# StateRAMP 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 as shown through StateRAMP Snapshot, Ready or Authorized status.

**Security and Control requirements** - The successful proposer‘s 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/Moderate/ High*).

**RAMP Ready Status** – Any resulting award will be made to selected respondent(s) offering a product that processes, stores, transmits and/or could impact government data, only if the proposal includes written documentation that the 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 –** Allcloud 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/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 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.