StateRAMP

StateRAMP + Procurement Overview

Meet The Team

Chance Grubb serves as the Government Engagement Director for the Western region. Chance possesses over 17 years of state government experience in procurement, information technology and cybersecurity. During his time at the State of Oklahoma, he oversaw several statewide programs that included establishing a vendor management program, sharing of cyber threat intelligence through the OK-ISAC and maturing a third-party security program.

Rebecca Kee serves our government members as the Government Engagement Director, focusing on the integration of StateRAMP into education processes and policies. She has 18 years of experience in the public procurement field and has worked extensively to develop, create, and support educational programs and opportunities for the profession.

StateRAMP

StateRAMP is a non-profit, with members in the public and private sectors with a mission to promote best practices in cloud cybersecurity and a standardized approach to verifying cloud solutions.

- Members leverage standardized assessments to verify cloud security.
- Ongoing information sharing helps partners manage risk and continuously improve.

What is StateRAMP?

Based on NIST 800-53, StateRAMP has developed tiers of independently verifiable security certifications for service providers to achieve to demonstrate that they are meeting the requirements needed for the type of data they hold, process, and transmit.

StateRAMP was created as a public-private venture to bring public sector interests, industry interests, and auditor interests together to create a seamless process and platform to:

- Gain clear, ongoing insight into the cybersecurity posture of business partners
- Relieve burden on procurement and IT/Info Sec teams to review diverse compliance frameworks
- Advance risk management strategy further upstream

- Gain a verify once, serve many approach to compliance
- Demonstrate 'trusted partner' status
- Reduce barriers to competition through a comprehensive compliance framework

How StateRAMP Works – Government Adoption Tiers

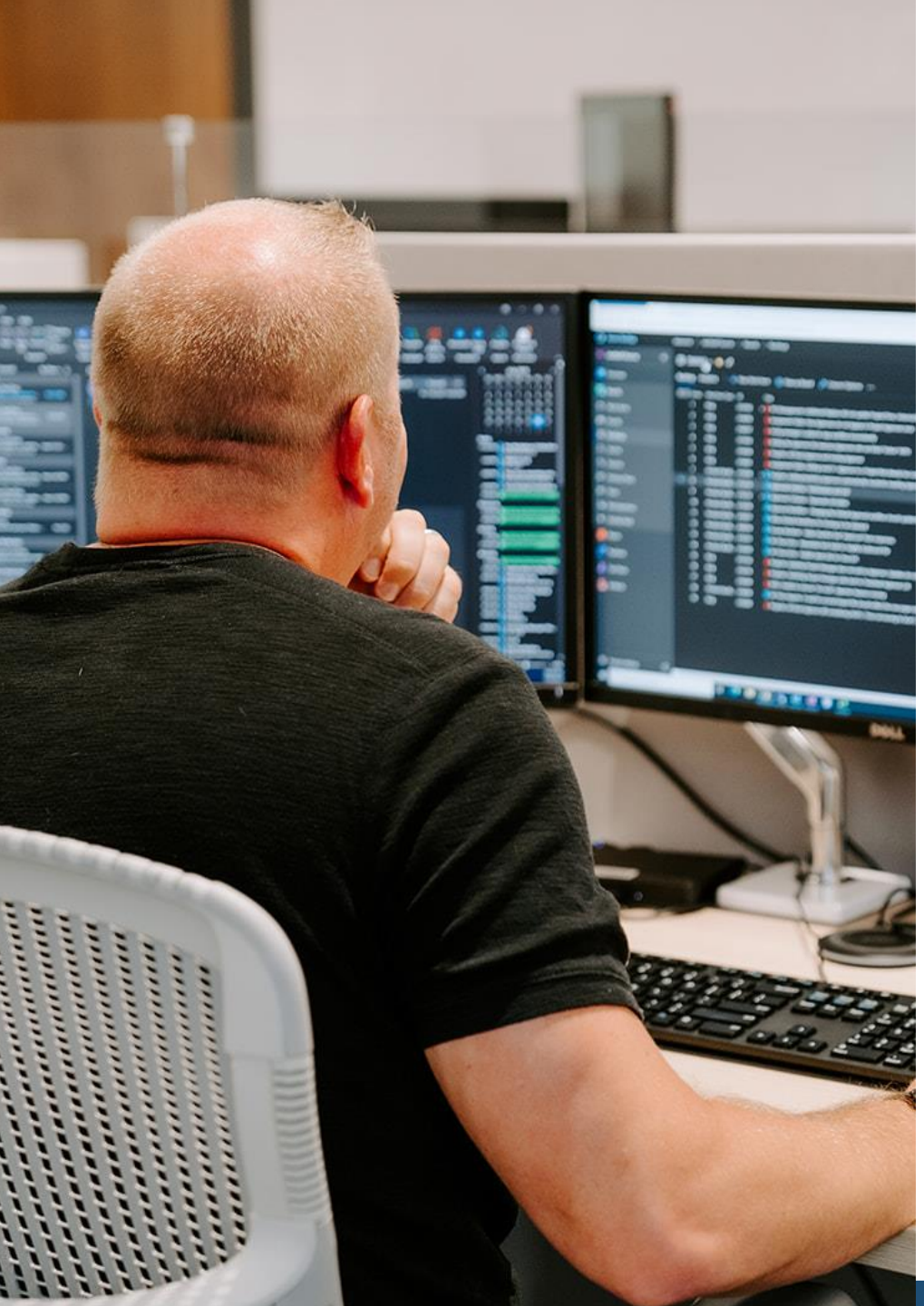
Accept	Prefer	Require
Accepting the StateRAMP program indicates that an organization allows a StateRAMP assessment to satisfy a business requirement in addition to other assessments.	**Preferring** the StateRAMP program indicates that an organization offers preference or additional evaluation points for StateRAMP assessed products.	**Requiring** the StateRAMP program indicates that an organization fully adopts StateRAMP from solicitation through award and contract management.
Example: Organization A accepts StateRAMP Ready at the point of solicitation, in addition to other risk assessments for IT contracts, and it satisfies the requirements for the organizations internal risk assessment management program. Organization B accepts StateRAMP Authorized for all cloud contracts that interact with moderate impact data in addition to other risk assessments. Organization C accepts StateRAMP Snapshot, Ready or Authorized for all technology contracts in addition to other risk assessments.	Example: Organization A offers preference to products with StateRAMP Ready validation; however no additional evaluation points are offered during the procurement process. Organization B offers additional evaluation points for StateRAMP engagement (ie. Full points for StateRAMP Ready/Authorized, half points for StateRAMP Security Snapshot, no additional points if not StateRAMP engaged.) Organization C gives the highest preference to StateRAMP products.	Example: Organization A requires StateRAMP Snapshot at the minimum at the point of solicitation. Organization B requires StateRAMP Ready or Authorized for all cloud contracts. Providers must grant visibility as a requirement of the contract. Organization C requires StateRAMP Authorized for all products with a technology component. Providers must grant visibility for the lifecycle of the contract,

How StateRAMP Works - Third Party Risk Management Policy

- As part of the adoption project, the State of Oregon and StateRAMP will work together to revise all documentation regarding third-party risk management.
  - State of Oregon Department of Justice is assisting with creation of this language.

State of Oregon Q2 2024

- Host education effort for IT teams and additional procurement staff from other key agencies (May 13 and 15)
- Share StateRAMP draft language & develop timeline for updating existing language (June)
- Review existing Policy, Procedures, Solicitation Language, Contract Language (June - July)



Solicitations for Cloud Services*

We want to tell potential vendors that are providing cloud services:

- What is needed for proposal.
- How it will be used in evaluation.
- What will be required if a contract is initiated.

StateRAMP Process – Provider Path

Pre-Solicitation

Step 1:

Become a member of StateRAMP.

**If pursuing a Ready or Authorized status, skip to Step 5.*

Step 2:

Complete StateRAMP Security Snapshot (one time cost dependent on annual revenue; single Snapshot valid for 12 months).

Solicitation/Upon Award

Step 3:

Submit StateRAMP Security Snapshot (or Ready/Authorized Letter, if applicable) and, if requested, provision Government partners to access documents

Step 4:

Enroll in StateRAMP Progressing Security Snapshot program and provision access to government (monthly cost dependent on annual revenue). Utilize monthly consulting calls to mature your cloud product.

During Contract

Step 5:

Engage Third-Party Assessment Organization (3PAO). Upon completion of audit, submit Security Review Request Form to StateRAMP Program Management Office (PMO). Technical review will be conducted, which is typically completed in 4-6 weeks. For products under review for Authorization status, a government sponsor or review by the StateRAMP Approvals Committee is required. Once Ready, Authorized, or Provisional status is achieved, Continuous Monitoring will begin.

** Suppliers can obtain a StateRAMP Security Snapshot within a 3-week timeline. More information on the process for providers at - https://stateramp.org/providers/.

StateRAMP Provider Path - What is Needed for Proposal

Purpose: To ensure that respondents know what to turn in for their proposal for cloud services.

- Explain to the vendor what their StateRAMP options are (Snapshot, Ready, Authorized, etc.)
- Tell the vendor what they need to turn in should they choose the StateRAMP option
  - Proof of current StateRAMP Authorization status in the form of a StateRAMP Letter
  - Proof of current StateRAMP Ready status in the form of a StateRAMP Letter
  - Valid StateRAMP Security Snapshot Score
    - Proof of enrollment in the StateRAMP Progressing Security Snapshot Program
- Inform the vendor of any consequences should they choose to utilize StateRAMP but fail to include the necessary documents

How Will StateRAMP Be Used in Evaluation ?

EVALUATION CRITERIA - Cyber Security

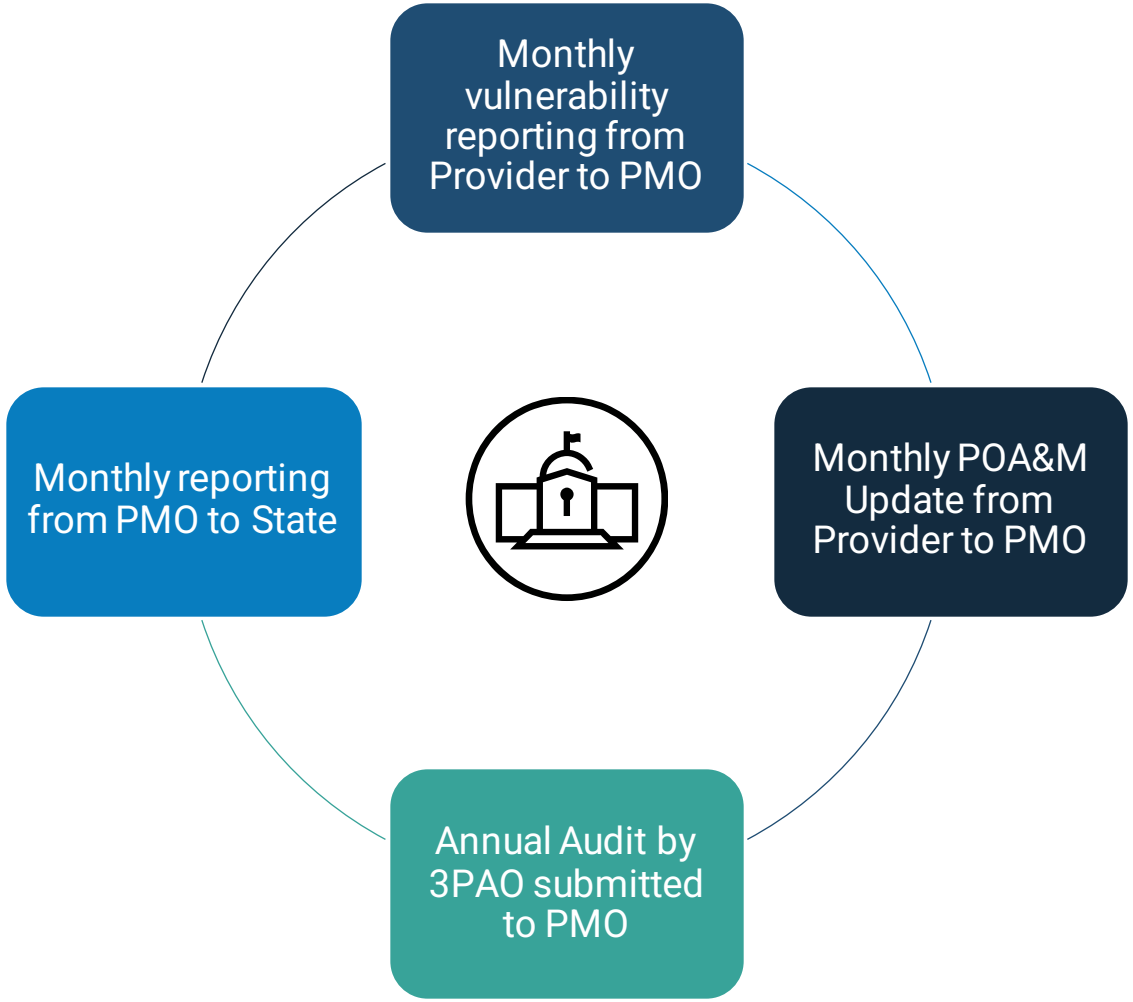
- Security requirements are evaluated on a pass/fail basis.
- StateRAMP engagement will meet the security requirement.

What to Include if Contract Initiated

StateRAMP Option

- Contract should include description of each type of StateRAMP engagement that is:
  - Accepted
  - What is necessary to stay compliant
  - Consequences of not being compliant

- Continuous Monitoring Compliance
  - State what is expected of provider to remain compliant
  - Consequences of not remaining compliant



Continuous Monitoring

Providers must comply with Continuous Monitoring requirements to maintain status of Ready, Authorized or Provisional. If a supplier becomes non-compliant, the StateRAMP PMO will notify the Participating Organization through our ConMon Escalation Process.

Providers may grant viewing access to Participating Governments.

View Continuous Monitoring Policies & Escalation Process for more: www.stateramp.org/templates-resources.

What about Contracts Where a Traditional Solicitation Isn't Issued?

In the instance where you are utilizing a cooperative, sole source, single source, etc. you can still request that the utilization of StateRAMP for the product is an option.

You can utilize the contract language developed during the State of Oregon adoption project.

Existing Contracts

At this time; No Change.

More information and guidance will be provided as the project progresses.

State of Oregon - Information and Resources

For project and program updates, please visit the State of Oregon program page at: https://programs.stateramp.org/oregon/

StateRAMP for Government: https://stateramp.org/governments/implementing-for-government/

Security Policies & Templates: www.stateramp.org/templates-resources/

Governance & Documents: www.stateramp.org/documents/

StateRAMP Frequently Asked Questions: https://stateramp.org/faqs/

Questions?