Leah dedicated more than 1,000 hours in 2020 working alongside Steering Committee members to develop StateRAMP’s governance and policy framework, and now serves as the non-profit’s first executive director.

Prior to her work with StateRAMP, Leah held leadership positions in both the public and private sector, including serving as the first deputy mayor of the City of Fishers, Indiana from 2015 - 2019.
Agenda

What is StateRAMP
  ◦ History
  ◦ How does it work for Providers
  ◦ How does it work for Government

How to Get Started with StateRAMP

Next Steps
About StateRAMP
As cyber threats grow, how do you know...

If a cloud solution is being used to deliver services that transmits, stores, processes and/or could impact security of Government data?

Bidders meet minimum security standards before making an award for contract?

Contracted vendor complies with your security standards throughout contract duration?
StateRAMP is a non-profit, 501c6, membership organization that brings together state and local governments, educational institutions, and special districts with the providers who serve them to promote best cyber practices and to establish a common set of security criteria.

A standard method of verifying cloud security:

- Allows providers to verify product’s security posture once to prove their cybersecurity compliance to all their government clients.
- Provides governments a shared resource for procurement and continuous compliance & monitoring.

Learn more at www.stateramp.org
StateRAMP Members

295 Individual Govt. Members
111 Provider Members

Government & Providers may join at
www.stateramp.org/register

*As of September 30, 2022
Growing Government Participation

Arizona
Arkansas (Judicial)
California
Colorado
Florida
Georgia
Maine
Massachusetts
Michigan
Nebraska (Judicial)
New Hampshire
North Carolina
North Dakota
Oklahoma
Texas
Vermont
West Virginia

Emerging Higher Ed + Local Government:
New York State Local Government IT Directors’ Association, UNC System, Sacramento County + More
How it Works & Security Requirements
Standing Committees

Standards & Technical

Dan Lohrmann, Chair  
Chief Strategist & Chief Security Officer  
Security Mentor  

Nancy Rainosek, Vice Chair  
Chief Information Security Officer, State of Texas  

Members:  
David Allen (Georgia)  
Glenn Herdrich (Sacramento Co.)  
Steve Nettles (Arizona)  
Jason Oskenhendler (Coolfire)  
Joe Bielawski (Board Member)  

Advisors:  
Phyllis Lee (Ctr Internet Security)  
Rick Zak (Microsoft)  
Maria Thompson (AWS)  
Noah Brown (StateRAMP PMO)  

Appeals

Owen Zorge, Chair  
State Compliance & Privacy Ofc  
City of Chandler, AZ  

Rich Banta, Vice Chair  
Co-owner & CISO,  
Lifelines Data Center  

Members:  
Chance Grubb (Oklahoma)  
Ted Cotterill (Board Member)  
Teri Takai (Ctr for Digital Govt)  

Advisors:  
Tony Bai (A-LIGN)  
Mase Izadjoo (Earthling Security)  

Approvals

David Allen, Chair  
Chief Information Security Officer  
State of Georgia  

Members:  
Jayson Cavendish (Michigan)  
Rob Main (North Carolina)  
Adam Mikeal (Texas A&M University)  
Antoine Charles (Oklahoma)  

Nominating

Jaime Schorr, Chair  
Chief Procurement Officer  
State of Maine  

Members:  
Fay Tan (NASPO ValuePoint)  
Doug Robinson (NASCIO)  
Dugan Petty (Advisor)  
J.R. Sloan (Board Member)  
Jay White (Mississippi)  
Paul Baltzell (Salesforce)
Templates & Resources

Governance committees adopt policies that define

- Baseline minimums standards
- Process for StateRAMP verification

Baseline requirements built on NIST 800-53 Rev. 4

- Rev. 5 in 2023
- Goal to map frameworks for CJIS, MARSE/MMIS/HIPAA and more

Find policies, templates and resources online

- www.stateramp.org/templates-resources
Verify Cloud Products Used by Public Agencies Meet Minimum Security Requirements

- Standardized Requirements (Based on NIST 800-53)
- Independent Annual Audits
- Centralized Program Management Office (PMO)
- Continuous Monitoring (Monthly Reporting + Annual Audit)
Authorized Product List (APL)

Public list on www.stateramp.org

Recognize progressing and verified statuses

Continuous monitoring is required to maintain a verified listing (Ready, Authorized, and Provisional)

Participating StateRAMP Governments provided secure access to portal to view continuous monitoring
Security Status Progression

**READY**
Meets minimum mandatory requirements and submits a completed 3PAO Readiness Assessment Report (SR-RAR).

**AUTHORIZED**
Requires Sponsor or Approvals Committee Support; Meets requirements by impact level and submits completed 3PAO Security Assessment Plan (SR-SAP) and documentation.

**PROVISIONAL**
Requires Sponsor; Meets minimum requirements for Ready; but not all for Authorized; Sponsor may assign Provisional Status.
StateRAMP Impact Levels

Government entity defines required procurement/contract security impact level. StateRAMP Impact Level Categories align to NIST 800-53 Rev. 4 (Rev. 5 in 2023).

**Low**
- StateRAMP Low Control Baselines

**Low+**
- StateRAMP Low+ Control Baselines

**Moderate**
- StateRAMP Moderate Control Baselines

**High**
- FedRAMP High Control Baselines

View Data Classification Tool at: [www.stateramp.org/templates-resources](http://www.stateramp.org/templates-resources).
# StateRAMP and FedRAMP

https://stateramp.org/blog/

<table>
<thead>
<tr>
<th>Feature</th>
<th>StateRAMP</th>
<th>FedRAMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on NIST 800-53 Rev. 4</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Requires annual independent Third Party Assessment Organization (3PAO) Audit</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Requires Monthly Continuous Monitoring</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Impact Levels of Low, Moderate, and High</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Verified statuses of Ready and Authorized</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Available to any provider, regardless of federal contract status</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Documentation available to federal, state, local, public education institutions, and special districts</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Centralized PMO reviews all security packages to ensure consistent application of standards and verification</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Fast Track option for products with FedRAMP or StateRAMP</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Plans for mapping to other compliance frameworks: CJIS, MARSE, MMIS, IRS</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Nonprofit mission to improve cyber posture for state, local, public education institutions and special districts and providers who serve them</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Continuous Monitoring

Providers must comply with Continuous Monitoring requirements to maintain status Ready, Authorized or Provisional.

View Continuous Monitoring Policies & Escalation Process for more:
www.stateramp.org/templates-resources.
Getting Started
Become a Member of StateRAMP

Government Membership
Individual + Certified Government Membership
No Cost to Government
www.stateramp.org/register

Schedule a call for your team:
Rebecca@stateramp.org

Provider Membership
Provider Membership
$500 Annual Membership Fee
www.stateramp.org/register

Schedule a call for your team:
info@stateramp.org

View *Getting Started Guides* for Government and Providers at www.stateramp.org
Government Adoption Support

StateRAMP Implementations Team Support

- Overall Procurement Implementation
- Overall InfoSec Implementation
- Onboarding to PMO Portal for ConMon
- Solicitation and Contract Language
- Education and Training
- Vendor Outreach
- Reporting and Communication

Schedule a meeting! Email info@stateramp.org.
Coming Soon: Bridge to StateRAMP

StateRAMP Security Snapshot

- StateRAMP will make available to providers and governments a new “pre-Ready” assessment, known as the StateRAMP Security Snapshot.
  - Available for products not yet achieved a verified security status of StateRAMP Ready, Authorized or Provisional
  - Snapshot to include a score that assesses the level of cyber maturity of the product in relation to achieving StateRAMP Ready

- Help bridge the transition to StateRAMP for providers and governments.
  - May be incorporated into solicitation requirements to provide governments an ability to assess NIST maturity upfront, while providers work to achieve StateRAMP authorization.
StateRAMP Security Snapshot in Procurement Process

Steps for Getting Started

1. Identify Security Impact Level Required (Use StateRAMP Data Classification Tool)

2. Require StateRAMP Security Snapshot Score as a Deliverable for Solicitation Response that is No Older than 6 Months at Submission. StateRAMP Ready, Authorized or Provisional Certifications exceed this requirement.

3. Require updated StateRAMP Security Snapshot within 6 months after Contract Execution (Note: This will demonstrate whether progress is being made toward StateRAMP authorization.)

4. Require StateRAMP Ready within 12 months of Contract Execution (Continuous Monitoring Begins)

5. Require StateRAMP Provisional/Authorized within 18 Months of Contract Execution
SECURITY FRAMEWORK & CONTRACTOR REQUIREMENTS
The State information security policies and standards adhere to the National Institute of Standards and Technology (NIST) 800-53 revision 4 (or latest version adopted by StateRAMP).

A contract will not be executed with a contractor that utilizes a cloud system to process, store and/or transmit government data, unless and until the service provider has achieved StateRAMP Ready Status. The Ready Status serves as an attestation to the providers capabilities to achieve full authorization.

The State requires all cloud systems that process, store and/or transmit government data must demonstrate compliance with NIST 800-53 at StateRAMP Impact Level (Low/Moderate/High/Specific State Requirements) by achieving StateRAMP authorization within 12 months of contract execution for the appropriate data classification.

Once a contract is issued, the provider must achieve full StateRAMP authorization within twelve (12) months. All contractors must comply with required continuous monitoring to maintain StateRAMP authorizations.

The State 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 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. Information about StateRAMP can be found at www.stateramp.org.
Resources
Helpful Links

[Image 16x7 to 122x36]
[Image 330x64 to 736x389]
[93x443]www.stateramp.org

Get Started as a Participating Government: rebecca@stateramp.org

Join as an Individual Government Member: www.stateramp.org/register

Join as a Provider Member: www.stateramp.org/register

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

Governance & Documents: www.stateramp.org/documents

Request a Security Review for Ready or Authorized: www.stateramp.org/providers

Future Events: www.stateramp.org/events

Blogs: www.stateramp.org/blog
Common FAQ
SOC 2 v. StateRAMP Audits

**SOC 2**

A SOC 2 report is a measurement against self-established security controls, procedures, and policies.

SOC 2 is a framework designed by financial experts of the American Institute of CPAs and “is intended to meet the needs of a broad range of users.”

**STATERAMP**

StateRAMP compliance is a measurement against a standard set of security controls, procedures, and policies established by the StateRAMP Committees.

StateRAMP requirements are designed by cyber security professionals specifically to measure compliance with NIST 800-53 for State and Local Government.
StateRAMP v. SOC 2 Audits for NIST 800-53

SOC 2 NIST 800-53 Compliance

14.8%

*Assumes audited CSP selects all 42 NIST Controls for audit

StateRAMP NIST 800-53 Compliance

100%

*StateRAMP audits are the same every time. Control requirements vary only by Impact Level.
Implementation Requirements are Critical

SOC 2 is a framework, not a control catalog. As such, its controls are not descriptive and allow interpretation of implementation.

- StateRAMP and FedRAMP have specific requirements and implementations for NIST 800-53 controls.
- The gap in SOC 2 coverage of NIST 800-53 controls is due to the lack of implementation requirements.

See following slides for example of differing requirements and impact.
Example of Differing Requirements

Below is an example of differing requirements for Access Control related to Password Requirements.

SOC 2 requires self-definition, while StateRAMP requires specific NIST 800-53 compliance.

**SOC 2**

“Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.”

**StateRAMP**

NIST: “The information system, for password-based authentication:

(a) Enforces minimum password complexity of case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters;

(b) Enforces at least the following number of changed characters when new passwords are created: at least one

(c) Stores and transmits only encrypted representations of passwords;

(d) Enforces password minimum and maximum lifetime restrictions of one day minimum, sixty day maximum;

(e) Prohibits password reuse for twenty four generations; and

(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.”
Example of Differing Requirements

This chart illustrates the difference in password compliance for audits.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>StateRAMP / NIST</th>
<th>SOC 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined number of characters</td>
<td>12</td>
<td>None</td>
</tr>
<tr>
<td>Required Upper Case Letters</td>
<td>At least one</td>
<td>None</td>
</tr>
<tr>
<td>Required Lower Case Letters</td>
<td>At least one</td>
<td>None</td>
</tr>
<tr>
<td>Required Numbers</td>
<td>At least one</td>
<td>None</td>
</tr>
<tr>
<td>Required Special Characters</td>
<td>At least one</td>
<td>None</td>
</tr>
<tr>
<td>Requires new password to not be the same as old password?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Password transmission must be encrypted</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Minimum age of password</td>
<td>1 Day</td>
<td>None</td>
</tr>
<tr>
<td>Maximum age of password</td>
<td>60 days</td>
<td>None</td>
</tr>
<tr>
<td>Prohibit password re-use</td>
<td>24 generations</td>
<td>None</td>
</tr>
</tbody>
</table>
Impact of Differing Requirements on Compliance

In this example, password compliance differs significantly.

**SOC 2**

Compliant IF:

Define a password as being four numbers

*Requirement self-defined*

**StateRAMP**

Compliant IF:

Password has “minimum of 12 characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters, one character change with each password changes, only transmit passwords encrypted, require lifetime restriction of one-day minimum and 60-day maximum, and prevent reuse of the previous 24 passwords”

*Requirement set by NIST 800-53*
Impact of Differing Requirements on Risk

More importantly, in this example, risk differs significantly.

**SOC 2**

4 Digit Password could be cracked instantly with brute force

**StateRAMP**

NIST Password would take 3,000 years