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.

☐ Complete StateRAMP Data Discovery form

- ☐ StateRAMP will provide the Data Discovery form.
- ☐ The government will gather information regarding all current contracts, RFP respondents from the last three years, and any upcoming RFPs involving the use of a cloud service offering including IaaS, PaaS, and SaaS systems that processes, store, and/or transmit government data including PII, PHI, and/or PCI.
- ☐ The government will use the above information to complete the StateRAMP Data Discovery form.

☐ Develop and adopt a security policy and sign the StateRAMP letter of agreement

- ☐ StateRAMP will provide a sample policy which requires suppliers utilizing a IaaS, PaaS or SaaS solution to 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 adopt and publish the security policy provided by StateRAMP or develop a similar policy for adoption and publication.
- ☐ The government will sign the StateRAMP Letter of Agreement.

☐ 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 CSPs.
- ☐ 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) CSPs are required to meet or exceed.

☐ Identify the security status requirement necessary for procurement

- ☐ StateRAMP will provide information about the different security statuses a CSP 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 CSP at the time of a contract initiation.
- ☐ The government will determine which security status to require from responding CSPs 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 CSPs understand what StateRAMP security status and security category are required.
- ☐ The government will determine which security status to require from responding CSPs at the time of RFP and upon contract initiation.

☐ Announce the new StateRAMP requirement to internal stakeholders and CSP community

- ☐ StateRAMP will provide a sample announcement that can be delivered to internal stakeholders as well as with the CSP community, including any CSP 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 CSP community.
- ☐ The government should coordinate with StateRAMP on the release of the announcement.
- ☐ StateRAMP will offer free education for government stakeholders and the CSP 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 CSPs for continuous monitoring to maintain their contract award.