CJIS Compliance Solutions

Implementing Approved Authentication Security

For law enforcement, courts and other public safety departments that access or exchange information with the Federal Bureau of Information (FBI) Criminal Justice Information Services (CJIS) division, a strict set of security controls must be followed. The policy provides a “minimum set of security requirements” for access to 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.

September 2014 Deadline

The latest CJIS Security Policy requires advanced authentication for access to the CJIS database from non-secure locations by September 30, 2014. This includes mobile devices such as laptops, smartphones and tablets that can access CJIS data from non-secure locations.

Authentication: Advanced

Deploy an approved solution that supports every advanced authentication method defined in the CJIS Security Policy — from a single authentication platform. Choose the authenticator, or combination of authenticators, that meets the unique requirements of your officers, authorized staff and other end-users.

Secure Critical Intelligence

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.

Extend Your Investment

Extend your 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

- Comply before FBI’s September 2014 deadline
- 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
- Avoid losing access or incurring fines
- Authenticate officer identities and secure field-based access
- Extend FRAC investment for CJIS compliance
Meet Advanced Authentication Requirements

Entrust’s proven identity framework helps law enforcement agencies and departments meet a number of the CJIS security requirements. 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.”

<table>
<thead>
<tr>
<th>Area #</th>
<th>CJIS Policy Area</th>
<th>Available Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information Exchange Agreements</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Security Awareness Training</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Incident Response</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Auditing &amp; Accountability</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Access Control</td>
<td>✓</td>
</tr>
<tr>
<td>6</td>
<td>Identification &amp; Authentication</td>
<td>✓</td>
</tr>
<tr>
<td>7</td>
<td>Configuration Management</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Media Protection</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Physical Protection</td>
<td>✓</td>
</tr>
<tr>
<td>10</td>
<td>Systems and Communications Protection &amp; Information Integritvty</td>
<td>✓</td>
</tr>
<tr>
<td>11</td>
<td>Formal Audits</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Personnel Security</td>
<td></td>
</tr>
</tbody>
</table>

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).

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 IdentityGuard Cloud 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**
Entertrust 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.

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 — to meet strict authentication requirements, including complying with the U.S. Department of Justice CJIS Security Policy.

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 Records
- Case/Incident History

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.

Entrust offers software authentication platforms that strengthen security in a wide range of identity and transaction ecosystems. Government agencies, financial institutions and other enterprises rely on Entrust solutions to strengthen trust and reduce complexity for consumers, citizens and employees.

Now, as part of Datacard Group, Entrust offers an expanded portfolio of solutions across more than 150 countries. Together, Datacard Group and Entrust issue more than 10 million secure identities every day, manage billions of secure transactions annually and issue a majority of the world’s financial cards. For more information about Entrust solutions, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com.

Company Facts
Website: www.entrust.com
Employees: 399
Customers: 5,000
Offices: 10 globally

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