THIRD PARTY ASSESSMENT ORGANIZATIONS

Standards, Accreditation, and StateRAMP Approval

VERSION:
1.0

DATE:
January 2021

TABLE OF CONTENTS

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
January 2021	Initial Publication	1.0	StateRAMP Staff

1. WHAT IS STATERAMP

StateRAMP provides a standardized approach to cybersecurity assessment, authorization, and continuous monitoring so that state and local governments can save time and money while improving their cybersecurity posture and ensuring their cloud data is protected. StateRAMP is an independent, not-for-profit, public-private partnership providing an efficient and cost-effective solution for verifying the cybersecurity profile of service providers on behalf of state and local governments. 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 protect citizen data; (2) save taxpayer and service provider 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 the Federal Risk and Authorization Management Program (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 service providers who offer IaaS, PaaS, or 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 service provider security packages, security statuses, and monthly and annual reporting tailored to the government's specific cybersecurity needs.

2. THE ROLE OF THE 3PAO IN STATERAMP

Third party assessment organizations (3PAOs) play an important role in the StateRAMP program. As certified independent assessors, 3PAOs are charged with performing initial and periodic assessments of service provider's solutions to ensure they meet the StateRAMP security standards required by state and local governments. In order to obtain a StateRAMP security status, service providers partner with 3PAOs to complete an evaluation of the service offering at one of the two StateRAMP security baselines: Category 1 and Category 3[*].

In order to ensure service providers receive independent, thorough, and consistent assessments, StateRAMP has adopted the same 3PAO accreditation standards required by FedRAMP and grandfathered all FedRAMP-approved 3PAOs into the StateRAMP program. To date, there are over 40 accredited 3PAOs approved by FedRAMP.

3. 3PAO ACCREDITATION STANDARDS

FedRAMP works with the American Association for Laboratory Accreditation (A2LA) to accredit and maintain the status of 3PAOs interested in conducting assessments. The A2LA 3PAO assessment process involves an in-depth evaluation of the technical competence of a 3PAO, and an independent verification and validation of 3PAO compliance with the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17020:2012 general requirements and additional FedRAMP specific requirements[†].

FedRAMP and A2LA update the accreditation standards and requirements are updated on a regular basis. The most recent update includes new and strengthened requirements related to 3PAO applicants, 3PAO personnel requirements for assessment teams, 3PAO assessment team training requirements, 3PAO renewal and service application, and updated subcontractor requirements. For additional information, see the A2LA publication R311-Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP).

[*] StateRAMP Category 1 is equivalent to FedRAMP Low Impact and StateRAMP Category 3 is equivalent to FedRAMP Moderate Impact. StateRAMP Category 2 is forthcoming.
[†] FedRAMP.gov