THE IMPORTANCE OF CJIS COMPLIANCE FOR LAW ENFORCEMENT AND CRIMINAL JUSTICE

How to Ensure Your Organization's Data Doesn't End Up in the Wrong Hands

Entrust Datacard™

+1-888-690-2424 | entrust.com

Table of contents

Introduction

Across law enforcement and criminal justice agencies at the local, state and national levels, there are two things that are universally important: intelligence and security. Intelligence provides these agencies with a vital means of solving crimes. Security, meanwhile, is the tool that ensures this privileged data doesn't fall into the wrong hands. In order to be of value, intelligence must be secured.

In our digital world, information sharing has become easier and more widespread than ever. Law enforcement agencies at all levels benefit from more direct access to cutting-edge, cross-agency intelligence that can help bring criminals to justice. This access to shared data has brought about law enforcement data sharing-based collaborations that have proven successful in delivering expedient justice, and the movement has only gained momentum with the evolution of the Internet.

There are many benefits that come from interjurisdictional cooperation – and these advantages apply to law enforcement operations at every level. Here are two illustrative examples of those benefits in action:

- In Indiana, the weapons possession arrest of repeat offender Anthony Jerome Bandy by local Gary, Indiana officers was able to be prosecuted more fully due to the work of **Firearms Interdiction Regional Enforcement**, a federal group that included local law enforcement workers.
- In the case of Luka Magnotta – a former Canadian pornographic actor **who killed and dismembered** a victim before going on the lam – the manhunt involved a highly coordinated effort between the Montreal police, INTERPOL, French authorities and German police. Magnotta was eventually nabbed at a café in Berlin, but it was thanks to the globe-spanning policing effort that he was able to be brought to justice.

The potential risks of information sharing

With the benefits of law enforcement-based data sharing concretely outlined, it might seem like there are no clear drawbacks. But there is one important thing to consider: If a pool of shared information is available to officers, it's also potentially available to an entirely unwanted element – criminals. In Tewksbury, Massachusetts, authorities learned this lesson the hard way when the department was **targeted in a series of ransomware intrusions** which prevented access to department's files. Following an unsuccessful attempt to eliminate the attack, the department eventually forked over a $500 ransom.

It's no surprise that criminals have an interest in privileged law enforcement data. In addition to the ransom-based attacks that Tewksbury police experienced, there are other key benefits that criminals can reap by accessing a police database. These include altering criminal records, gathering personal information, embarrassing or distracting police, and gaining a competitive knowledge-based advantage over other criminal enterprises. For police departments, a criminal network intrusion can come at a much greater cost than $500: If, for instance, it's demonstrated that a hack led to case-related data being compromised, that could lead to the entire case getting thrown out.

CJIS: The basics

There's no denying the importance of securing law enforcement data, particularly when interjurisdictional collaboration enters the picture. At the federal level, there's an answer to that: the **Criminal Justice Information Services (CJIS) Security Policy**, which exists "to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit."

The CJIS policy first emerged in 1998, and has evolved to Version 5.4 as of October 6 of 2015. Throughout its evolution, the fundamental idea of the policy has been the same: It's intended to offer a set of security criteria that law enforcement and criminal justice agencies need to adhere to. Unfortunately, however, not all agencies find it easy to comply with this security framework, particularly as it pertains to cloud and mobile network security. Ensuring agency network security in a cloud-centric world — and one with evolving identity-based threats — means making sure protection advances to meet the times.

What agencies need to keep in mind when it comes to compliance

To be a CJIS-compliant agency, there are several key boxes to check. Here are some of the most important points that agencies need to keep in mind for their systems when it comes to not falling out of compliance.

1 Not all users are the same

No two network users are the same. While this tends to be true across the board, it's particularly the case for law enforcement network users, which encompasses sworn officers, foot patrol officers, and many others, including select civilians. In terms of information access, therefore, a hierarchy needs to apply. CJIS standards account for this via access control standards, which state that file access should be regulated according to privilege status. To maintain this standard, agencies need to be able to support multiple user groups with different access levels.

2 Problems today are not the same as tomorrow

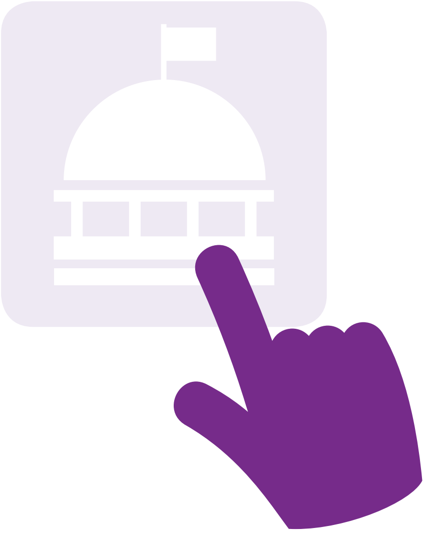
The issues that departments face in terms of compliance are always evolving. Therefore, departments need to ask themselves if their CJIS standards are built to grow alongside this evolution.

3 The mobility question

Mobile solutions are becoming a fixture of policing. But as mobile becomes increasingly important for police, departments need to ensure that it's not only being leveraged safely, but securely as well. Therefore, departmental CJIS compliance must extend to any mobile presence.

4 Presence of several different CJIS-compliant authentication methods

Agencies are taking a huge risk if they don't implement future-focused authentication methods that ensure the security that CJI requires. Examples of these methods include soft tokens, smart cards and PKI. These advanced authentication tools are examples of top-tier two-factor authentication, which is the industry standard for access to CJI data. Without 2FA, only an inherently vulnerable password stands between imposters and privileged information.



5 An extendable approach

When it comes to CJIS compliance, it's not enough for an agency to just have two-factor authentication internally — that 2FA needs to extend to non-sworn staffers as well. Agencies need to ensure that everyone accessing the network is put through the same identity-vetting process. Otherwise, a malicious presence can slip through the cracks.

6 24/7 self service

Law enforcement is 24/7 work, and officers need to securely have access to the information they require at the precise moment they need it. But while law enforcement officers operate in always-on mode, the help desk typically doesn't, which means that network infrastructure needs to be built around self-service capabilities to ensure both information access and security.

Meeting CJIS with advanced authentication

In terms of meeting CJIS standards for network security, the first step for law enforcement agencies is to implement two-factor authentication. While this is an absolutely imperative stride toward security, it's a step that some agencies haven't taken yet.

As Government Technology pointed out, law enforcement agencies are meeting the demands of implementing forward-focused tech **like body-worn cameras**. Tracking the data to come out of devices like these often leads agencies into the cloud, but when it comes to reaching a security baseline for a virtualized infrastructure — CJIS represents, after all, "a minimum" for data protection, according to networking and security expert Ted Byerly — that's a task with which agencies have more difficulty.

For agencies looking to surmount the challenges of CJIS compliance, the solution lies in advanced authentication. This is exactly what the Entrust IdentityGuard software authentication platform provides. Here are some of the key ways that **Entrust IdentityGuard** allows organizations to meet CJIS standards in a way that's straightforward and cost-efficient:

○ Integration with existing systems

Just because your agency doesn't meet CJIS yet doesn't mean you'll have to do away with your current system. In terms of convenience, Entrust IdentityGuard is first-rate in that it **integrates with existing systems**, which means that CJIS won't have to signal a major overhaul. This ease of deployment saves money and offers a level of flexibility that agencies need.

○ Low cost

As an agency, going out and purchasing hardware tokens may seem like a correct step, but in reality it's a costly measure that can be avoided thanks to Entrust IdentityGuard, whose deployment comes at just a fraction of the cost of other solutions. An investment in Entrust IdentityGuard means more money to put toward other agency-critical functions.

○ Wide range of authenticators

Another disadvantage to going out and purchasing a single authentication solution like hardware tokens is that you'll just have the one. And when it comes to CJIS, we've already established the importance of having several different CJIS-vetted authentication methods present. Entrust IdentityGuard provides users with the broadest range of authenticators out there. From digital certificates and biometrics to mobile smart credentials and transaction signing — and many more — Entrust IdentityGuard guarantees users a level of identity protection that's vital for agencies.

○ Encrypted information sharing

When data is shared between agencies or individuals, it has to be treated with sensitivity. Entrust IdentityGuard Smart Credential provides support for a range of X.509 solutions including encrypted email, smartcards and support for smartphones and tablets. This encryption ensures that a free flow of information can take place without agencies having to be concerned about that data becoming vulnerable to malicious interception.

Beyond these benefits, one of the key **advantages of an Entrust Datacard solution** – and what sets it apart from the pack – is the fact that it can do much more than just meet CJIS. When departments leverage Entrust Datacard, they go beyond just compliance, and enjoy **additional business-critical benefits** like secure communication tools, transaction signing solutions and cutting-edge **mobile security**.

Conclusion

Law enforcement today relies on both the exchange of information and the security of that data. Entrust IdentityGuard is the platform that can enable any agency to ensure that advances in information exchange don't come at the expense of CJIS compliance.

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Twitter Facebook Youtube LinkedIn Google+ RSS

Entrust Datacard™