



Entrust Solutions for Law Enforcement

CJIS Security Policy Compliance

For the law enforcement community, intelligence is a critical component of fighting crime. Whether patrolling in the community, protecting a border or access to an event, combating smuggling and piracy, or stopping child-trafficking, being able to verify identities, and quickly and securely access and share intelligence, is critical to success.

To help protect this collaboration, a strict set of security controls must be adhered to by organizations that access or exchange information with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division.

Applicable to criminal and non-criminal agencies alike, the policy provides a “minimum set of security requirements” for access to the CJIS database maintained by the FBI. These requirements help ensure the security of sensitive information and provide guidance in the protection of critical Criminal Justice Information (CJI) — “from creation through dissemination; whether at rest or in transit.”

Authentication: Advanced

The latest CJIS Security Policy requires advanced authentication for access to the CJIS database from non-secure locations.

Under these guidelines, police cruisers are considered insecure and the use of advanced authentication is required to verify identities prior to accessing the CJIS database.

The Entrust IdentityGuard software authentication platform supports every authentication method defined in the CJIS policy and allows organizations to meet this requirement while minimizing the impact on officers, agents, court officials and more.

Extending the Investment

Entrust solutions enable organizations to extend investments in network security and authentication solutions — and all beyond compliance with the CJIS Security Policy. Entrust helps law enforcement to work efficiently and securely, while ensuring information privacy.

Solution Benefits

- Meet advanced authentication and encryption guidelines set forth by the FBI’s CJIS Security Policy
- Helps agencies consolidate and manage digital identities for physical, logical and mobile access
- May be deployed at a fraction of the cost of traditional authentication solutions (e.g., hardware tokens)
- Evolves with future requirements such as PKI authentication and biometric data (e.g., retina scan, facial recognition, fingerprints)

What is Criminal Justice Information?

CJI is sensitive information or data that is critical to the core missions of federal, state or local law enforcement agencies.

- Biometric Data
- Identity History Information
- Biographic Data
- Property Data
- Case/Incident History

For detailed definitions, see the CJIS Security Policy at www.entrust.com/cjis.

MEETING CJIS SECURITY POLICY REQUIREMENTS

Entrust's proven identity framework helps law enforcement agencies and departments meet the most critical CJIS security requirements.

Area #	CJIS Policy Area	Available Solution
1	Information Exchange Agreements	
2	Security Awareness Training	
3	Incident Response	
4	Auditing & Accountability	
5	Access Control	✓
6	Identification & Authentication	✓
7	Configuration Management	
8	Media Protection	
9	Physical Protection	✓
10	Systems and Communications Protection & Information Integrity	✓
11	Formal Audits	
12	Personnel Security	

"The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a **minimum set of security requirements for the access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division** systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit."

— **Criminal Justice Information Service (CJIS) Security Policy, Version 5.1**



ENTRUST SOLUTIONS FOR CJIS COMPLIANCE

Entrust IdentityGuard

A software authentication platform for physical, logical, cloud and mobile access. Core to an identity-based security approach, this solution offers the widest range of authenticators on the market today, and helps law enforcement organizations verify the online identities of agents, officers and employees accessing agency information.

Entrust Managed Services PKI

A hosted PKI service for certificate issuance, strong authentication, physical and logical access, and a wide range of useful applications, including secure email and digital document-signing.

SSL Digital Certificates

Entrust Certificate Services provide law enforcement with SSL and specialty digital certificates that are proven, cost-effective and supported by standards-based technology.



Entrust Entelligence Messaging Server

The Entrust Entelligence Messaging Server provides the ability to send information securely via email between individuals, regardless of whether they have an existing relationship.

This greatly increases the ability of different law enforcement agencies to collaborate on specific cases without compromising the confidentiality and integrity of the information. The solution transparently manages encryption functions and enforces secure email policies, making it easy for officers to communicate while protecting data and enforcing regulatory compliance.

Entrust Entelligence Group Share

Entrust Entelligence Group Share allows law enforcement organizations to create folders where individuals working on a project — from specific criminal investigations, fighting child pornography or tracking the contents of a recovered asset locker — may share information in a secure way.

Sensitive information related to a particular project placed into a workgroup folder is automatically encrypted. Only current authorized participants in the project can unencrypt, read and add to folder contents.

A HISTORY OF SUCCESS

For more than 15 years, Entrust has provided proven identity-based security solutions to local law enforcement agencies — including LA Sheriffs, Orange County Sheriff's Department, Illinois State Police and the Kansas City (Mo.) Police Department — to meet strict authentication requirements, including complying with the U.S. Department of Justice CJIS Security Policy.



SECURITY
ON

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

Entrust's identity-based solutions secure enterprises, consumers, citizens and websites in more than 5,000 organizations spanning 85 countries. This identity-based approach offers the right balance between affordability, expertise and service. For strong authentication, fraud detection, digital certificates, SSL and PKI, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com/cjis**.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, TX 75240 USA

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

About Entrust

A trusted provider of identity-based security solutions, Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Entrust[®] Securing Digital Identities & Information