STATERAMP OVERVIEW

StateRAMP

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*

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?

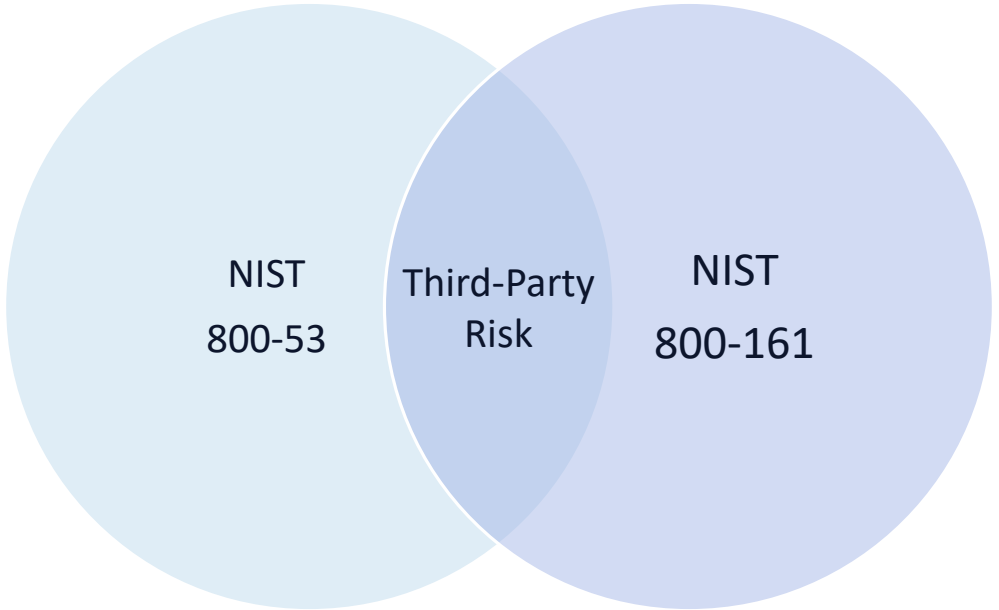
Security Requirements

Security in Supply Chains

NIST Framework SP 800-53 and SP 800-161 both contain specific controls to assist organizations identify, assess and manage supply chain risk.

- SP 800-53 contains security and privacy controls to assist with the protection of organizational operations and assets
- SP 800-53 is the foundational framework for SP 800-161
- SP 800-161 provides guidance to organizations on identifying, assessing and mitigating risks throughout the supply chain

When coupled together, state and local governments can greatly reduce risk and improve their supply chain resiliency.



Security Framework

Governance committees adopt policies that define:

- Baseline minimums standards
- Process for StateRAMP verification

StateRAMP baseline requirements built on NIST 800-53 Rev. 4

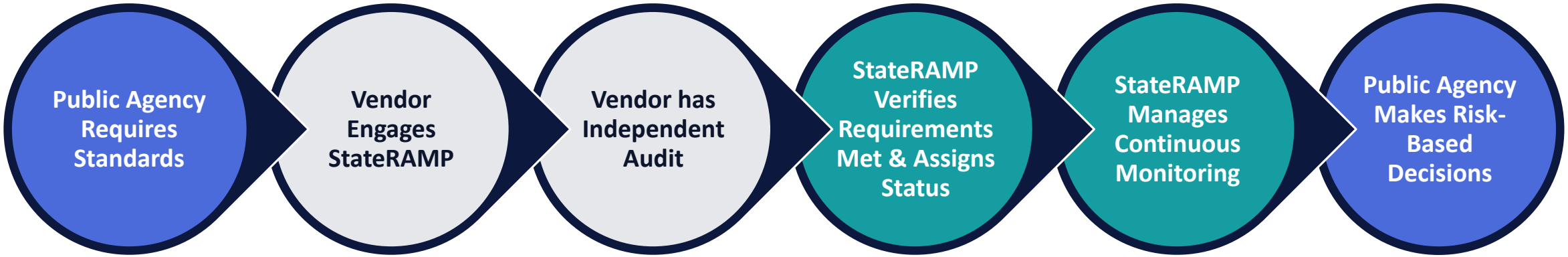
- Transition to Rev. 5 in 2023
- Goal to map to other regulatory frameworks
  - CJIS, MARSE/MMIS/HIPAA and more

StateRAMP process and policies built on NIST 800-161

Find policies, templates and resources online

- www.stateramp.org/templates-resources

StateRAMP: Trust but Verify



Verify Cloud Products Used by Public Agencies Meet Minimum Security Requirements Ongoing

- Standardized Requirements (Based on NIST 800-53)
- Independent Annual Audits
- Centralized Program Management Office (PMO)
- Continuous Reporting & Validation (Monthly & Annual)
- Shared Service for Government
- Verify Once to Serve Many for Vendors

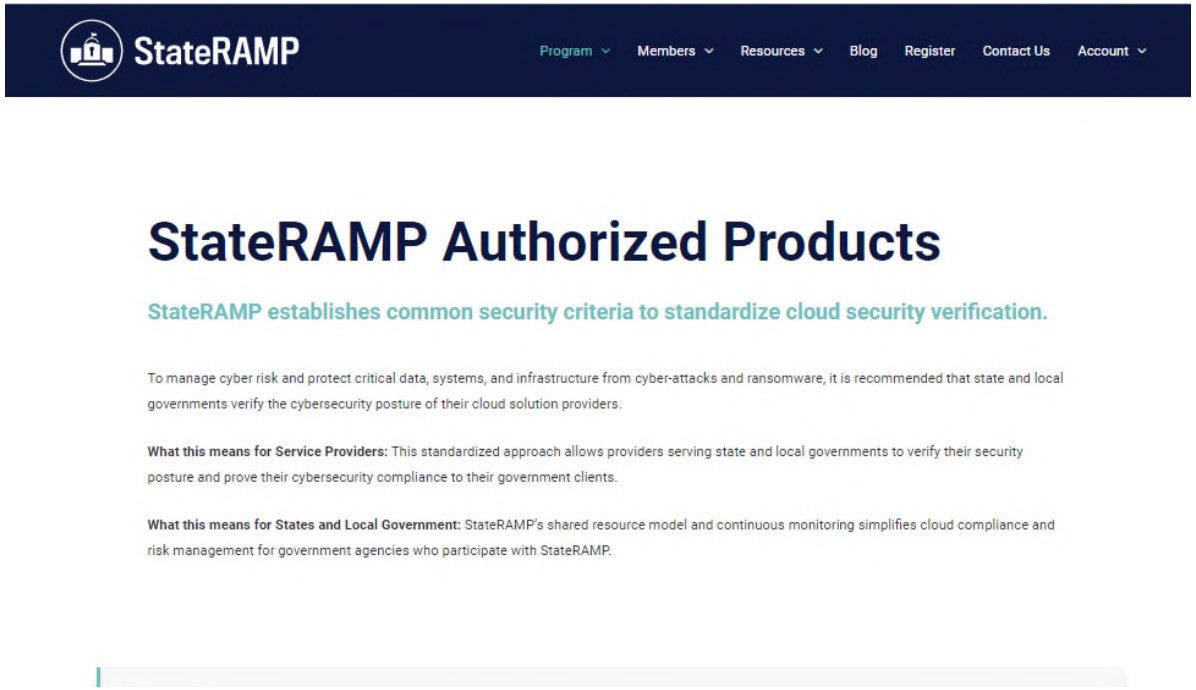
Authorized Product List (APL)

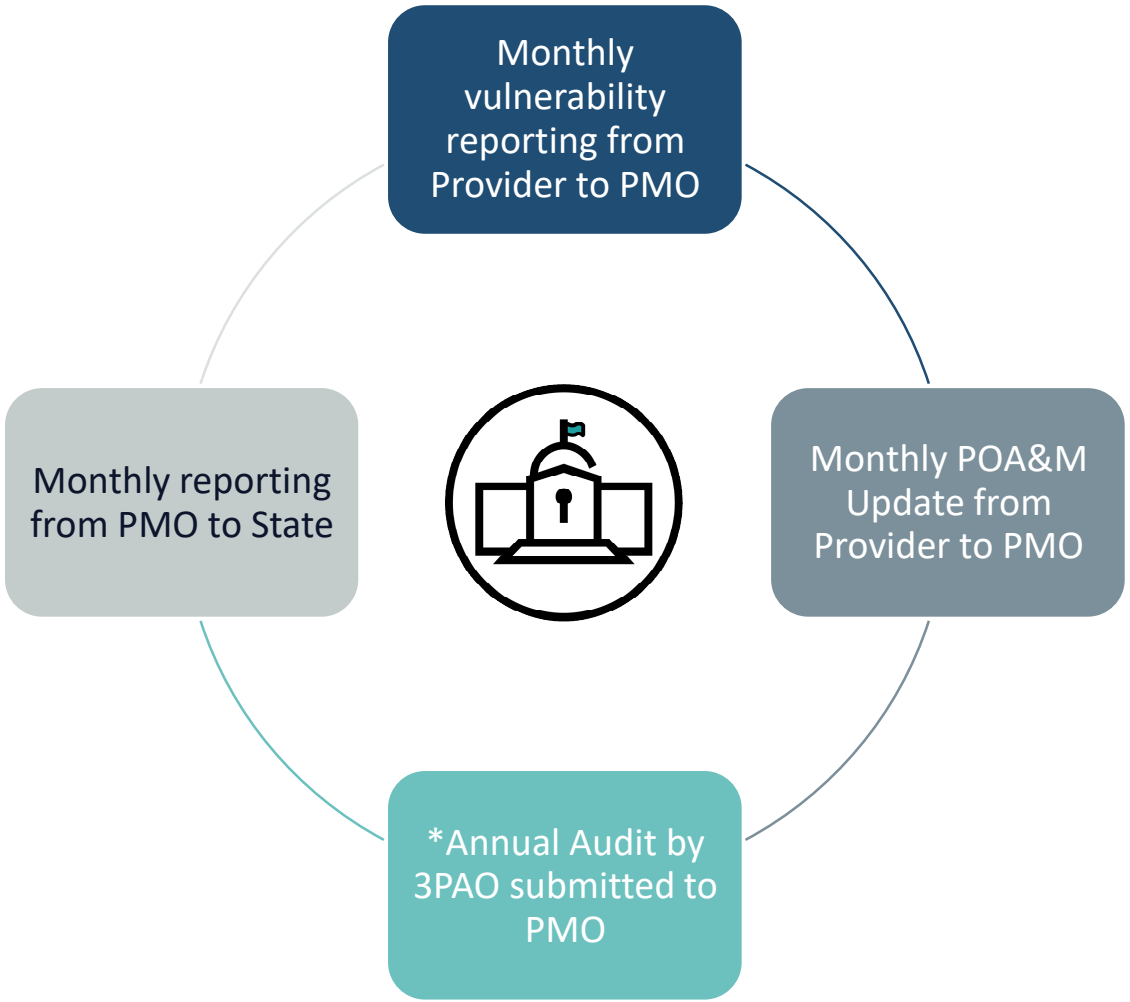
Public list on www.stateramp.org

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





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.

NIST Security Maturity Score

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 Awarded Vendor maintain monthly StateRAMP Security Progress Updates, including updating the StateRAMP Security Snapshot Quarterly (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

StateRAMP & Other Frameworks

StateRAMP and FedRAMP

https://stateramp.org/blog/

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

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.”

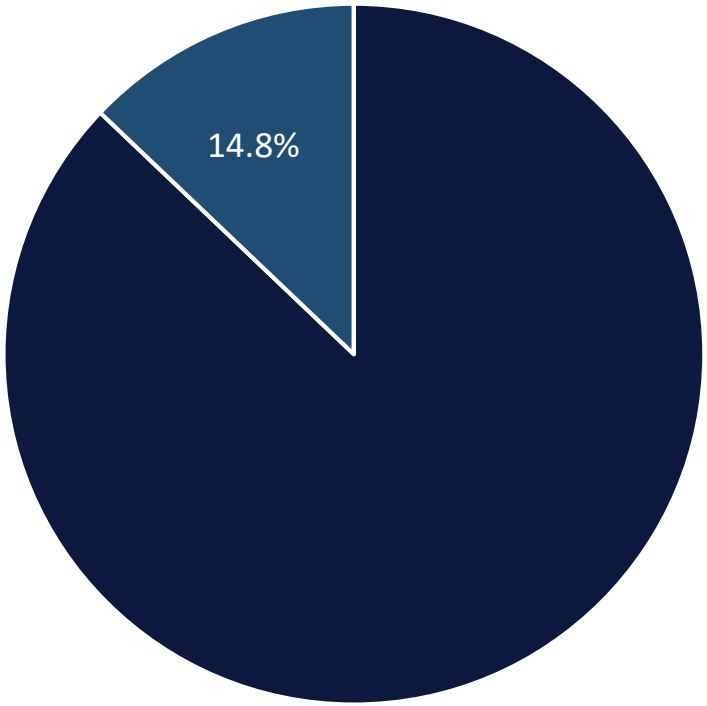
STATERAMP

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.

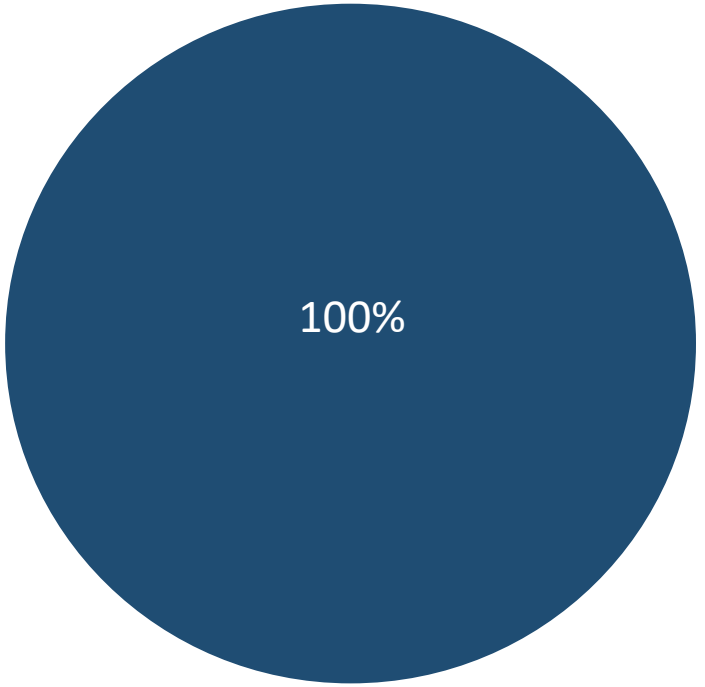
StateRAMP v. SOC 2 Audits for NIST 800-53

SOC 2 NIST 800-53 Compliance



*Assumes audited CSP selects all 42 NIST Controls for audit

StateRAMP NIST 800-53 Compliance



*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.

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

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

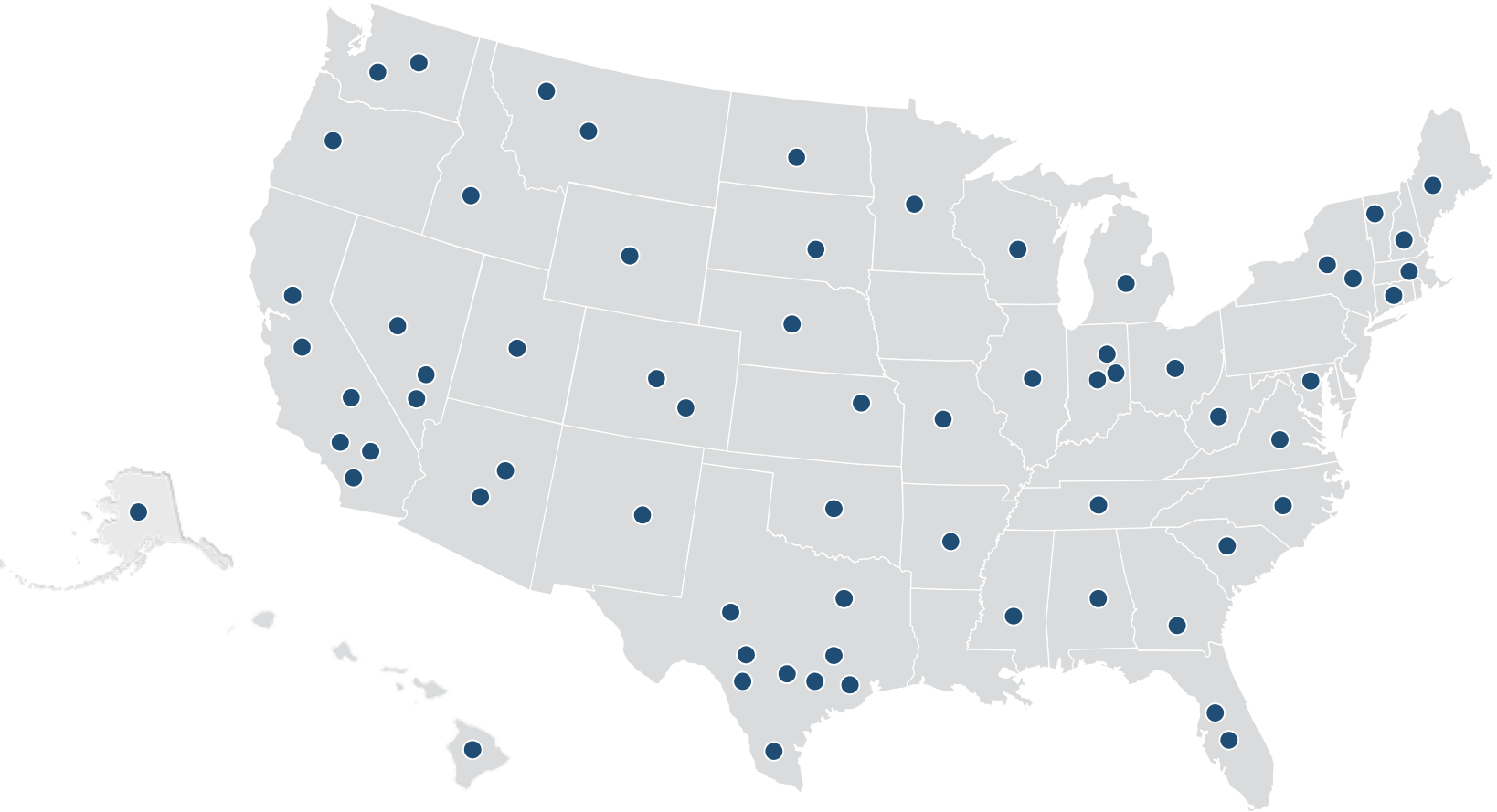
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Image: Hive Systems

Who is Involved

StateRAMP Members



356 Individual Govt. Members
141 Provider Members

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

*As of Nov. 1, 2022

Strategic Partners

NASPO
National Association of State Procurement Officials

NASCIO
Representing Chief Information Officers of the States

K12 SIX

NACo NATIONAL ASSOCIATION of COUNTIES

CENTER FOR DIGITAL GOVERNMENT

CIS Center for Internet Security®

Next Steps

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

REBECCA KEE, NIGP-CPP, CPPO, CPPB

SR DIRECTOR, GOVERNMENT ENGAGEMENT

REBECCA@STATERAMP.ORG