The presentation will begin shortly.

THANK YOU FOR JOINING US!
Our mission is to promote cybersecurity best practices through education, advocacy, and policy development to support its members and improve the cyber posture of state and local governments and the citizens they serve.

StateRAMP brings together public and private voices to establish a common set of security criteria so a standard method of verifying cloud security can be recognized.

This standardized approach allows providers serving state and local governments to verify their security posture and prove their cybersecurity compliance to their government clients.

Learn more at www.stateramp.org
# StateRAMP v. FedRAMP

<table>
<thead>
<tr>
<th>StateRAMP</th>
<th>Both</th>
<th>FedRAMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>• PMO Support for Government and Service Providers</td>
<td>• Built on NIST 800-53 Rev. 4</td>
<td>• Must do business with federal government</td>
</tr>
<tr>
<td>• Centralized PMO</td>
<td>• Requires 3PAO Audit</td>
<td>• JAB v. Agency PMO</td>
</tr>
<tr>
<td>• States/Locals have visibility into ConMon</td>
<td>• Impact Levels Low, Moderate and High</td>
<td>• Federal have visibility in ConMon</td>
</tr>
<tr>
<td>• Ready Status does not expire (ConMon required)</td>
<td>• Require ConMon</td>
<td>• Provisional Status awarded by Joint Authorized Board (JAB) v. Agency</td>
</tr>
<tr>
<td>• Provisional Status awarded by government sponsor.</td>
<td>• Verified Statuses of Ready and Authorized</td>
<td></td>
</tr>
<tr>
<td>• Fast Track option for products with FedRAMP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** ConMon indicates the use of continuous monitoring in the authorization process.
LEAH MCGRATH
EXECUTIVE DIRECTOR
LEAH@STATERRAMP.ORG | 317-806-0054
Problem Statement

How to provide state and local government procurement and security officials assurance that their contractors have the processes and capabilities necessary to deliver with the appropriate security controls in place

Goals

- Standardized approach
- Meet minimum requirements
- Consistency in RFPs
- Best value

Outcome

Improve security for state and local government
Board of Directors & Steering Committee

J.R. Sloan  
CIO  
State of Arizona

Ted Cotterill  
CPO / General Counsel  
State of Indiana

Joe Bielawski  
President  
Knowledge Services

Rich Banta  
CISO & Managing Partner  
Lifeline Data Centers

Tony Bai  
Federal Practice Lead  
A-LIGN

Paul Baltzell  
Vice President Strategy & Bus. Dev.  
Salesforce

Curtis Dukes  
Executive VP Center for Internet Security

Dan Lohrmann  
Chief Strategist & CISO  
Security Mentor

Steve Nettles  
Procurement Group Mgr.  
State of Arizona

Jason Oksenhendler  
Sr. Mgr., Cyber Security  
Coalfire

Dugan Petty  
Advisor  
Retired CIO / CPO

Doug Robinson  
Executive Director  
NASCIO

Tim Roemer  
Dir. Homeland Security + CISO  
State of Arizona

Jaime Schorr  
Chief Procurement Officer  
State of Maine

Teri Takai  
Vice President Center for Digital Govt.

Fay Tan  
NASPO ValuePoint

Paul Toomey  
CEO  
Geographic Solutions

Jay White  
CISO  
State of Mississippi

Owen Zorge  
CISO  
City of Chandler, AZ

Not pictured: Tom Considine, Sr., Sr. InfoSec/AZRamp, State of Arizona
## Standards & Technical

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

### Members:
- David Allen (Georgia)  
- Glenn Herdrich (*Sacramento Co.*)  
- Steve Nettles (Arizona)  
- Jason Oskenhendler (Coalfire)  
- Nancy Rainosek (Texas)  
- 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*)

## 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)
Government members can join at no cost.

Arizona and Texas adopting RAMP Programs

Government and Providers can become members by completing forms at:
www.stateramp.org/register
StateRAMP Verification Process

State or Local Government
Policy defines cyber requirements for Service Providers

Provider
Engages accredited and approved Third Party Assessment Organization (3PAO) to complete assessments & audit

3PAO
Completes audit of Provider’s security and submits Security Package to StateRAMP for review

StateRAMP
Reviews 3PAO-submitted Security Package and assigns Security Status of Provider, publishing status
Procurement Process

- Incorporate requirements into RFPs and contracts
- Announce requirements to vendor community
- Work with CIO/CISO to evaluate existing contracts

Policy defines cyber requirements for Service Providers

States or Local Government

Set Control Requirements with CISO and Owner
Identify StateRAMP Impact Level Category
Identify Security Status Level
Set Status Level Deadline
Set Continuous Monitoring
Confirm Impact Level Compliance w/3PAO
Confirm Compliance Continuous Monitoring

RFP Development  Eval/Award  Contract Admin
## Authorized Vendor List

### Security Status Categories

**Verified** *(Ready, Authorized & Provisional)*

**Progressing** *(Active, In Process & Pending)*

---

### StateRAMP Authorized Vendors

StateRAMP establishes common security criteria to standardize cloud security verification.

Verified offerings and those in the process of working toward an authorization are listed on the Authorized Vendor List (AVL) below. The AVL, first published September 14, 2021, is updated weekly.

<table>
<thead>
<tr>
<th>Company</th>
<th>Product Name</th>
<th>Security Status</th>
<th>Service Model</th>
<th>Impact Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zoomer</td>
<td>Zcomer Internet Access - Government (Secure Web Gateway - TIC)</td>
<td>Ready</td>
<td>SaaS</td>
<td>Moderate</td>
</tr>
<tr>
<td>Zoomer</td>
<td>Zcomer Private Access - Government (Zero Trust Networking - VPR Replacement)</td>
<td>Ready</td>
<td>SaaS</td>
<td>Medium</td>
</tr>
<tr>
<td>Project Hosts, Inc.</td>
<td>Project Hosts Federal Private Cloud</td>
<td>Ready</td>
<td>PayGo</td>
<td>Moderate</td>
</tr>
<tr>
<td>Knowledge Services</td>
<td>dotSift</td>
<td>Ready</td>
<td>SaaS</td>
<td>Moderate</td>
</tr>
<tr>
<td>Aurigo Software Technologies Inc.</td>
<td>Masterworks Cloud and Aurigo Essential's</td>
<td>Pending</td>
<td>SaaS</td>
<td>Moderate</td>
</tr>
<tr>
<td>OICLC</td>
<td>WorldShare Management Services</td>
<td>Pending</td>
<td>SaaS</td>
<td>Low</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>BlackBerry Government Mobility Suite (BGMS)</td>
<td>InProcess</td>
<td>SaaS</td>
<td>Moderate</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>BlackBerry Cloud - Android Services for Government (ACGforGov)</td>
<td>InProcess</td>
<td>SaaS</td>
<td>Moderate</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>BlackBerry Protect</td>
<td>InProcess</td>
<td>SaaS</td>
<td>Moderate</td>
</tr>
<tr>
<td>Boomi</td>
<td>AlertSphere</td>
<td>InProcess</td>
<td>SaaS</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

Showing 1 to 10 of 51 entries

To manage cyber risk and protect critical data, systems, and infrastructure from cyber-attacks and ransomware, it is recommended that state and local governments verify the cybersecurity posture of their cloud solution providers.

**What this means for Service Providers:** This standardized approach allows providers serving state and local governments to verify the security posture and prove their cybersecurity compliance to their government clients.

**What this means for State and Local Government:** StateRAMP’s shared resource model and continuous monitoring simplifies cloud compliance and risk management for government agencies who participate with StateRAMP.
Steps for a Provider to Verify an Offering

Provider Decides to Become a StateRAMP Member

If Federal Authorization, see StateRAMP FastTrack

Provider Engages Approved 3PAO to Begin Assessment

Complete Ready Review packet

State Sponsors Product for Authorization

Ready

Complete Authorization Review Packet

Authorized Provisional
Templates & Resources

www.stateramp.org/templates-resources

Policies
◦ Security Assessment Framework
◦ Data Classification
◦ Baseline Security Controls
◦ Minimum Mandatory Requirements for Ready
◦ Continuous Monitoring Guide

Documents & Templates

Authorized Vendor List Resources
Security Impact Levels

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

<table>
<thead>
<tr>
<th>Impact Level</th>
<th>StateRAMP Low Control Baselines</th>
<th>*Low + StateRAMP Low + Select Moderate Controls</th>
<th>Moderate StateRAMP Moderate Control Baselines</th>
<th>High FedRAMP High Control Baselines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Low +</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Low+ not currently available.
Security Status Progression

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

Requires Sponsor; meets mandatory minimums and deemed to meet most, but not all requirements, Sponsor may assign Provisional Status.

Requires Sponsor; Meets requirements by impact level and submits completed 3PAO Security Assessment Plan (SR-SAP) and documentation.
A Government Sponsor is required for Authorization

Eligible Government Sponsors include:
- Any SLED government official or employee who serves in the role of Chief Information Security Officer or designee; and a Member of StateRAMP

Government Sponsors Agree to the Following:
- Designate an Information Security Authorizing Official, who will be provided access to the secure portal
- Review PMO recommendations and associated artifacts
- Accept, reject, or make suggestions for modification to the PMO’s recommendations regarding Authorizations, continuous monitoring, and annual renewal
StateRAMP Fast Track

Federal Authorizations
- Ready
- ATO
- P-ATO

Required Documentation
- Security Packet as submitted and approved
- Prior 90 days of Continuous Monitoring

PMO Review
- Call to Review Boundary and Architecture
- Review Submission

Read our blog about StateRAMP Fast Track at www.stateramp.org/blog
Continuous Monitoring

Providers must comply with Continuous Monitoring requirements to maintain status of Authorization or Provisional

*Annual Audit must be provided in StateRAMP templates
PMO Review for Authorized Vendor List

StateRAMP Authorized Vendor List

Cost for Subscriber Members to List Offering on StateRAMP Authorized Vendor List:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>$2,500</strong></td>
<td><strong>$5,000</strong></td>
<td><strong>$5,000</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Ready Review</strong></td>
<td><strong>Authorization Review</strong></td>
<td><strong>Annual Fee</strong></td>
<td></td>
</tr>
<tr>
<td>conducted by PMO to verify requirements for Ready Status</td>
<td>conducted by PMO to verify requirements for Authorization Status</td>
<td>for Continuous Monitoring to verify requirements are met ongoing</td>
<td></td>
</tr>
</tbody>
</table>

Inaugural year pricing
Creating a framework for verification and continuous improvement in cybersecurity for state and local governments and their providers

- Shared Services Model for SLED
- “Verify Once, Use Many” Approach for Providers
- Centralized Resources for SLED & Providers
- Standard Path for Procurement to Verify Security
- Ongoing Education & Best Practices
- Government-Led Governance & Collaboration
Get Started

www.stateramp.org

Join at: www.stateramp.org/register

Resources at: www.stateramp.org/templates-resources

Future events at: www.stateramp.org/Events

info@stateramp.org
Questions?

THANK YOU.