RSA

SOLUTION OVERVIEW

Secure, Compliant, and Resilient Identity Security for Government

Tested by government. Trusted by government.

Executive Order 14028 and CISA's Zero Trust Architecture strategy set clear mandates for federal agencies: implement phishing-resistant authentication, enforce Zero Trust principles, and govern identity across complex, multi-environment workforces. The milestones are specific, and the consequences of identity failure are mission-critical. RSA helps federal agencies close the gap between mandate and execution with strong authentication, identity governance, and AI-driven risk insights that work across on-premises, cloud, hybrid, and air-gapped environments.

Prevent account takeovers and ransomware attacks

Federal agencies face persistent, sophisticated attacks targeting user credentials and authentication systems. Adversaries exploit password-based authentication, social engineer IT help desks to bypass MFA, and use compromised accounts to move laterally across agency networks. CISA's Zero Trust mandate specifically requires phishing-resistant MFA—yet a significant majority of organizations have not yet reached optimal Zero Trust maturity, leaving critical gaps in the identity layer.

How RSA helps:

- Phishing-resistant passwordless authentication—hardware tokens, FIDO2, PIV/CAC, biometrics—stops credential-based attacks
- Adaptive access policies block suspicious login attempts and enforce risk-based session controls
- Bi-directional identity verification defends IT help desk personnel against social engineering and MFA bypass
- AI-driven identity risk analytics detect anomalous behavior and enable automated threat response before damage occurs
- Identifies dormant and orphaned accounts across all environments, eliminating a common attack vector in federal network compromises

Ensure compliance with government mandates

Federal agencies must meet a growing set of identity and authentication mandates—including EO 14028, CISA Zero Trust Architecture, FISMA, and NIST SP 800-63B. These frameworks require phishing-resistant MFA, role-based access controls, privileged account governance, continuous monitoring, and documented access certifications. Agencies that fall short face audit findings, authority to operate (ATO) delays, and increased breach exposure.

How RSA helps:

- FIPS 140-2 and 140-3 validated authentication meets federal cryptographic requirements for all environments
- FedRAMP-authorized deployment available for government cloud environments
- PIV/CAC and smart card integration natively supported for federal employee and contractor access
- Automated audit trails and access certifications support FISMA reporting and inspector-general reviews
- Supports CJIS Security Policy requirements for identity proofing, MFA, and account lifecycle management for agencies handling criminal justice information

Built for government

Four decades securing America's most critical missions.

RSA in government

- Trusted by 90%+ of US federal agencies and departments
- Deployed by 67 governments globally
- 40+ years of government identity security
- Proven in air-gapped and classified environments

Key mandates addressed

- EO 14028 + CISA Zero Trust Architecture
- FISMA / NIST SP 800-53
- NIST SP 800-63B (AAL2 / AAL3)
- FedRAMP
- CJIS Security Policy
- CMMC 2.0

Deployment models

- On-premises
- Air-gapped / classified environments
- Private cloud
- Hybrid (cloud and on-premises)

Certifications

- FIPS 140-2
- FIPS 140-3
- FedRAMP
- FIDO2
- PIV/CAC
- ISO9001:2015
- CMMC 2.0

Streamline identity governance and lifecycle management

Federal agencies manage large, complex workforces that include civil servants, contractors, partner organizations, and temporary staff—often across dozens of systems and multiple security domains. Manual identity processes lead to provisioning delays, orphaned accounts, excessive permissions, and insider risk. FISMA and NIST 800-53 require documented access governance controls that scale with the agency.

How RSA helps:

- Automates onboarding, role changes, and offboarding to ensure users have the right access at the right time
- Enforces role-based access controls (RBAC) and least-privilege policies across on-prem, private cloud, and hybrid environments
- Uses AI to continuously analyze entitlements across on-premises, cloud, and hybrid environments, surfacing excessive permissions and access drift before they become audit findings
- Automates access request, approval, and certification workflows to support FISMA reporting
- Delivers a unified view of access, authentication, and governance activity across the identity landscape, giving agencies the visibility to act before risks becomes incidents

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.