Secure, Compliant, and Continuous Identity Governance for State and Local Government

From digital transformation to identity risk: How RSA helps state and local government stay secure

State, local government agencies, and public education institutions operate in an environment of growing complexity, managing access for employees, contractors, seasonal workers, and partner organizations across an expanding mix of on-premises, cloud, and hybrid systems.

As these public agencies expand digital services and connect more systems to deliver benefits, process permits, and support public safety operations, manual identity governance can no longer keep pace. Access accumulates. Reviews are rubber-stamped. Orphaned accounts persist. Without continuous governance, agencies cannot demonstrate that access policies are being enforced consistently across every connected system.

RSA® Governance & Lifecycle helps state and local agencies move beyond periodic compliance activities to a continuous, defensible identity governance posture. With AI-driven risk insights, automated lifecycle management, and real-time policy enforcement, agencies can reduce identity risk, protect sensitive citizen data, and meet regulatory obligations before they become audit findings.

Excessive access and insider risk

State and local agencies rely on a complex mix of civil servants, contractors, seasonal staff, and inter-agency partners, each requiring access across multiple systems and departments. Managing this manually leads to permission sprawl, excessive entitlements, and orphaned accounts that persist long after they should. When access issues go undetected for months, agencies incur higher costs at best, and might suffer from regulatory exposure, audit findings, and risks to sensitive resident data at worst.

How RSA helps:

- Enforces least-privilege access and role-based access controls (RBAC) to limit exposure across all user types, including contractors and temporary workers
- Automates onboarding, offboarding, and access changes to ensure users have the right access at the right time and nothing more
- Applies AI-driven analytics to continuously evaluate access and surface anomalies before they become incidents
- Provides continuous visibility into identities, roles, and entitlements across on-premises and cloud environments, including non-human identities

Built for government

Trusted by the agencies with the most to lose

RSA by the numbers

- Trusted by more than 90% of US federal agencies and departments
- Deployed by 67 governments globally

Key regulations addressed

- CJIS Security Policy
- HIPAA
- IRS 1075
- NIST CSF

Deployment models

On-premises

Air-gapped / classified environments

Private cloud

Hybrid (cloud and on-premises)

What RSA Governance & Lifecycle governs

- Human identities
- Non-human identities
- Privileged and high-risk entitlements

Regulatory compliance and audit readiness

State and local agencies face strict compliance requirements under frameworks such as CJIS, HIPAA, IRS 1075, and more, each of which imposes specific controls on who can access sensitive systems and data and requires agencies to demonstrate compliance. Manual compliance processes are costly, error-prone, and difficult to scale as regulatory requirements continue to evolve. For agencies managing criminal justice information, the stakes are especially high: CJIS requires meticulous access controls, audit logging, and ongoing governance across every individual and system that touches that data.

How RSA helps:

- Automates access reviews, certifications, and segregation of duties (SoD) controls to reduce compliance gaps and reviewer fatigue
- Provides continuous, tamper-evident audit trails that demonstrate policy enforcement to auditors and oversight bodies
- Generates customizable reports aligned to CJIS, HIPAA, IRS 1075, NIST 800-53, as well as other regulations and internal policy requirements

Privileged access sprawl and toxic combinations

Over time, public sector users accumulate entitlements that create risk: permissions that allow a single individual to both initiate and approve a transaction, or to access sensitive law enforcement or financial data without a legitimate business need. These toxic combinations frequently go undetected until they surface as an audit finding or a loss event. Standard review campaigns, relying on managers certifying access they lack context to evaluate, are not reliable enough to catch them.

How RSA helps:

- Uses AI-driven insights to identify high-risk entitlement combinations and anomalous access patterns that periodic reviews miss
- Detects and enforces SoD controls across a broad range of on-premises and SaaS applications, so violations can be remediated before they become audit findings
- Provides contextual AI guidance during access reviews, helping reviewers focus on what matters most and reducing reliance on rubber-stamp approvals

Built for the organizations that serve the public

For more than 40 years, RSA has helped government agencies protect critical systems, safeguard sensitive data, and support mission-critical operations.

RSA Governance & Lifecycle delivers AI-powered insights, automated lifecycle management, and continuous compliance controls that help state and local agencies reduce identity risk, meet regulatory obligations, and strengthen operational resilience.

To learn more about how RSA secures identity for government agencies worldwide, visit **https://www.rsa.com/solutions/government**.

About RSA

RSA is the identity standard for government agencies, finance, and high-assurance organizations. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, maintain operations, and surpass compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For additional information, visit our website to **contact sales**, **find a partner**, or **learn more** about RSA.

RSA