StateRAMP

GETTING STARTED WITH STATERAMP

A Guide for Government

VERSION:
1.6
DATE:
August 2023

StateRAMP

TABLE OF CONTENTS

WHAT IS STATERAMP? 2

GETTING STARTED 3

COMMUNICATING WITH STATERAMP 5

OUTCOMES 3

IDENTIFY GOVERNMENT STAKEHOLDERS AND PROCESS 3

MILESTONES 4

BECOME A PARTICIPATING GOVERNMENT 4

DOCUMENT STATERAMP REQUIREMENTS 6

OBTAIN ACCESS TO CONTINUOUS MONITORING 6

ONGOING SUPPORT AND COMMUNICATION 7

GLOSSARY 0

WHAT IS STATERAMP?

For governments, today's security environment is complicated by diverse security standards coupled with significant data sprawl through cloud service providers that process, store, and/or transmit government data, leaving governments less secure than ever against the increasingly challenging cyber-threat environment.

StateRAMP [Risk & Authorization Management Program] exists as a free resource[1] for governments in bringing together state and local governments with cloud service providers to address these challenges head on by streamlining and enhancing security standards for cloud- and internet-enabled service products, as well as educating on risk management best practices for the public sector. StateRAMP's purpose is:

(1) Help state and local government, public education institutions and special districts protect citizen data;

(2) Save taxpayer and vendor dollars with a "verify once, serve many" model;

(3) Lessen the burdens on governments in managing security risk; 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 (or current version)—the same publication the Federal Government used to develop FedRAMP, a similar cybersecurity program for federal entities. While the NIST 800-53 Rev. 4 (or current) 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 accepted set of standards, controls, policies, and procedures which specifically meet the cybersecurity needs of state and local governments.

StateRAMP provides a simplified and standardized approach for validating the cybersecurity of the vendors who offer **Infrastructure as a Service (IaaS)**, **Platform as a Service (PaaS)**, or **Software as a Service (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 vendor security packages, security statuses, and monthly and annual reporting tailored to the government's specific cybersecurity needs.

[1] StateRAMP is organized under the Indiana Nonprofit Corporations Act as a domestic nonprofit organization.

StateRAMP

GETTING STARTED

Partnering with a StateRAMP Government Engagement Director and completing the milestones outlined below is the quickest way for governments to trust but verify the security of cloud products and services.

- ☐ **Become a Participating Government**
  - ☐ StateRAMP will provide a Memorandum of Understanding (MOU).
  - ☐ The government will review the MOU and add/change all necessary sections, sign, and return to StateRAMP.
  - ☐ StateRAMP will sign and return the fully executed MOU to the entity.
  - ☐ StateRAMP will then list the entity on StateRAMP's website as a participating government.
- ☐ **Document StateRAMP Requirements**
  - ☐ Update Policy
  - ☐ Update Procedure(s)
  - ☐ Incorporate Requirements into Procurement Language
    - Solicitation
    - Contract
  - ☐ Provide Links to StateRAMP
    - Solicitations with StateRAMP Requirements
    - Contracts with StateRAMP engaged vendors with Cooperative Language
- ☐ **Obtain Access to Continuous Monitoring**
  - ☐ Provide Contract List to StateRAMP
  - ☐ Provide Bidder's List to StateRAMP
  - ☐ Complete Intro to PMO Onboarding Document and Return to StateRAMP
  - ☐ Attend PMO Onboarding

IDENTIFY GOVERNMENT STAKEHOLDERS AND PROCESS

As your organization beings to consider StateRAMP adoption, 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, the additional stakeholders identified should

participate in StateRAMP discussions, planning, and adoption, including the updates to internal policies and procedures related to cybersecurity and the procurement of cloud solutions.

- These could include the following individuals, or their representatives: Chief Information Officer
- Chief Procurement Officer [from the IT Department and Administrative Departments]
- Chief Information Security Officer
- Chief Privacy Officer
- Chief Risk Officer
- Chief Technology Officer

WORKING WITH STATERAMP

The following results / outputs can be expected from StateRAMP implementation:

- Procedures, including language in solicitations and contracts, will be updated to reflect improved cyber security requirements.
- Organizational policies will be updated to include improved cyber security language and vendor requirements.
- The service provider community will be educated by StateRAMP staff on the improved cyber security requirements and will have access to ongoing training and assistance as needed.
- Information Security staff will be fully trained to access vendor security documents and to receive reporting from StateRAMP PMO.
- Procurement staff across the organization will be educated by StateRAMP staff on improved cyber security requirements and will have access to ongoing training as needed.

ONGOING SUPPORT AND COMMUNICATION

StateRAMP support continues after adoption. We recommend the following activities to ensure continued support.

MONTHLY MONITORING

As your organization acquires new products, you will want to ensure access to the continuous monitoring and any available progress reporting. StateRAMP recommends submitting requests for visibility on these new products on a monthly basis by requesting access through the StateRAMP PMO.

QUARTERLY REVIEWS

StateRAMP staff will engage your identified point of contact on a quarterly basis and additionally as needed to provide any needed support.

COMMUNICATING WITH STATERAMP

StateRAMP is Government's partner from solicitation development through to contract administration via continuous monitoring after the contract has been awarded. If you need to contact StateRAMP for any reason, please contact your dedicated government engagement representative or 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:
get@stateramp.org

GLOSSARY

TERM	DEFINITION
3PAO	Third Party Assessment Organization
Continuous monitoring	Activities conducted by the vendor on a monthly, quarterly, annual, and ad hoc basis to be provided to the State to ensure ongoing data protection and security standard compliance.
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.
IaaS	Infrastructure as a Service
NIST 800-53 Rev. 4 (or current version)	The National Institute of Standards and Technology Special Publication 800-53 Revision 4 (or current version) provides the official requirements of security and privacy controls for information systems handling government information and is the adopted security baseline for StateRAMP.
PaaS	Platform as a Service
PCI	Payment Card Industry (Data Security Standard)
PHI	Protected Health Information
PII	Personally Identifiable Information
PMO	Project Management Office
SaaS	Software as a Service
Security Category	The Security Category is the category or level of security compliance a vendor must achieve to meet State security requirements.
Service Provider	A cloud vendor 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.
Security Status	The Security Status indicates where the vendor is in the StateRAMP process. The Security Statuses in the process include: Snapshot, Progressing Snapshot Program, Ready, In Process, Provisional, and Authorized.