GETTING STARTED WITH STATERAMP

A Guide for Government

VERSION:
1.5

DATE:
December 2022

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
October 2021	Updated security categories	1.3	StateRAMP Staff
May 2022	Updates to implementation information	1.4	StateRAMP Staff
December 2022	Clarify adoption language	1.5	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 vendors 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, public education institutions and special districts protect citizen data; (2) save taxpayer and vendor 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 vendors who offer Infrastructure as a Service (IaaS), 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.

2. GETTING STARTED

To get started, review the StateRAMP Adoption Checklist provided in Appendix A. Partnering with a StateRAMP Government Engagement Director and completing the milestones outlined in the Adoption 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 on the Implementation Checklist.

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

OUTCOMES

The following outcomes can be expected from StateRAMP adoption:

- 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 vendor 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.

Use the following sections to complete all tasks and milestones included in the StateRAMP Adoption Checklist in located in Appendix A.

COMMUNICATING WITH STATERAMP

StateRAMP is government's partner from solicitation development through 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:
info@stateramp.org

IDENTIFY GOVERNMENT STAKEHOLDERS AND PROCESS

To ensure a successful 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, 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

Governance Process Determination. The 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.

3. COMPLETING THE ADOPTION CHECKLIST

DOCUMENT STATERAMP REQUIREMENTS

StateRAMP provides a sample language for policy, procedure, contract and solicitation language developed by cybersecurity professionals, government CIOs, procurement officials, and legal experts that incorporates the following recommendations to ensure successful adoption:

- The State/County/City/University/etc. information security policies and standards adhere to the National Institute of Standards and Technology (NIST) 800-53 revision 4.
- The State/County/City/University/etc. 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 Authorization for the appropriate impact level.
- All contractors must comply with the required continuous monitoring to maintain StateRAMP Authorizations.
- The State/County/City/University/etc. 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 a mutually agreed upon timeframe to resolve the issue and/or implement a compensating control.
- Any deviation from these requirements must be approved by the Chief Information Officer or a designated authority.

Update Policy

Before adding StateRAMP requirements to government solicitations or contracts, it is important to update cybersecurity requirements in any policies that apply to vendors who use or offer IaaS, PaaS, or SaaS solutions that may process, transmit, store and/or impact any government data to be compliant with NIST 800-53 Rev. 4 (or current version) and verified by StateRAMP.

Update Procedure

Once all necessary policy updates have been completed, it is important to update internal procedures to ensure that the now updated policies are easily followed. The updating of these procedures ensures that updates to policy are incorporated into practice of the government entity.

Incorporate Requirements into Procurement Language

Once the government has updated policy and procedure, solicitation and contract language should also be developed and adopted. We recommend including the following information in your solicitations and/or contracts to ensure a reasonable obligation and clarity for potential respondents:

- The State/County/City/University/etc. information security policies and standards adhere to the National Institute of Standards and Technology (NIST) 800-53 revision 4 or current version.
- All contractors must comply with required continuous monitoring activities to maintain StateRAMP Authorized Status. The State/County/City/University/etc. 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 in writing and signed by both parties.

Language reflecting the updated cyber security requirements should be incorporated into solicitation documents and into contract documents. Clear statements instructing respondents to solicitations what documents are required at the time of submission, how the maturity of their cyber security will be evaluated, and what will be expected of any awarded contractor is necessary to ensure compliance with updated policies and procedures as well as a procurement best practice.

To ensure that the awarded contractor complies with all requirements set forth in the solicitation, adoption of the solicitation criteria along with specific contract language should be incorporated into resultant contracts.

For sample language, see Appendix B – StateRAMP Standard Language.

While StateRAMP may withhold a security status from the awarded cloud vendor if government security requirements do not adhere to the appropriate guidelines, the final determinations for risk acceptance and procurement are the State's responsibility.

BECOME A PARTICIPATING GOVERNMENT

State and local governments interested in 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 Participating Government membership. Government Individual members are any SLED (state, local, education, tribal/territorial) government official or employee with responsibility for information security, information technology, legal, privacy, and/or procurement. Participating 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, and both classifications receive full StateRAMP member benefits.

Letter of Agreement

In addition, StateRAMP will provide a Letter of Agreement that must be completed by the government organization to formalize the Participating Government Membership with StateRAMP.

See Appendix C - StateRAMP Letter of Agreement Sample and Supporting Documents

OBTAIN ACCESS TO CONTINUOUS MONITORING

Continuous monitoring and reporting are required after the contract is awarded to ensure contractors are maintaining their service offering's security and integrity throughout the duration of their contract. Continuous monitoring is also required for vendors 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.

Contract/Bidder's List

StateRAMP will ensure that the vendor community, including those who may have responded to solicitations within the last three years are aware of StateRAMP and how to engage. The correspondence from StateRAMP can introduce the partnership with your organization and StateRAMP along with the new cybersecurity verification process if desired. 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 vendors.

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

Program Management Office (PMO) Onboarding

Upon return of the completed StateRAMP PMO Onboarding Document (See Appendix D), StateRAMP will schedule a meeting with those government officials who wish to access the StateRAMP secure portal to view continuous monitoring reports and artifacts. StateRAMP will utilize the Contract List to provide access to those products that are StateRAMP Ready or Authorized, as well as any progress reports available for those products being utilized by the government entity. During this meeting, the StateRAMP PMO will educate government officials on how to utilize the secure portal to view reports and other security documents.

ONGOING SUPPORT AND COMMUNICATION

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

Monthly

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

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

4. GLOSSARY

TERM	DEFINITION
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.
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.
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.
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
SaaS	Software as a Service
Security Category	The Security Category is the category or level of security compliance a vendor must achieve in order to meet State security requirements.
Security Status	The Security Status indicates where the vendor is in the StateRAMP process. The Security Statuses in the process include: Ready, In Process, Provisional, and Authorized.
3PAO	Third Party Assessment Organization

APPENDIX A

STATERAMP ADOPTION CHECKLIST

If you are interested in learning more, contact the StateRAMP Adoption Team to schedule a call at info@stateramp.org.

- □ **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

Great Start! You now have an updated security requirement.

- ☐ **Become a Participating Government**
  - ☐ StateRAMP will provide a Letter of Agreement.
  - ☐ The government will add/change all necessary sections, sign, and return to StateRAMP.
  - ☐ StateRAMP will sign and return the fully executed copy to the entity.
  - ☐ StateRAMP will then list the entity on StateRAMP's website as a participating government.

Congratulations! Your government is now a member of StateRAMP.

- ☐ **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

You did it! You have adopted StateRAMP. Now let's keep it going.

- ☐ **Ongoing Support and Communication**
  - ☐ Monthly
    - Request Secure Access to any newly acquired products for Continuous Monitoring
  - ☐ Quarterly
    - Update users for Continuous Monitoring if needed
    - Update Primary Contact for StateRAMP communication needs

APPENDIX B

STATERAMP STANDARD LANGUAGE

STATERAMP STANDARD POLICY LANGUAGE

Purpose

This policy requires Third Parties that do business with the State/Entity of XXX to implement security and privacy controls derived from NIST 800-53, R4 or most current version, that align with the controls the State requires of itself.

Policy

Third-Party Risk Management

The State of XXX requires an independent 3rd party attestation StateRAMP for systems containing confidential or proprietary data, as defined in Section XXX.

For these systems, at minimum, a current StateRAMP Security Snapshot must be provided not later than the time of contract award, and StateRAMP Ready status will be achieved and documented not more than 12 months after contract award, and StateRAMP Authorization status will be achieved and documented not later than 18 months after contract award. A StateRAMP Security Snapshot must be maintained, to include monthly progress reporting until StateRAMP Ready Status is achieved. StateRAMP Security Snapshot monthly progress reporting should indicate progression toward StateRAMP Ready status.

STATERAMP STANDARD PROCEDURE LANGUAGE

Purpose: This purpose of this standard operating procedure is to provide implementation guidance for the Government's Third-Party Risk Policy, Policy No. XXX.

Procedure

For Applications, Systems, Networks that store/process, or have access to protected data:

During the procurement process, preferably at the Request for Proposal/Request for Quote stage, but in all cases prior to contract award, Agencies shall receive a StateRAMP Security Snapshot, unless the product is listed as StateRAMP Ready or StateRAMP Authorized for systems containing protected data. The preferred attestation is StateRAMP Authorized.

If StateRAMP Authorization status is not in place at the time of contract award a valid StateRAMP Security Snapshot may be accepted with the inclusion of contract language that requires StateRAMP Ready certification within 12 months of contract execution and StateRAMP Authorization certification within 18 months of contract execution. StateRAMP Security Snapshot should be maintained along with monthly progress reporting until StateRAMP Ready status is achieved. StateRAMP Security

Snapshot monthly progress reporting should be monitored and should indicate progress until such time as the product receives StateRAMP Ready status.

ACCOUNTABILITY

All Agency and Executive Branch Employees that participate in the RFP/RFQ/Contacts process for their Agencies shall ensure they receive proof of StateRAMP Authorized or StateRAMP Ready statuses or a valid StateRAMP Security Snapshot prior to contract award for the product. The Chief Information Security Officer shall not approve any RFP, RFQ, or Contract in the Contract Technical Review Process unless these statuses or a valid StateRAMP Security Snapshot is available.

STATERAMP STANDARD SOLICITATION LANGUAGE

Purpose: Each of these requirements fulfill the requirement of the third-party risk management policy and provides guidance to bidders/respondents for fulfillment of response requirements and expectations of the awarded vendor(s) throughout the life of any resulting contract.

CYBER SECURITY REQUIREMENTS

(Requests for Proposals/Bids)

Cloud service products subject to RAMP authorization – All cloud service products that process, store, transmit and/or could impact government data must demonstrate compliance with NIST 800-53 at the specified Impact Level.

Security and Control requirements - The successful proposer's cloud product offering must comply with the (*Insert jurisdiction and reference any include any specific security and RAMP policies*) information security policies and adhere to the National Institute of Standards and Technology (NIST) Special Publication 800-53 (revision 4 or latest version) controls for StateRAMP Impact Level (*Insert selected Impact Level for appropriate NIST 800-53 control package. Example: Low/ Low Plus/Moderate/ High*).

RAMP Ready Status – Any resulting award will be made to selected respondent(s) offering a cloud product that processes, stores, transmits and/or could impact government data, only if the proposal includes written documentation that the cloud product has achieved StateRAMP {(Ready/Provisional/Authorized) status (*select the minimum status required)*} or a valid StateRAMP Security Snapshot at the time of proposal submission.

Respondents **must** submit one of the following with their response/bid:

- 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

Failure to submit one of the documents listed above will result in disqualification of your response/bid.

RAMP Impact Level Requirement – All cloud product offerings submitted in response to the RFP that process, store, transmit and/or could impact government data must demonstrate compliance with NIST 800-53 at StateRAMP Level (*Select the appropriate Impact Level: Low/Low Plus/Moderate/High*) by achieving StateRAMP Ready certification not later than 12 months after contract execution and full StateRAMP Authorization not later than 18 months after contract execution.

Continuous Monitoring – For any resulting award(s) and subsequent contract(s), the awarded contractor(s) will grant access to continuous monitoring and reporting upon receiving award for StateRAMP Security Snapshot, Ready status and Authorization status through the life of the contract. The *(insert jurisdiction)* reserves the right to request and review all Third-Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, and penetration tests of the contractor's environment. The contractor shall respond to all flaws discovered by providing a mutually agreed upon timeframe to resolve the issue and/or implement a compensating control.

(Optional Clause to be considered on a project-by-project basis)
Authorized Use Cloud Service Products – Use of any resulting contract(s) is limited to agencies authorized to purchase from the agreement by the *(Identify the jurisdiction and approving official or body)* and only for IT projects that have been authorized by the *(identify the authorizing person or body that approved the procurement of the project or relevant project approval information.)*

Compliance with Requirements – By signature of the proposal the offeror represents and warrants that the cloud product offered in the proposal complies with the requirements of this section. *(If there is written policy that supports this section for the jurisdiction's RAMP program add the reference here).*

EVALUATION CRITERIA

(Request for Proposals)

(Point value can obviously change, but we recommend at minimum of 20 points as third-party risk should be a significant consideration when choosing a vendor that deals with protected data. We have weighted Authorized at 100%, Ready at 75% and Snapshots between 0% and 50% of the available points)

Cyber Security – 20 Points

This evaluation criteria shall be calculated utilizing StateRAMP reporting. Proposed products that possess a current StateRAMP Authorization status shall receive the total available points (20). Proposed products that possess a current StateRAMP Ready status shall receive 75% of the total available points (15). Proposed products that submitted a StateRAMP Security Snapshot score will receive points between zero and ten (0 – 10) based on that score.

(Optional statement: If you wish to propose a minimum cyber score this line can be added.)

Proposed products must meet a minimum of five (5) points to be considered for further evaluation.

STATERAMP STANDARD CONTRACT LANGUAGE

Purpose: This language fulfills the requirement of third-party risk management policy and provides guidance to contractors for fulfillment and maintenance of requirements throughout the life of the contract.

TERMS AND CONDITIONS

(RECOMMENDED FOR USE IN ALL CONTRACTS)

All products and services that manage, have access to or the ability to impact protected data, as identified by Government must adhere to Government Third-Party Risk Management Policy XXXX.

SPECIAL TERMS AND CONDITIONS

(RECOMMENDED FOR USE IN CONTRACTS WHICH ARE SPECIFICALLY IDENTIFIED AS THOSE THAT WILL OR MAY IMPACT GOVERNMENT DATA)

Risk Management

All products and services that manage, have access to or the ability to impact protected data, as identified by Government must meet the following requirements:

StateRAMP Authorization. Products with StateRAMP Authorization status must maintain StateRAMP Authorization status for the duration of the contract. Government must be granted visibility and access through StateRAMP for continuous monitoring as requested.

StateRAMP Ready. Products with StateRAMP Ready status must maintain StateRAMP Ready status until StateRAMP Authorization status is achieved. StateRAMP Authorization status must be achieved not later than 18 months after execution of this contract. Government must be granted visibility and access through StateRAMP for continuous monitoring as requested.

StateRAMP Security Snapshot. Products with StateRAMP Security Snapshot must maintain a valid StateRAMP Security Snapshot and provide monthly progress reporting to StateRAMP until StateRAMP Ready or StateRAMP Authorization status is obtained. StateRAMP Ready status must be obtained not later than 12 months after execution of this contract and StateRAMP Authorization status must be obtained not later than 18 months after execution of this contract. Subsequent Security Snapshots should reflect progress toward increased security controls and StateRAMP status. Government must be granted visibility and access through StateRAMP for progress reviews as requested.

Liquidated Damages
If contractor fails to maintain or achieve security requirements as listed in Risk Management, liquidated damages may be assessed in the amount of $XXX for each day that the contractor is not in compliance with the security requirements as set forth in this document.

APPENDIX C

STATERAMP LETTER OF AGREEMENT AND SUPPORTING DOCUMENTS

Month __, 2022

Contact Name
State of ____
Address
Address
Address

Re: Letter of Agreement

Dear _____,

StateRAMP's goal is to create a framework for continuous improvement in cybersecurity for state and local governments, service providers, and the constituents they serve.

As such, StateRAMP is pleased to have the opportunity to provide the benefits outlined in this letter of agreement ("**Agreement**") to service provider members of StateRAMP engaged by the *Insert State, Local, Tribal Territory* ("**Government**"). This Letter describes the scope of benefits to be provided by StateRAMP, and the timing of performance by StateRAMP.

This Agreement also sets forth certain duties, obligations, and responsibilities to be performed by the Government and StateRAMP in accordance with the time periods set forth herein, as well as certain conditions of the engagement.

The Government agrees to require its third-party vendors who use a cloud platform or deliver services that require the use of a cloud platform to transmit, store, and/or process, and/or impact the security of Government data to verify compliance with the Government's adopted cyber policy based on NIST 800-53 Rev. 4 (or current) as listed on StateRAMP's Authorized Product List. (May reference or link to the Government's adopted policy here). These entities or vendors can include one or more of the following: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and service contracts which require the storing, processing, and/or transmitting of Government data in environments outside control of the Government.

The Government agrees to serve as a sponsor for provider members of StateRAMP working to attain a StateRAMP security status of Authorized. The Government maintains full discretion around which providers to sponsor, and sponsorship is anticipated generally for providers who have been awarded a contract with the Government. As a sponsor, the Government agrees to review the provider's submitted StateRAMP security package and make a determination in support or objection to the StateRAMP's determination for status.

Final determinations of risk acceptance and contracting decisions always remain with the Government.

The Government agrees to be listed on the StateRAMP website as a participating entity and member of StateRAMP. The Government will provide StateRAMP a primary point of contact (PoC) to receive security reviews and continuous monitoring reports.

StateRAMP agrees to promote a common method of verification for service providers products that is based on NIST 800-53 Rev. 4 (or current) and modeled in part after FedRAMP, utilizing independent assessments provided by FedRAMP authorized third party assessment organizations (3PAOs). StateRAMP will manage the Project Management Office (PMO), who will review security packages, assign and/or recommend security statuses, publish providers' security statuses on a public website, and manage continuous monitoring activities. StateRAMP security statuses include the following:

Security Status	Description
Active	Provider begins working with 3PAO for Readiness Assessment Report (SR-RAR) and has registered with StateRAMP
Pending	3PAO submits Ready package for Provider to StateRAMP
Ready	StateRAMP and 3PAO attest to Provider's Readiness and compliance with StateRAMP's published Minimum Mandatory Requirements
In Process	Provider begins with 3PAO for security package, including Security Assessment Report (SR-SAR) and has registered with StateRAMP.
Authorized	StateRAMP and Government Sponsor accept security package; Provider begins Continuous Monitoring.
Provisional	Government Sponsor determines Provider's security package meets minimum mandatory and most critical controls, but not all. Government Sponsor may assign Provisional Status as Provider works toward Authorization. Provider begins Continuous Monitoring.

StateRAMP agrees to publish a Data Classification Tool to guide selection of appropriate security impact levels that align with the following:

1) StateRAMP Category 1: NIST Low Impact Control Baseline: ~125 Controls
   - For Data Classification Category: Public
   - For data requiring: Integrity and Availability
   - For SaaS, PaaS, and IaaS vendors or service providers storing, processing, or transmitting Government public data

2) StateRAMP Category 3: NIST Moderate Impact Control Baseline: ~325 Controls
   - For Data Classification Category: Confidential
   - For data requiring: Confidentiality, Integrity, and Availability

- For SaaS, PaaS, and IaaS vendors or service providers storing, processing, or transmitting Government confidential data

StateRAMP agrees to provide the Government PoC with an account in the secure StateRAMP portal to view monthly reports on providers that the Government has sponsored and/or on providers who have given expressed permission for viewing privileges.

StateRAMP agrees to provide quarterly reviews with the Government Stakeholders. StateRAMP will provide Government a PoC with the PMO.

Please confirm your acceptance by signing in the space provided herein below and returning the signed document to StateRAMP.

StateRAMP, Inc.

By:
Date
Print Name:_____

Title: _____

[Government Entity]

By:
Date
Print Name:_____

Title: _____

Letter of Agreement Support Memo

DATE:

TO:

FROM:

RE: StateRAMP

StateRAMP is the only vendor certification that both verifies and validates all NIST 800-53 security controls and offers continuous monitoring visible to governments. StateRAMP follows the same verification model as FedRAMP which is required by the federal government for all vendor solutions that process, transmit and/or stores government data. StateRAMP offers that same level of assurance to state, local, higher education, K-12 and other local government entities, but with added visibility and communication that is not available under the FedRAMP models to these governments.

As a member of StateRAMP, sample language for inclusion in solicitation and contracts will be provided. This language was developed by cybersecurity professionals, government CIOs, procurement officials, and legal experts. It is (appropriate government name)'s recommendation that such language be considered for inclusion in all applicable solicitations and contracts involving the processing, transmission, storage and/or the ability to impact government data.

Government membership in StateRAMP is free and requires a Letter of Agreement which is respectfully attached for your review.

APPENDIX D

STATERAMP PMO ONBOARDING DOCUMENT

Introduction to PMO Onboarding

WHO SHOULD ATTEND?

Individuals who will have and control access to view vendor records.

WHAT TO EXPECT

The StateRAMP PMO team will walk through what records are available and how to access those records. Governments will be asked to provide a list of current and anticipated vendors with cloud services to search for and request access to those vendors already engaged with StateRAMP.

POINTS OF CONTACT

These individuals will have access to StateRAMP vendor files and artifacts for review. They will also be consulted prior to other government stakeholders gaining access.

Access Primary Point of Contact:

Name:

Email:

Access Secondary Point of Contact:

Name:

Email:

PREPARATION

There is no preparation for the meeting required. A list of current and anticipated contracts with name of vendor, vendor contact email and name of product and a bidder's list will be requested. PMO onboarding is more meaningful if this list is shared with StateRAMP prior to PMO onboarding.

Anticipated Date for submission of current contracts and bidder's list - _____.