StateRAMP

Streamline Procurement & Strengthen Security

June 2023

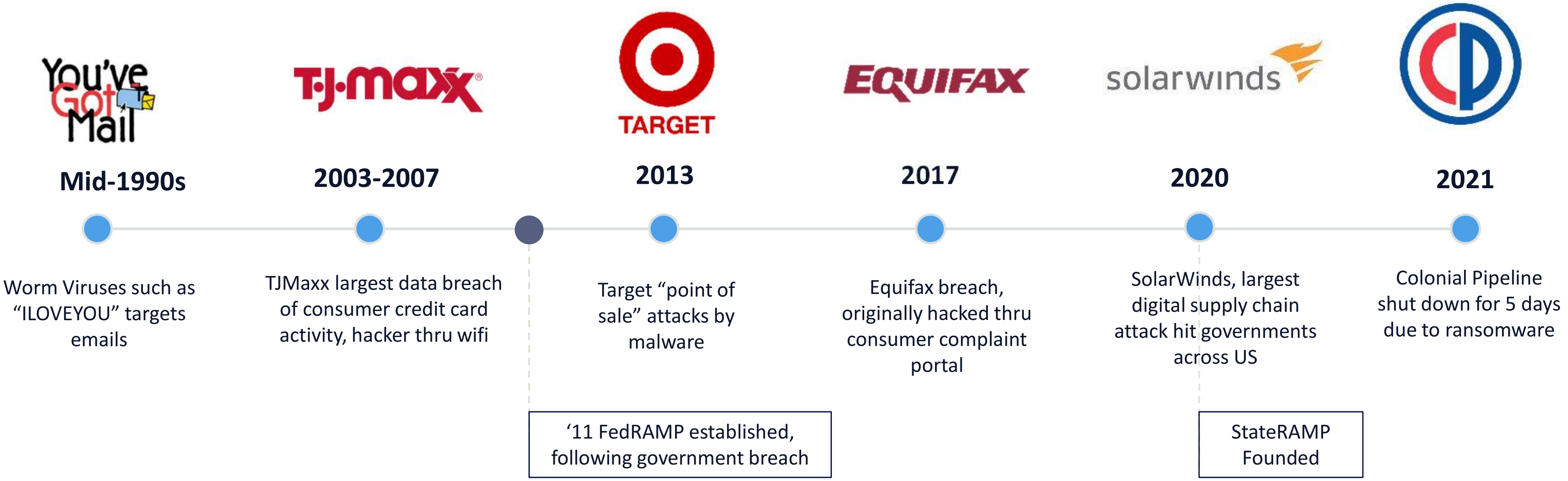
The Future of Government & Technology

Technology is rapidly increasing government's ability to engage and serve citizens in more **rapid, responsive, and business-friendly ways**

- Significant level of business done via email
- Online license renewals/registrations
- Tax returns
- Digital identity considerations

"By 2025, over 50% of government agencies are predicted to have modernized critical core legacy applications to improve resilience and agility" – Gartner, Top 10 Government Technology Trends

Cyber Threats: A Reality We Cannot Ignore



Mid-1990s

Worm Viruses such as "ILOVEYOU" targets emails

2003-2007

TJMaxx largest data breach of consumer credit card activity, hacker thru wifi

'11 FedRAMP established, following government breach

2013

Target "point of sale" attacks by malware

2017

Equifax breach, originally hacked thru consumer complaint portal

2020

SolarWinds, largest digital supply chain attack hit governments across US

StateRAMP Founded

2021

Colonial Pipeline shut down for 5 days due to ransomware

StateRAMP

StateRAMP is a non-profit, with members in the public and private sectors with a mission to promote best practices in cloud cybersecurity and a standardized approach to verifying cloud solutions.

Members leverage standardized assessments to verify cloud security.

Ongoing information sharing helps partners manage risk and continuously improve.

What is StateRAMP

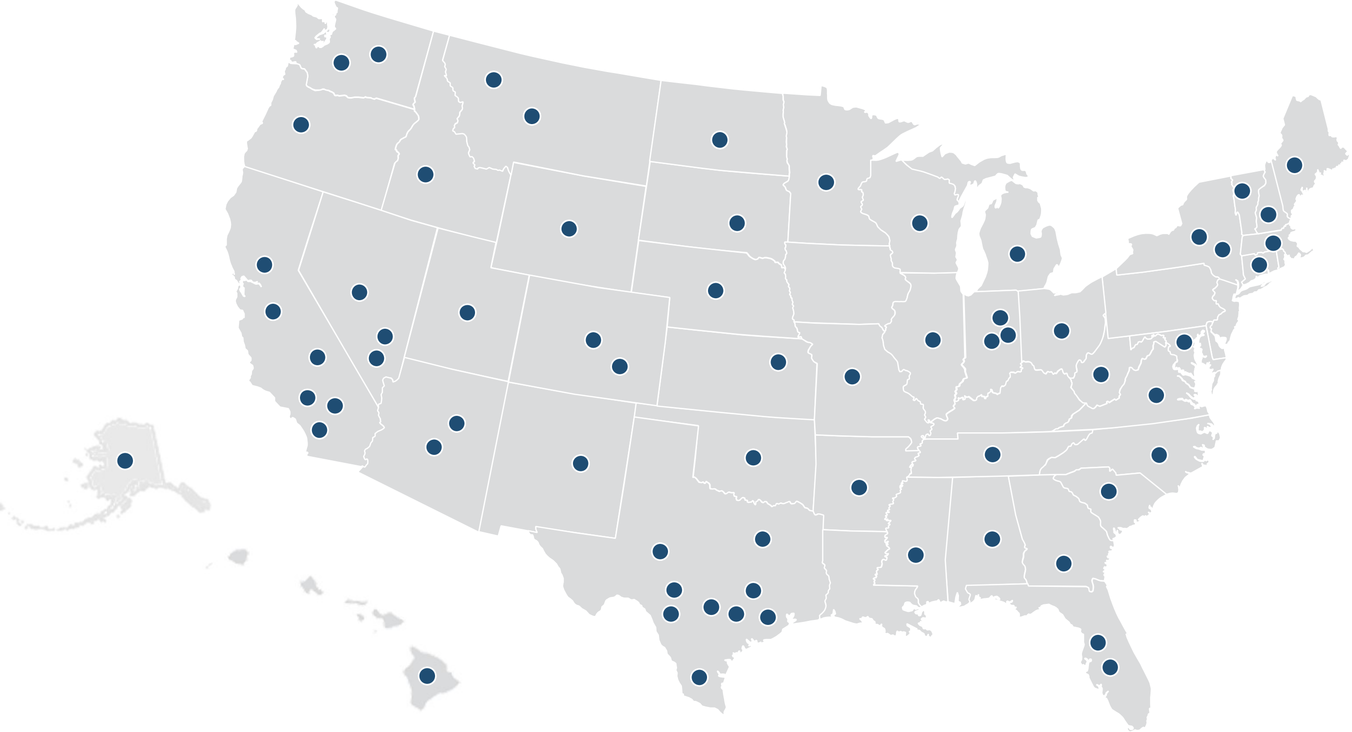
StateRAMP is focused on promoting cybersecurity best practices through education and policy development to improve the cyber posture of public institutions and the citizens they serve

StateRAMP was created as a public-private venture to bring public sector interests, industry interests, and auditor interests together to create a **seamless process and platform for:**

- Gain clear, ongoing insight into the cybersecurity posture of business partners
- Relieve burden on procurement and IT/Info Sec teams to review diverse compliance frameworks
- Advance risk management strategy further upstream

- Gain a verify once, serve many approach to compliance
- Demonstrate ‘trusted partner’ status
- Reduce barriers to competition through a comprehensive compliance framework

StateRAMP Members



356 Individual Govt. Members
141 Provider Members

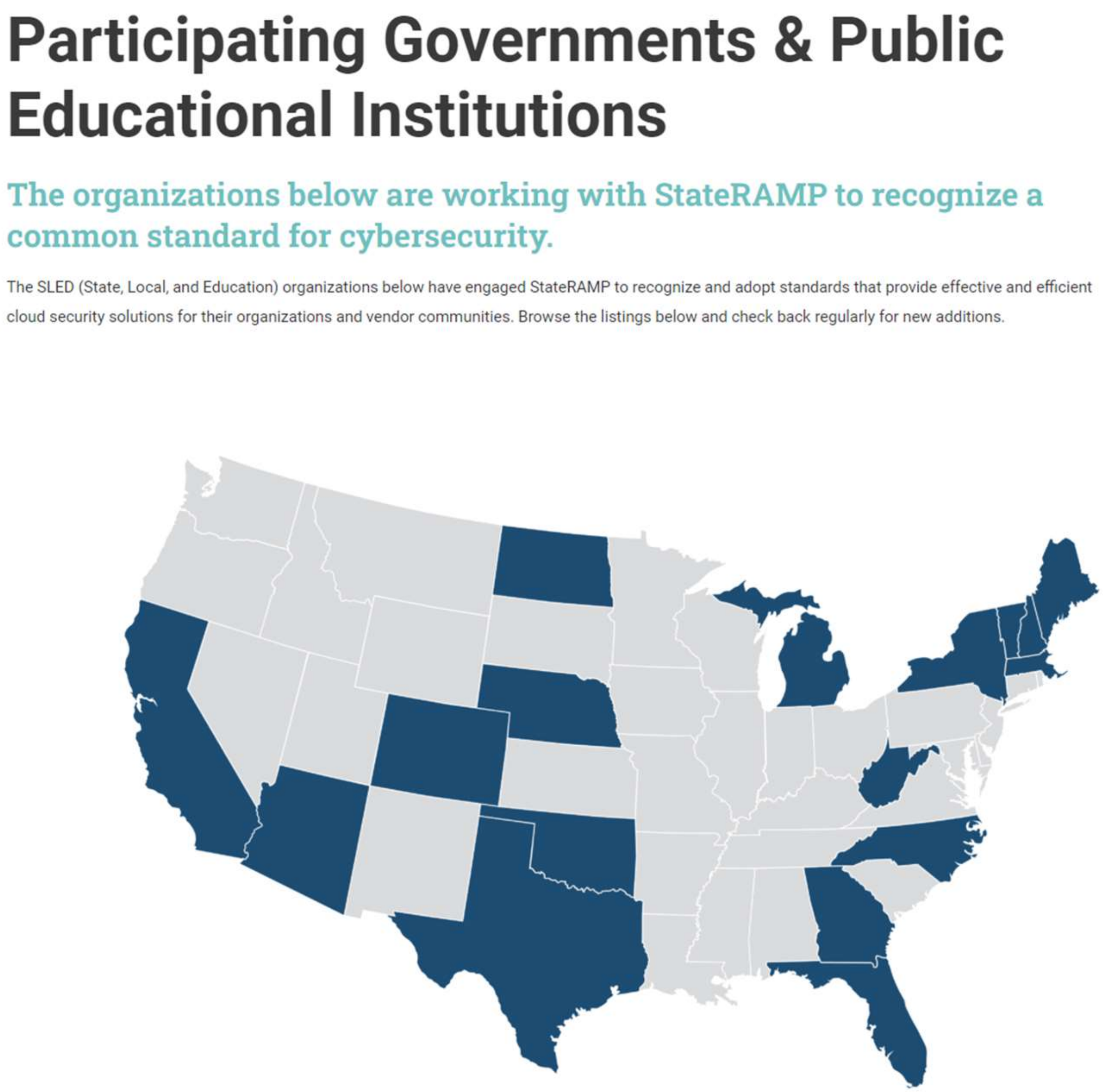
Government & Providers may join at
www.stateramp.org/register

*As of Jan. 1, 2022

Government Participation

View more at www.stateramp.org/participating-governments

StateRAMP



Participating Governments & Public Educational Institutions

The organizations below are working with StateRAMP to recognize a common standard for cybersecurity.

The SLED (State, Local, and Education) organizations below have engaged StateRAMP to recognize and adopt standards that provide effective and efficient cloud security solutions for their organizations and vendor communities. Browse the listings below and check back regularly for new additions.

StateRAMP Board of Directors

J.R. Sloan, Chief Information Officer, State of Arizona

Joe Bielawski, President, Knowledge Services

Ted Cotterill, Chief Privacy Officer, State of Indiana / General Counsel, Management Performance Hub

Dugan Petty, Retired NASPO ValuePoint, Subject Matter Expert

Glenn Herdrich, Information Security Manager, Sacramento County

StateRAMP

Standing Committees

Standards & Technical

Sean Hughes, Chair
Assistant Secretary for Technology, Security, and Operations/Chief Operating Officer, Massachusetts
Dan Lohrmann, Vice Chair
Field Chief Information Security Officer, Public Sector, Presidio

Members:
Danielle Cox *(West Viriginia)*
Charles Rote *(Maine)*
Matthew Kelly *(Texas)*
Steve Nettles *(Arizona)*
Jason Oskenhendler *(Coalfire)*
Joe Bielawski *(Board Member)*
Rick Zak *(Microsoft)*

Advisors:
Jim Garrett *(Missouri)*
Earl Crane *(UT Austin)*
Phyllis Lee *(Ctr Internet Security)*
Maria Thompson *(AWS)*
James Mason *(NASPO)*
Rashad Munawar *(BlackBerry)*
Siddique Chaudhry *(Snowflake)*

Appeals

Owen Zorge, Chair
Chief Information Security Officer
City of Chandler, AZ

Ray Yepes, Vice Chair
Chief Information Security Officer, Colorado

Members:
Ted Cotterill *(Board Member)*
Teri Takai *(Ctr for Digital Govt)*
Charlie Mewshaw *(Fayetteville State University)*
Rich Banta *(Lifelines Data Center)*
Ramanuj Kushwaha *(Cisco)*

Advisors:
Jeff Wann *(Missouri)*
Neil Slagle *(City of Springfield)*
Jennifer Hawks *(NCC Group)*
Tony Bai *(A-LIGN)*
Mase Izadjoo *(Earthling Security)*

Approvals

Antoine Charles, Chair
Third Party Risk Analyst, Oklahoma

Todd Ryan, Vice Chair
Chief Information Officer, Hillsborough County

Members:
Jayson Cavendish ***(Michigan)***
Josh Kadrmas *(North Dakota)*
Adam Mikeal *(Texas A&M University)*

Nominating

Fay Tan, Chair
Legal Counsel, NASPO

McCall Ginsberg, Vice Chair
Deputy General Counsel, Georgia Department of Administration

Members:
Doug Robinson *(NASCIO)*
Dugan Petty *(Advisor)*
J.R. Sloan *(Board Member)*

Steering Committee

-Founding Steering Committee Members, Strategic Partners, and Committee Chairs

Committee Charters

- Steering Committee
- Standards & Technical Committee
- Nominating Committee
- Appeals Committee
- Approvals Committee
- Board of Directors

Why StateRAMP

StateRAMP is a tool used to fill the gap between IT and procurement when it comes to ensuring that the service providers that **touch, transmit, or hold our public sector and critical infrastructure's data** have a truly **robust cybersecurity posture**

Current State

- Complex review process with diverse compliance frameworks, comparing apples to oranges, **creates a business 'unfriendly' process**
- Limited review, due to lack of bandwidth, **leads to concerns about true security**
- Self-attestation from service providers potentially leaves a **wide security gap**

How StateRAMP Works

For Public Sector Organizations

- Share procurement templates and best practices with participating public sector organizations
- Assists with incorporating StateRAMP compliance standards into existing procurement documents
- Supports vendor & stakeholder education on StateRAMP
- Provides ongoing education and awareness on procurement & security best practices
- Offers ongoing insight into vendor security posture through continuous monitoring

For Service Providers

- PMO supports Snapshot review – think credit score for cyber posture
- Offers progressing support for closing gaps in cybersecurity posture
- Coordinates vendor path to achieving StateRAMP Authorized
- Coordinates Continuous Monitoring Portal access by public sector institutions
- Shares Authorized Product List
- Manages membership & benefits

Security Framework

StateRAMP Baselines

Governance committees adopt policies that define

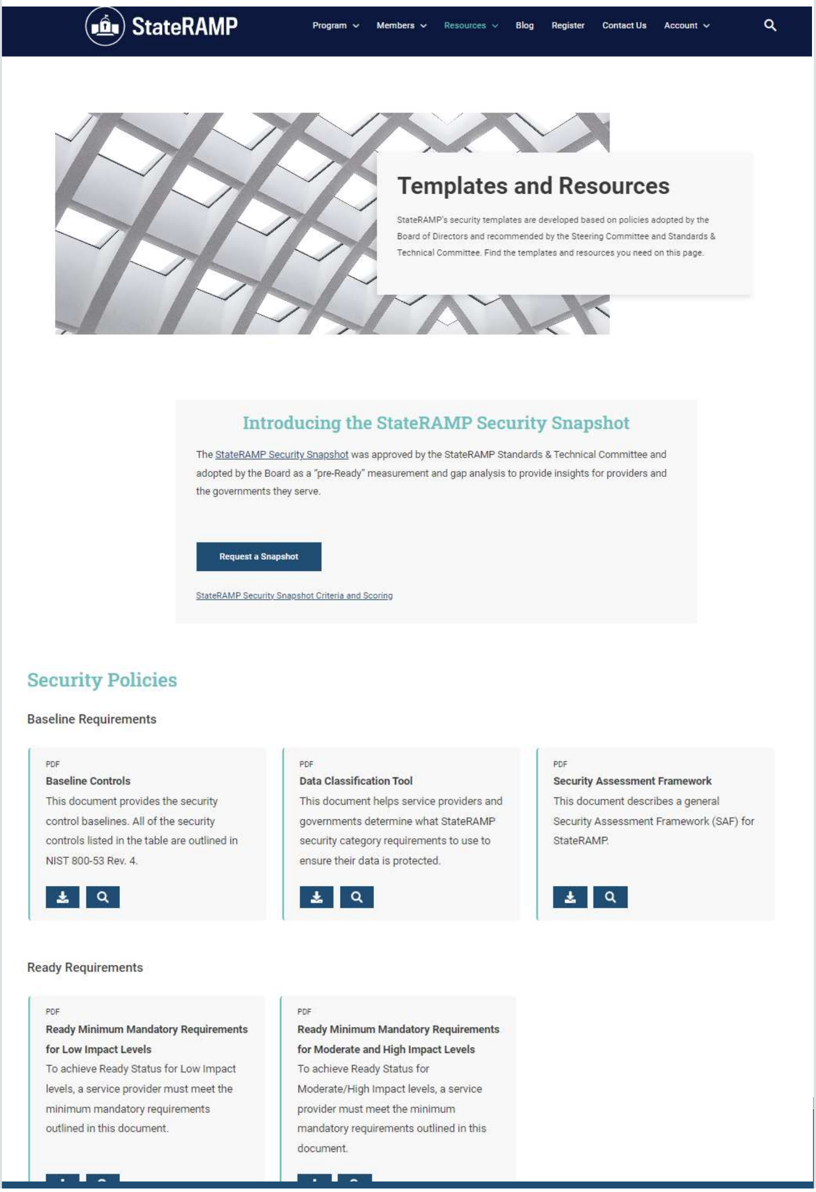
- Baseline minimums standards
- Criteria for StateRAMP Security Snapshot
- Process for StateRAMP verification for Ready & Authorized

Baseline requirements built on NIST 800-53 Rev. 4

- Rev. 5 Baselines adopted, effective in 2024
- Goal to map frameworks for CJIS, IRS, MARSE/MMIS/HIPAA and more

Find policies, templates and resources online

- www.stateramp.org/templates-resources



Templates and Resources

StateRAMP's security templates are developed based on policies adopted by the Board of Directors and recommended by the Steering Committee and Standards & Technical Committee. Find the templates and resources you need on this page.

Introducing the StateRAMP Security Snapshot

The StateRAMP Security Snapshot was approved by the StateRAMP Standards & Technical Committee and adopted by the Board as a "pre-Ready" measurement and gap analysis to provide insights for providers and the governments they serve.

StateRAMP Security Snapshot Criteria and Scoring

Security Policies

Baseline Requirements

PDF
Baseline Controls
This document provides the security control baselines. All of the security controls listed in the table are outlined in NIST 800-53 Rev. 4.

PDF
Data Classification Tool
This document helps service providers and governments determine what StateRAMP security category requirements to use to ensure their data is protected.

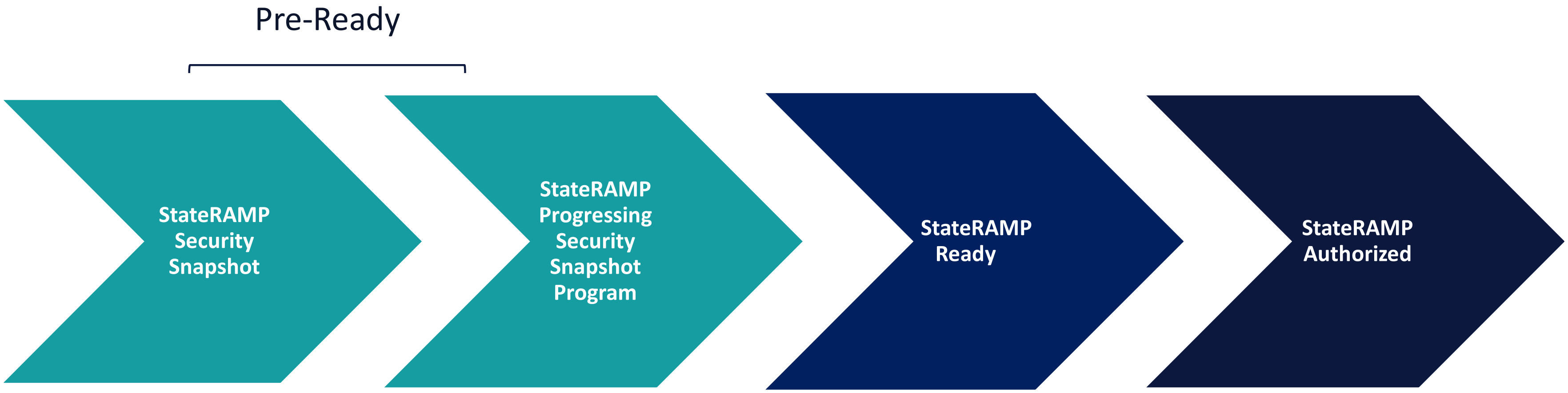
PDF
Security Assessment Framework
This document describes a general Security Assessment Framework (SAF) for StateRAMP.

Ready Requirements

PDF
Ready Minimum Mandatory Requirements for Low Impact Levels
To achieve Ready Status for Low Impact levels, a service provider must meet the minimum mandatory requirements outlined in this document.

PDF
Ready Minimum Mandatory Requirements for Moderate and High Impact Levels
To achieve Ready Status for Moderate/High Impact levels, a service provider must meet the minimum mandatory requirements outlined in this document.

How Do Providers Get Started with StateRAMP


Pre-Ready
StateRAMP Security Snapshot
StateRAMP Progressing Security Snapshot Program
StateRAMP Ready
StateRAMP Authorized

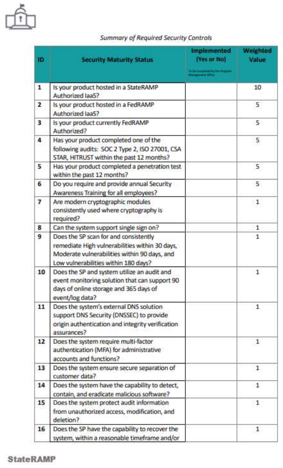
Path available to any provider to begin cyber maturity assessment

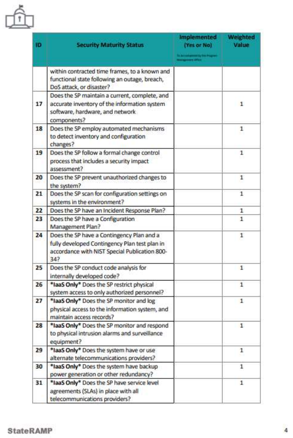
Providers may provision access to share reporting and continuous monitoring with their government clients.

Progressing Security Snapshot Program

Combines trust but verify principles and a consultative approach to improve cyber maturity for providers and begin information sharing critical to effective risk management for government.

StateRAMP Security Snapshot





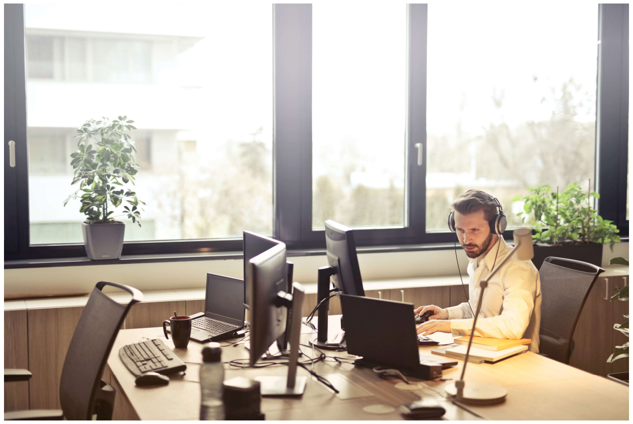
Summary of Required Security Controls

ID	Security Maturity Status	Implemented (Yes or No) To be completed by the Program Management Office	Weighted Value
1	Is your product hosted in a StateRAMP Authorized IaaS?		10
2	Is your product hosted in a FedRAMP Authorized IaaS?		5
3	Is your product currently FedRAMP Authorized?		5
4	Has your product completed one of the following audits: SOC 2 Type 2, ISO 27001, CSA STAR, HITRUST within the past 12 months?		5
5	Has your product completed a penetration test within the past 12 months?		5
6	Do you require and provide annual Security Awareness Training for all employees?		5
7	Are modern cryptographic modules consistently used where cryptography is required?		1
8	Can the system support single sign on?		1
9	Does the SP scan for and consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days?		1
10	Does the SP and system utilize an audit and event monitoring solution that can support 90 days of online storage and 365 days of event/log data?		1
11	Does the system's external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances?		1
12	Does the system require multi-factor authentication (MFA) for administrative accounts and functions?		1
13	Does the system ensure secure separation of customer data?		1
14	Does the system have the capability to detect, contain, and eradicate malicious software?		1
15	Does the system protect audit information from unauthorized access, modification, and deletion?		1
16	Does the SP have the capability to recover the system, within a reasonable timeframe and/or within contracted time frames, to a known and functional state following an outage, breach, DoS attack, or disaster?		1
17	Does the SP maintain a current, complete, and accurate inventory of the information system software, hardware, and network components?		1
18	Does the SP employ automated mechanisms to detect inventory and configuration changes?		1
19	Does the SP follow a formal change control process that includes a security impact assessment?		1
20	Does the SP prevent unauthorized changes to the system?		1
21	Does the SP scan for configuration settings on systems in the environment?		1
22	Does the SP have an Incident Response Plan?		1
23	Does the SP have a Configuration Management Plan?		1
24	Does the SP have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34?		1
25	Does the SP conduct code analysis for internally developed code?		1
26	***IaaS Only*** Does the SP restrict physical system access to only authorized personnel?		1
27	***IaaS Only*** Does the SP monitor and log physical access to the information system, and maintain access records?		1
28	***IaaS Only*** Does the SP monitor and respond to physical intrusion alarms and surveillance equipment?		1
29	***IaaS Only*** Does the system have or use alternate telecommunications providers?		1
30	***IaaS Only*** Does the system have backup power generation or other redundancy?		1
31	***IaaS Only*** Does the SP have service level agreements (SLAs) in place with all telecommunications providers?		1

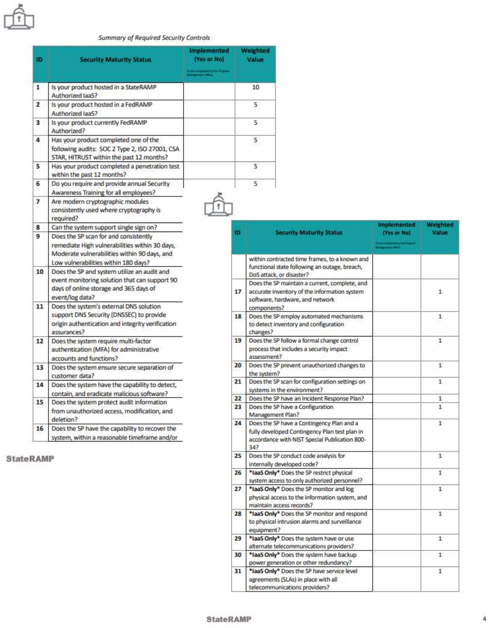
StateRAMP

StateRAMP 4

Monthly Consultative Progress Calls



StateRAMP Progressing Security Snapshot Program



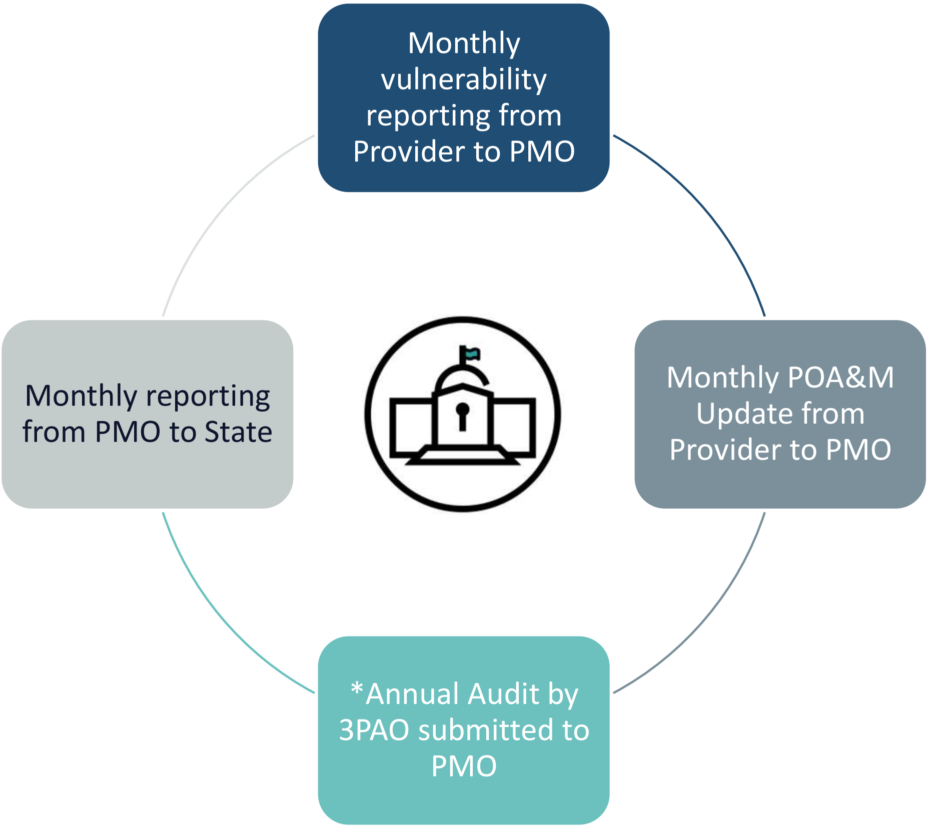
Summary of Required Security Controls

ID	Security Maturity Status	Implemented (Yes or No) To be completed by the Program Management Office	Weighted Value
1	Is your product hosted in a StateRAMP Authorized IaaS?		10
2	Is your product hosted in a FedRAMP Authorized IaaS?		5
3	Is your product currently FedRAMP Authorized?		5
4	Has your product completed one of the following audits: SOC 2 Type 2, ISO 27001, CSA STAR, HITRUST within the past 12 months?		5
5	Has your product completed a penetration test within the past 12 months?		5
6	Do you require and provide annual Security Awareness Training for all employees?		5
7	Are modern cryptographic modules consistently used where cryptography is required?		
8	Can the system support single sign on?		
9	Does the SP scan for and consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days?		
10	Does the SP and system utilize an audit and event monitoring solution that can support 90 days of online storage and 365 days of event/log data?		
11	Does the system's external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances?		
12	Does the system require multi-factor authentication (MFA) for administrative accounts and functions?		
13	Does the system ensure secure separation of customer data?		
14	Does the system have the capability to detect, contain, and eradicate malicious software?		
15	Does the system protect audit information from unauthorized access, modification, and deletion?		
16	Does the SP have the capability to recover the system, within a reasonable timeframe and/or within contracted time frames, to a known and functional state following an outage, breach, DoS attack, or disaster?		
17	Does the SP maintain a current, complete, and accurate inventory of the information system software, hardware, and network components?		1
18	Does the SP employ automated mechanisms to detect inventory and configuration changes?		1
19	Does the SP follow a formal change control process that includes a security impact assessment?		1
20	Does the SP prevent unauthorized changes to the system?		1
21	Does the SP scan for configuration settings on systems in the environment?		1
22	Does the SP have an Incident Response Plan?		1
23	Does the SP have a Configuration Management Plan?		1
24	Does the SP have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34?		1
25	Does the SP conduct code analysis for internally developed code?		1
26	***IaaS Only*** Does the SP restrict physical system access to only authorized personnel?		1
27	***IaaS Only*** Does the SP monitor and log physical access to the information system, and maintain access records?		1
28	***IaaS Only*** Does the SP monitor and respond to physical intrusion alarms and surveillance equipment?		1
29	***IaaS Only*** Does the system have or use alternate telecommunications providers?		1
30	***IaaS Only*** Does the system have backup power generation or other redundancy?		1
31	***IaaS Only*** Does the SP have service level agreements (SLAs) in place with all telecommunications providers?		1

StateRAMP

StateRAMP 4

- Gap assessment & score
- Independent verification & validation by StateRAMP PMO
- Criteria based off NIST 800-53
- Initial Snapshot delivered within 3 weeks (complete request)
- Quarterly Snapshot Updates
- Monthly consultative calls with PMO Security Team
- Providers may provision access for government clients to view Snapshots and Progressing Notes
- Monthly subscription (<u>$250 - $1000 based on revenue</u>)


Monthly vulnerability reporting from Provider to PMO
Monthly POA&M Update from Provider to PMO
*Annual Audit by 3PAO submitted to PMO
Monthly reporting from PMO to State

Continuous Monitoring

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

Providers may grant viewing access to Participating Governments

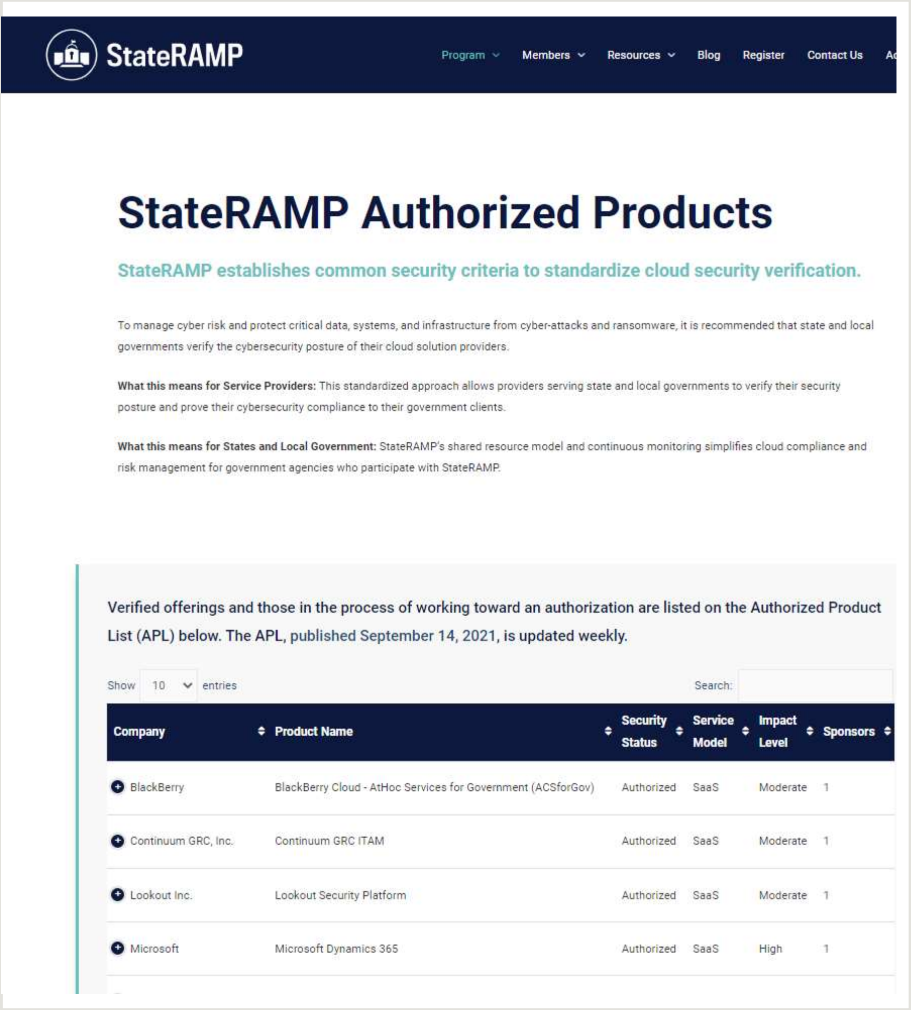
View Continuous Monitoring Policies & Escalation Process for more: www.stateramp.org/templates-resources.

Authorized Product List

Public list on www.stateramp.org for those products Progressing and Verified.

Participating StateRAMP Governments provided secure access to portal to view continuous monitoring and progressing Snapshot reporting, provisioned by providers.

View StateRAMP Security policies and templates at www.stateramp.org/templates-resources



StateRAMP Authorized Products

StateRAMP establishes common security criteria to standardize cloud security verification.

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 their security posture and prove their cybersecurity compliance to their government clients.

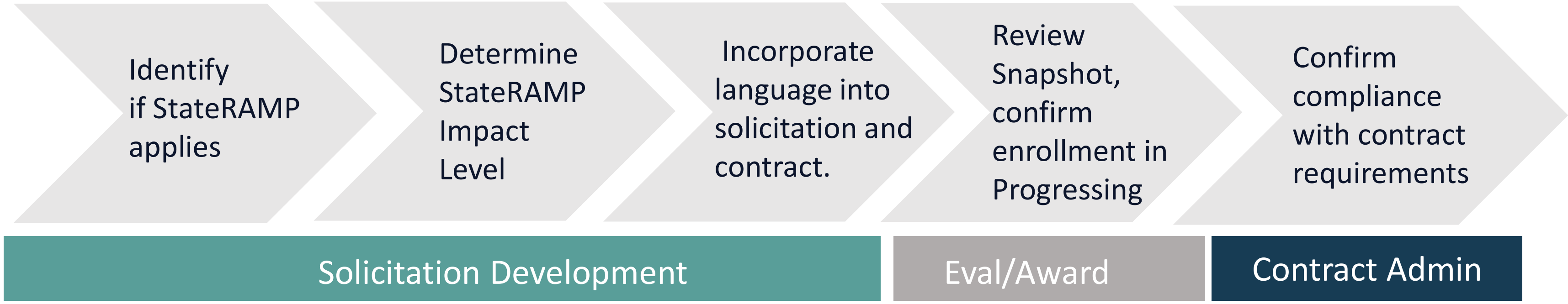
What this means for States and Local Government: StateRAMP's shared resource model and continuous monitoring simplifies cloud compliance and risk management for government agencies who participate with StateRAMP.

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

Company	Product Name	Security Status	Service Model	Impact Level	Sponsors
BlackBerry	BlackBerry Cloud - AtHoc Services for Government (ACSforGov)	Authorized	SaaS	Moderate	1
Continuum GRC, Inc.	Continuum GRC ITAM	Authorized	SaaS	Moderate	1
Lookout Inc.	Lookout Security Platform	Authorized	SaaS	Moderate	1
Microsoft	Microsoft Dynamics 365	Authorized	SaaS	High	1

StateRAMP & Procurement

Incorporating requirements into solicitations and contracts



Identify if StateRAMP applies

Determine StateRAMP Impact Level

Incorporate language into solicitation and contract.

Review Snapshot, confirm enrollment in Progressing

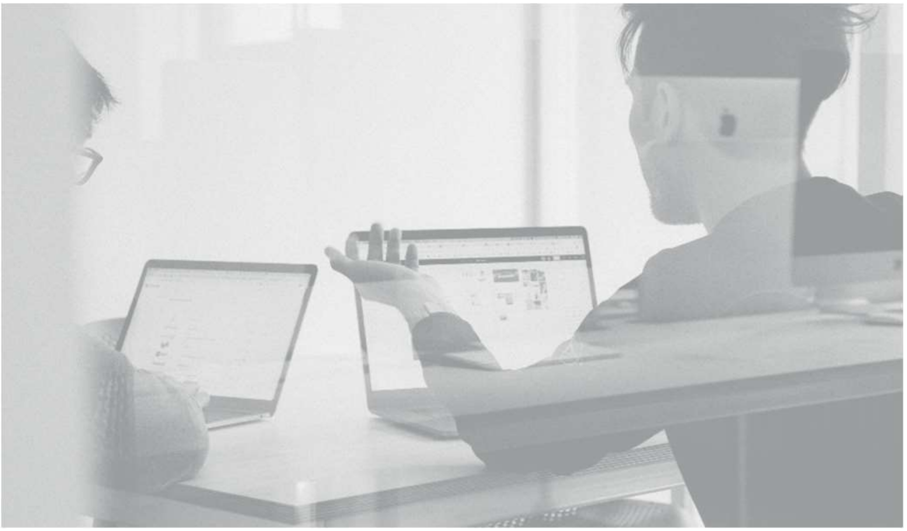
Confirm compliance with contract requirements

Solicitation Development

Eval/Award

Contract Admin

StateRAMP Implementation 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

Join the Mission

Become a Member at www.stateramp.org/register

Governments: Connect with our Government Engagement Team at get@stateramp.org

Providers: Connect with a Membership Engagement Specialist at met@stateramp.org

Membership Benefits

- Have a Voice
- Nominate for Committee
- Provider Leadership Council
- Access StateRAMP Program
- Education & Resources
- Improve Nation's Security!

Helpful Links

www.stateramp.org

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

Request a Snapshot or Security Review: www.stateramp.org/providers

View Participating Governments: www.stateramp.org/governments

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

Governance & Documents: www.stateramp.org/documents

Future Events: www.stateramp.org/events

Blogs: www.stateramp.org/blog

Info@stateramp.org

www.stateramp.org