STRONG AUTHENTICATION FOR CJIS COMPLIANCE

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 THIS AFFECTS

Any organization that:

- Accesses the CJIS information system including federal, state, and local government agencies

DETERMINE YOUR RISK

- Are you under a mandate to adhere with CJIS compliance standards?
- Do you have officers who access CJIS system criminal justice information 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, two-factor authentication (2FA), or multi-factor authentication (MFA) for remote user access?

USE CASE/ DRIVERS

- FBI Security Policy section 5.6.2.2.1 mandates the use of strong authentication for remote access to the CJIS system
- 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
- Non-compliance could result in the loss of access rights to the CJIS database, loss of employment, and possible prosecution

RSA SecurID® Access

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

Enables the Business
Seamlessly connects users to all of the resources they need most — anytime, from anywhere, with any device

Preserves Existing Investments
Benefit from a cloud and mobile access product that integrates with your existing on-premises security solutions including RSA Authentication Manager and web access management solutions

VISIT RSA.COM/TRYSECURID TO SIGN UP FOR A FREE TRIAL

RSA

BE SECURE IN THE KNOWLEDGE THAT RSA SecurID ACCESS:

PROVIDES
World-leading two-factor authentication

PROTECTS

- 25,000+ organizations
- 55 million users

EXTENDS SECURITY

- Cloud
- Mobile
- BYOD
- Web Portals
- Traditional VPNs

CONTROLS ACCESS
Based on the context or risk of the situation

DELIVERS
Convenient and secure access for any user, from anywhere, to anything

LEARN MORE
RSA.COM/ACCESStheSOLUTION

THE RSA SOLUTION

RSA SecurID Access:

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

TECHNOLOGY/ INTEGRATION DETAILS

RSA SecurID Access provides:

- Market-leading 2FA and MFA with authenticators for every use case
- More than 500 out-of-the-box integrations for a seamless integration process and end-user experience
  - Includes integration for NetMotion, one of the most common integrations for CJIS
- For the full list of integrations visit rsa.com/integrations

SECURE ACCESS CAN'T WAIT.
VISIT RSA.COM/CONTACTUS
GET THE CONVERSATION STARTED.