entire State, agency, and/or institution who has signed a letter of agreement with StateRAMP and requires applicable third party solutions to be StateRAMP verified. There are no fees associated with either government membership class and both receive full StateRAMP member benefits.

3.4 ADOPT A SECURITY POLICY AND LETTER OF AGREEMENT

Before adding StateRAMP requirements to government RFPs or contracts, it is important to adopt a general cybersecurity policy requiring service providers who offer IaaS, PaaS, or SaaS solutions that may process, transmit, and/or store any government data to be NIST 800-63 Rev. 4 compliant and verified by StateRAMP. Compliance verification provided by FedRAMP, a Federal cybersecurity program, is also acceptable. In addition, StateRAMP will provide a Letter of Agreement that must be completed by the State in order to formalize the adoption of StateRAMP.

StateRAMP will provide a sample policy developed by cybersecurity professionals, government CIOs, Procurement Officials, and legal experts. When adopting a security policy, governments may use the language provided by StateRAMP or develop their own policy. We recommend including the following information in the government policy to ensure successful adoption:

- The State information security policies and standards adhere to the National Institute of Standards and Technology (NIST) 800-53 revision 4.
- The State requires all contractors and suppliers that utilize a cloud system to process, store, and/or transmit government data to demonstrate compliance with NIST 800-53 revision 4 by achieving StateRAMP or FedRAMP authorization for the appropriate impact level.
- Security impact level is determined by data classification and categorization based on the sensitivity of data and criticality of the system. The State requires adherence to FIPS PUB 199 for data classification. A system determined to be Low Impact would require StateRAMP Category 1 or FedRAMP Low Authorization, and a system that is determined to be Moderate Impact would require StateRAMP Category 3 or FedRAMP Moderate Authorization. A system determined to be High Impact would require FedRAMP High Authorization.
- All contractors must comply with required continuous monitoring to maintain StateRAMP or FedRAMP Authorizations.
- The State reserves the right to request and review all Third Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, and/or penetration tests of or relating to the contractor's environment.
- The contractor shall respond to all serious flaws discovered by providing an acceptable timeframe to resolve the issue and/or implement a compensating control.
- Any deviation from these requirements must be approved by the Chief Information Officer.
- Information about StateRAMP can be found at www.stateramp.org. Information about FedRAMP can be found at www.fedramp.gov.

3.5 DETERMINE REQUIRED SECURITY CATEGORY

To determine the appropriate security category with which service providers must comply, use the Data Classification Tool provided by StateRAMP. This tool was designed by cybersecurity experts, government CIOs and CISOs, Procurement Officials, and Privacy Officers to allow governments to more easily determine the risk level associated with processing and storing various types of data in a cloud solution and to quickly identify the appropriate security category that should be required of cloud services to meet government policy and protect the government's data.

There are three StateRAMP security categories: Category 1, Category 2, and Category 3. Each category represents a different set of data characteristics and corresponding security requirements ranging from non-private, generally accessible information to protected, personally identifiable information (PII) or classified data.

- Category 1 aligns with FedRAMP Low Impact
- Category 2 aligns with FedRAMP Low with select additional controls*
- Category 3 aligns with FedRAMP Moderate
- Category 3+ aligns with FedRAMP High

When using the Data Classification Tool, it is up to government to determine how to apply the definitions and terms used to identify the appropriate security level as every government is unique in its interpretation and application of cybersecurity principles.

3.6 SECURITY STATUSES AND PROCUREMENT

After the security level necessary to protect government data has been identified, the government should determine the StateRAMP security status service providers are required to obtain prior to a contract award.

As service providers progress through the StateRAMP process, security statuses are published to indicate the provider's level of fitness to protect the government data in their system. The five StateRAMP security statuses are: Active, Ready, In Process, Provisional, and Authorized. Providers who have engaged a 3PAO but have not yet submitted an assessment are listed as Active on the StateRAMP Authorized Vendor List (AVL). Providers listed as Ready on AVL have been audited by a third party assessment organization (3PA0) who attested to the provider's fitness and ability to meet the cybersecurity standards required by the government. Each subsequent status represents a greater effort on the part of the service provider to protect their cloud offering and the government's data.

In order to maintain procurement timelines, it is best practice to require RFP respondents to have obtained at least a StateRAMP Ready status at the time of the RFP and/or upon contract initiation.

* Category 2 is in development, and details will be published on www.stateramp.org upon adoption.

3.7 RFP LANGUAGE AND ADOPTION

Once the government has determined the security status service providers are required to obtain prior to contract initiation, additional RFP language should be developed and adopted. StateRAMP will provide sample RFP language detailing the security status requirement as well as the corresponding security category. When adopting RFP language relating to required security status and security category, the government may use the language provided by StateRAMP or develop its own requirements. While StateRAMP may withhold a security status from the awarded cloud service provider if State security requirements do not adhere to the appropriate guidelines, the final determinations for risk acceptance and procurement are the State's responsibility. We recommend including the following information in your RFP to ensure a reasonable obligation and clarity for potential respondents:

- The State information security policies and standards adhere to the National Institute of Standards and Technology (NIST) 800-53 revision 4.
- A contract will not be executed with a contractor that uses a cloud system to process, store, and/or transmit government data unless and until the cloud service provider has achieved StateRAMP or FedRAMP Ready Status.
- The Ready Status serves as an attestation to the service providers capabilities to achieve full authorization.
- The State requires all cloud systems that process, store, and/or transmit government data must demonstrate compliance with NIST 800-53 revision 4 by achieving StateRAMP or FedRAMP authorization within 12 months of contract execution for the appropriate data classification.
- Once a contract is issued, the service provider must achieve a StateRAMP or FedRAMP Authorized Status within 12 months.
- All contractors must comply with required continuous monitoring activities to maintain StateRAMP or FedRAMP Authorized Status. The State reserves the right to request and review all Third Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, and penetration tests of or in relation to the contractor's environment.
- The contractor shall respond to all serious flaws discovered by providing an acceptable timeframe to resolve the issue and/or implement a compensating control.
- Any deviation from these requirements must be approved by the Chief Information Officer.
- Information about StateRAMP can be found at www.stateramp.org. Information about FedRAMP can be found at www.fedramp.gov.

3.8 ANNOUNCEMENT AND EDUCATION

An announcement should be made to internal government stakeholders as well as to the service provider community, including those who may have responded to RFPs within the last three years. The announcement will introduce the partnership with StateRAMP and the new cybersecurity verification process. StateRAMP will provide a sample announcement that can be delivered as is, or the government can develop a similar announcement to share with stakeholders and service providers.

Release of the announcement should be coordinated with StateRAMP staff. Following the announcement's publication, StateRAMP will offer free education for the government's internal stakeholders and the service provider community regarding the StateRAMP mission and goals, verification process, and the government's cybersecurity requirements.

3.9 CONTINUOUS MONITORING AND REPORTING

Continuous monitoring and reporting are required after contract award to ensure service providers are maintaining their service offering's security and integrity throughout the duration of their contract. Continuous monitoring is also required for service providers to maintain their StateRAMP security status. To prepare for this phase of the StateRAMP process, it is important to determine the government's capability to handle and assess incoming continuous monitoring reports, the intervals at which the government would like to receive milestone reporting, and the level of ongoing support the government would like to receive from the StateRAMP staff.

4. GLOSSARY

TERM	DEFINITION
Continuous monitoring	Activities conducted by the service provider on a monthly, quarterly, annual, and ad hoc basis to be provided to the State to ensure ongoing data protection and security standard compliance.
service provider	A cloud service provider is any organization who offers or uses IaaS, PaaS, or SaaS solutions that may process, transmit, and/or store any government data including PII, PCI, and PHI.
IaaS	Infrastructure as a Service
NIST 800-53 Rev. 4	The National Institute of Standards and Technology Special Publication 800-53 Revision 4 provides the official requirements of security and privacy controls for information systems handling government information and is the adopted security baseline for StateRAMP and FedRAMP.
FIPS PUB 199	The Federal Information Processing Standards Publication 199 is issued by NIST and provides the standards for security categorization of data in information systems.
PaaS	Platform as a Service
PCI	Payment Card Industry (Data Security Standard)
PHI	Protected Health Information
PII	Personally Identifiable Information
PMO	Project Management Office
RFP	Request for Proposals
SaaS	Software as a Service
Security Category	The Security Category is the category or level of security compliance a service provider must achieve in order to meet State security requirements.
Security Status	The Security Status indicates where the service provider is in the StateRAMP process. Security Statuses include: Ready, In Process, Provisional, and Authorized.
3PAO	Third Party Assessment Organization

5. APPENDIX

5.1 STATERAMP IMPLEMENTATION CHECKLIST

☐ **Identify stakeholders and determine a governance process**

- ☐ The government's primary stakeholder(s) and the StateRAMP PMO will work together to identify additional government stakeholders whose involvement will be required in the implementation process.
- ☐ The government must identify the steps and requirements necessary for implementing and adopting StateRAMP.

☐ **Become a StateRAMP Member**

- ☐ Government Individual membership is available for any SLED (state, local, education, tribal/territorial) government official or employee with responsibility for information security, information technology, privacy, and/or procurement.
- ☐ Certified Government membership is available for an entire State, agency, and/or institution who has signed a letter of agreement with StateRAMP and requires applicable third party solutions to be StateRAMP verified.

☐ **Develop and adopt a security policy and sign the StateRAMP Letter of Agreement**

- ☐ StateRAMP will provide a sample policy which requires Service providers offering IaaS, PaaS, or SaaS solutions that may process, transmit, and/or store any government data including PII, PHI, or PCI, to be NIST 800-53 Rev. 4 compliant and verified by StateRAMP (or FedRAMP).
- ☐ The government will sign the StateRAMP Letter of Agreement.
- ☐ The government will adopt and publish the security policy provided by StateRAMP or develop a similar policy for adoption and publication.

☐ **Determine security impact and the required security category**

- ☐ StateRAMP will provide a Data Classification Tool used to determine the security impact of the government data being processed, transmitted, and/or stored by Service providers.
- ☐ The government will determine how to apply the Data Classification Tool based on individual application of security concepts and risk thresholds.
- ☐ Based on the security impact identified using the Data Classification Tool, the government will select the appropriate security category (Category 1, 2, or 3) Service providers are required to meet or exceed.

☐ **Identify the security status requirement necessary for procurement**

- ☐ StateRAMP will provide information about the different security statuses a service provider can achieve in the StateRAMP process, how the statuses relate to readiness, and best practice recommendations for which security status should be required from the service provider at the time of a contract initiation.

- ☐ The government will determine which security status to require from responding Service providers at the time of RFP and upon contract initiation.

☐ **Adopt new RFP cybersecurity language**

- ☐ StateRAMP will provide sample RFP and/or contract language that can be used to ensure Service providers understand what StateRAMP security status and security category are required.
- ☐ The government will adopt the provided RFP and/or contract language or develop similar language for adoption.

☐ **Announce the new StateRAMP requirement to internal stakeholders and service provider community**

- ☐ StateRAMP will provide a sample announcement that can be delivered to internal stakeholders as well as with the service provider community, including any service provider who has responded to an RFP in the past three years.
- ☐ The government can use the sample announcement or develop a similar announcement to be shared with internal stakeholders and the service provider community.
- ☐ The government should coordinate with StateRAMP on the release of the announcement.
- ☐ StateRAMP will offer free education for government stakeholders and the service provider community regarding the StateRAMP mission and goals, verification process, and cybersecurity outcomes.

☐ **Begin identifying continuous monitoring and reporting requirements**

- ☐ StateRAMP will provide recommended and best practice continuous monitoring guidelines.
- ☐ The government should determine what reporting is required of Service providers for continuous monitoring to maintain their contract award.