



**CJIS Security Policy Alignment**  
How Entrust enables and supports compliance.

**Overview**

A 2016 response since 1988 when the Central Justice Information Services (CJIS) division of the FBI first drafted its policies governing information sharing. Entrust helps law enforcement efficiently and effectively comply with these regulations so you can stay focused on today's high demand, high threat environments.

**Three important concepts**

- **Flexible identity and access management.** Identity data and authentication is central to CJIS compliance and the strong foundation you need to build a Zero Trust framework. Entrust identity solutions support an unlimited number of use cases and deployment options.
- **Role-Based Access Controls.** Assign users the fewest number of permissions necessary to perform their duties. Leverage capabilities like view history and secondary approval to further limit repetitive actions. Capture every user action for comprehensive auditing and user behavior analysis.
- **Multifactor authentication (MFA).** In terms of meeting CJIS standards for network security, the first step for law enforcement is to implement multifactor authentication. While MFA is official, some agencies have yet to deploy it.

**Key Alignment Principles**

- Role-Based Access Controls
- Identification & Authentication
- Configuration Management
- Systems & Communications Protection and Information Integrity (including machines and devices)
- Incident Response
- Auditing and Accountability
- Mobile device support

[Learn more at entrust.com](#)

# CJIS Security Policy Alignment

How Entrust enables and supports compliance.

Thank you for downloading this Entrust resource. Carahsoft is the Public Sector Distributor for Entrust's Cybersecurity solutions available via GSA, MHEC, and NJSBA.

To learn how to take the next step toward acquiring Entrust's solutions, please check out the following resources and information:



For additional resources:  
[carah.io/EntrustResources](https://carah.io/EntrustResources)



For upcoming events:  
[carah.io/EntrustEvents](https://carah.io/EntrustEvents)



For Capability Domains met by Entrust:  
[carah.io/EntrustCMMC](https://carah.io/EntrustCMMC)



For additional Cybersecurity solutions:  
[carah.io/Cybersecurity](https://carah.io/Cybersecurity)



To set up a meeting:  
[Entrust@carahsoft.com](mailto:Entrust@carahsoft.com)  
888-662-2724



To purchase, check out the contract vehicles available for procurement:  
[carah.io/EntrustContracts](https://carah.io/EntrustContracts)



ENTRUST

# CJIS Security Policy Alignment

How Entrust enables and supports compliance.

## Overview

A lot's happened since 1998 when the Criminal Justice Information Services (CJIS) division of the FBI first drafted its policies governing information sharing. Entrust helps law enforcement efficiently and effectively comply with these regulations so you can stay focused on today's high demand, high threat environments.

## Three important concepts

- **Flexible identity and access management.** Protecting **data and communications is central to CJIS compliance** and the strong foundation you need to realize a Zero Trust framework. Entrust Identity **options** support an unparalleled number of use cases and deployment options.
- **Role-Based Access Controls**  
Assign users the fewest number of permissions necessary to perform their duties, leverage capabilities like view hiding and secondary approver to further limit / monitor actions. Capture every user action for comprehensive auditing and user behavior analysis.
- **Multifactor authentication (MFA)**  
In terms of meeting CJIS standards for network security, the first step for law enforcement is to implement multi-factor authentication. While MFA is critical, some agencies have yet to deploy it.






## Key Alignment Principles

- Role-Based Access Controls
- Identification & Authentication
- Configuration Management
- Systems & Communications Protection and Information Integrity (including machines and devices)
- Incident Response
- Auditing and Accountability
- Mobile device support



# CJIS Security Policy Alignment

CJIS Policy Alignment - Entrust can be your advisor and implementation partner.

	<p><b>Policy Area 5 - Access Control Systems</b></p> <ul style="list-style-type: none"><li>• Comprehensive role-based access controls</li><li>• Auditing captures allows and denies, model user behavior, detect insider threat</li><li>• Enforce strict remote access security policy</li></ul>
	<p><b>Policy Area 6 – Identification &amp; Authentication</b></p> <ul style="list-style-type: none"><li>• Manage one identity tool for all your user types.</li><li>• Operate via secure portals, best-in-class MFA, risk-based adaptive step-up authentication, and identity proofing, on-premises or in the cloud</li></ul>
	<p><b>Policy Area 7 – Configuration Management</b></p> <ul style="list-style-type: none"><li>• Gain efficiency by reducing manual intervention, mitigate risk via automation</li><li>• Restrict / Control who can make changes to what data when</li><li>• Enterprise reports provide current security posture vs compliance mandate</li></ul>
	<p><b>Policy Area 10 – Systems &amp; Communications Protection and Information Integrity</b></p> <ul style="list-style-type: none"><li>• Datacenter and cloud encryption for data-at-rest &amp; in-transit</li><li>• Enterprise secrets and privileged access management</li><li>• Hardware Security Modules (HSMs) for increased security and FIPS level compliance</li></ul>
	<p><b>Supporting:</b></p> <ul style="list-style-type: none"><li><b>Policy Area 1 – Formal Audits</b></li><li><b>Policy Area 3 – Incident Response</b></li><li><b>Policy Area 4 – Auditing &amp; Accountability</b></li><li><b>Policy Area 13 – Mobile Devices</b></li></ul> <ul style="list-style-type: none"><li>• Comprehensive auditing for Root Cause Analysis, monitoring and reporting</li><li>• Proactively address formal audits – configuration hardening</li></ul>



# CJIS Security Policy Alignment

## BEST PRACTICES

### Integrate with existing systems

You may not fully comply with CJIS requirements yet. That doesn't mean you have to do away with current systems. In terms of convenience, Entrust identity platforms integrate with existing systems, which means that you don't have to face or pay for major overhauls. Entrust ease of deployment saves money and offers a level of flexibility that you need.

### Manage a wide range of authenticators

When it comes to CJIS compliance, we've put in place several CJIS-compliant authentication methods present. From digital certificates and biometrics to mobile smart credentials and transaction signing, and more, Entrust identity platforms assure users' identity protection so they can stay focused on their responsibilities.

### Keep an eye on costs

One example of how costs can sneak up on you is purchasing hardware tokens. It may seem like a correct step, but it's a costly measure that can be avoided thanks to cost-effective Entrust identity platforms. We'll keep your total cost exposure in mind as we work together.

### Encrypt shared information

Data is regularly shared between agencies or individuals. The Smart Credentials in Entrust identity platforms provide support for a range of communications protocols including X.509 for email and smartcard encryptions and support for smartphones and tablets. Entrust ensures that a free flow of information can take place without agencies having to be concerned about that data becoming vulnerable to malicious interception.

Considerations	
<b>Not all users are the same</b>	Sworn officers, foot patrols, and select civilians all have different needs. Tools need to support multiple user groups with different access levels
<b>Tomorrow brings new challenges</b>	The issues that departments face in terms of compliance evolve. Solutions need to be able to grow alongside the organization's needs.
<b>Mobility, machines, and devices</b>	As mobility becomes increasingly important, departments need to ensure that it's being addressed safely and securely using PKI best practices. Mobility extends to people as well as devices.
<b>Different authentication methods abound</b>	The industry standard for access to CJI data calls for multifactor authentication. Without MFA, only a vulnerable password stands between bad actors and privileged information.
<b>An extendable approach</b>	Secure identification and authorization need to extend to a myriad of individuals – quickly. Everyone should be put through the same identity-vetting process.
<b>24/7 self service</b>	Law enforcement is 24/7 work. Officers need to have secure access to information when they need it. The network infrastructure needs to be built around self-service capabilities to ensure smooth and secure always-on access to information.



# Entrust Product/Service Name

## About Entrust

Entrust keeps the world moving safely by enabling trusted experiences for identities, payments, and digital infrastructure. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.



Learn more at

[entrust.com](https://www.entrust.com)



**ENTRUST**

Entrust and the Hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.  
© 2023 Entrust Corporation. All rights reserved.

Global Headquarters  
1187 Park Place, Minneapolis, MN 55379  
U.S. Toll-Free Phone: 888 690 2424  
International Phone: +1 952 933 1223  
[info@entrust.com](mailto:info@entrust.com) [entrust.com/contact](https://www.entrust.com/contact)