RSA

WHITE PAPER

STRONG AUTHENTICATION FOR CJIS COMPLIANCE

RSA PUBLIC SECTOR SOLUTIONS

Criminal Justice Information Services (CJIS) is the FBI's largest division. CJIS maintains a central, national criminal justice database that stores highly sensitive motor vehicle, criminal history, gun tracking, fingerprint records, and more. The CJIS system equips law enforcement, national security, and intelligence community partners with the information they need to protect the US and its citizens. CJIS policy requires advanced authentication for all users that access the CJIS system from unsecure locations.

WHO IS AFFECTED?

Any organization that:

- Access the CJIS information system including federal, state, and local government agencies and approved private contractors

WHAT'S YOUR RISK?

- Are you under a mandate to adhere with CJIS compliance standards?
- Do you have officers who access CJIS system from a mobile data terminal or handheld device?
- How are you protecting remote user access to CJIS from laptops and mobile devices?
- Does your organization leverage strong authentication, multi-factor authentication (MFA) for remote user access?
- Are you able to audit, govern and ensure least-privileged access to your users?

MEETING CJIS ACCESS REQUIREMENTS

- The FBI's Criminal Justice Information Service (CJIS) Security Policy Version 5.8 (2019)[1] in section 5.6.2.2.1
- Compliance with this policy ensures users maintain consistent levels of data security and encryption in order to keep the system's sensitive criminal justice intel protected

RSA SECURID® SUITE

A COMPLETE ACCESS SOLUTION FOR ON-PREMISES, CLOUD, AND MOBILE

Assures Identity
Risk-based and context-aware authentication deliver security and convenience

Provides Options
A broad range of multi-factor authentication (MFA) methods support an increasingly diverse set of users and use cases

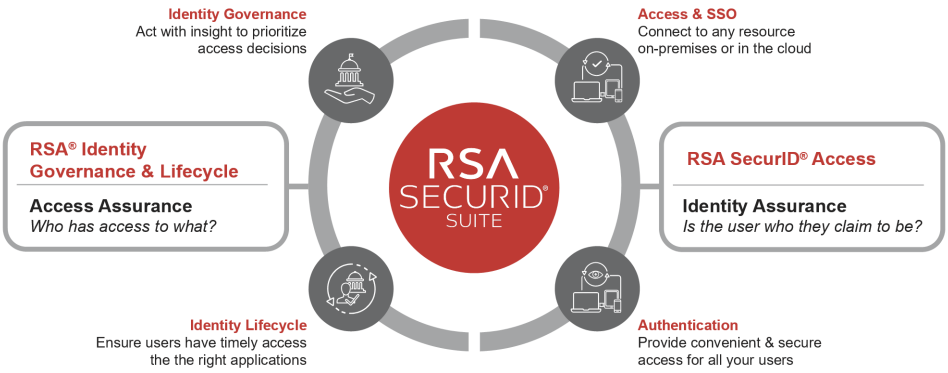
Bridges Islands of Identity
Provides consistent visibility and enforces access and authentication policies across cloud, mobile, and on-premises applications

Access Assurance
Know who has access, if the access is appropriate and compliant with policy and regulations

Least-Privileged Access Governance
Manage least-privileged access and entitlements, so users only have access to what they need

Visit rsa.com/trysecurid to Sign Up for a Free Trial

- The CJIS Security Policy also requires see section 5.5.2.1 that access entitlements must be controlled and auditable to ensure least-privileged access controls are in place
- Identity Governance and Lifecycle Management is needed to continuously monitor who has access to the CJIS and provide audit trails of changes as well as de-provision users that leave or no longer need access
- Non-compliance could result in the loss of access rights to the CJIS database, loss of employment, and possible prosecution



The RSA SecurID Suite provides access and identity assurance to public and private sector organizations to ensure they know who has access to what, whether the access is appropriate and compliant as well as having confidence that once a user attempts to access, that they are who they say they are.

The RSA SecurID Suite is a solution that supports key access security requirements for the CJIS.

RSA SECURE ACCESS SOLUTION

RSA SECURID ACCESS:

- Provides the 2FA or MFA required by CJIS
- Includes CJIS-cited "advanced authentication" methods
- Policy-driven, risk-based MFA can be enforced for multiple use cases
  —Mobile push and biometrics authentication capabilities
  —Hardware, software, and mobile-optimized authenticators; and risk-based authentication
- Ensures that credentials are secured and access is granted only to authorized users

IDENTITY AND ACCESS ASSURANCE FOR PUBLIC AND CONTRACTORS

PROVIDES
Industry leading multifactor authentication

PROTECTS

- 25,000+ organizations
- 55 million users

EXTENDS SECURITY TO ALL MAJOR USE CASES

- Cloud
- Mobile
- BYOD
- Web Portals
- Traditional VPNs
- And More...

CONTROLS ACCESS

- Based on the context or risk of the situation
- Automates access reviews and entitlement audits reducing complexity and manual effort

Learn More
rsa.com/accessthesolution

RSA IDENTITY GOVERNANCE AND LIFECYCLE:

- Manage least-privilege access to CJIS system
- Provision and deprovision access based on roles and policies and maintain audit trail
- Ensure appropriate segregation of duties controls are enforced

INTEROPERABILITY WITH THE BROADEST SET OF RESOURCES TO SUPPORT THE MISSION

RSA SECURID ACCESS PROVIDES:

- Market-leading multi-factor authentication with authenticators for every use case
- With tested, documented, certified, fully supported interoperability with 500+ technology partners and standards-based interoperability with thousands more
  —Includes interoperability for NetMotion, one of the most common integrations for CJIS
- For the full list of integrations visit rsa.com/en-us/partner/rsa-ready-program

ABOUT RSA SECURID SUITE

RSA SecurID® Suite provides the modern workforce with convenient, frictionless access to resources across digital environments, while preventing unauthorized access. The suite is part of the RSA portfolio of business-driven security solutions, which provides a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.

1. https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center