AuthAnvil
Password Solutions

Password Security and the New CJIS Security Policy

scorpion software | A Kaseya Company

It's no secret criminals have become more sophisticated in their use of technology. Fortunately, American law enforcement agencies have been more than able to keep pace. Interconnectedness is the name of the game in modern law enforcement. Gone are the days when criminals could evade arrest and prosecution by staying on the move, skipping from one jurisdiction to the next. Law enforcement organizations—from small town police forces to federal agencies thousands of agents strong—are talking to each other. The central hub of this far-reaching network of law enforcement communication and sharing is the FBI's Criminal Justice Information Services Division (CJIS).

Based out of a massive facility in West Virginia, CJIS acts as a repository for information on crime and criminals. Officers and staff within your law enforcement agency rely on CJIS every day for access to key crime fighting data like criminal records, outstanding arrest warrants, fingerprints, stolen property reports, firearms records, just about anything they can use to connect their investigations to other ongoing or completed investigations nationwide. Thanks to CJIS, criminal justice data that is generated locally can be shared nationally, and even internationally.

Here's an example:
An officer makes a routine traffic stop for speeding. He runs the plates of the car through a CJIS database and discovers that it was reported used as an escape vehicle during an armed robbery several counties away. Now the officer not only has the opportunity to apprehend a dangerous criminal, he also knows to protect himself by calling for backup and approaching the driver with caution.

CJIS AND LAW ENFORCEMENT IT

For those working in law enforcement, CJIS data is an important tool for preventing and combating crime. If you oversee the information technology (IT) systems of a police department, county sheriff's department, or municipality, ensuring officers and agency staff have a reliable and secure pipeline to CJIS data is a critical part of your job. For better or for worse, that job just got a little more complicated.

The FBI completed a major rewrite of its CJIS Security Policy in August 2013. The CJIS Security Policy governs how law enforcement agencies may access CJIS databases and sets standards for minimum levels of security. The FBI's policy changes were motivated by a number of circumstances:

- The use of laptops and mobile devices is on the rise among police departments and other law enforcement agencies.
- 3G and 4G cellular networks have extended the ability of officers to access criminal justice information from their stations to the street. This provides greater efficiency and enhances officer security.
- The CJIS databases hold critical information, like fingerprints, criminal histories, and sex offender registration. This information could be used maliciously if accessed by the wrong people.
- Along with corporate and government IT security experts, the FBI recognizes the security risks associated with weak password-based authentication.

The new Security Policy is wide ranging. Anyone involved with the administration of a police department or other law enforcement facility should give it at least a cursory review here: http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view.

IT personnel should be particularly concerned with three sections of the policy:

Policy Area 4:
Auditing and Accountability

This section of the CJIS Security Policy requires law enforcement agencies to generate and keep records of certain events "relevant to the security of the information system" used to access CJIS data. Events to be logged include successful and unsuccessful attempts to:

- Logon
- Access, create, change, or delete permissions
- Change account passwords
- Use privileged accounts
- Access or change the audit log file

Policy Area 5:
Access Control

The Access Control section regulates who within an agency should have access to CJIS data and the extent of each user's access. Its key requirements include:

- Agencies are responsible for creating and managing user accounts for accessing CJIS data, limiting individual users and groups of users to only what they need to know and need to share, based on their role.
- Agencies must update these accounts when a user's role changes or the user is terminated.
- Systems used to access CJIS data must enforce these different levels of access, granting access to "privileged functions" only to those who are authorized.
- A system must limit unsuccessful login attempts to five.
- A system must lock users out after 30 minutes of inactivity, after which time they must re-authenticate themselves.
- Agencies must "authorize, monitor, and control" all forms of remote access to CJIS data.

Policy Area 6:
Identification and Authentication

This section is meant to ensure that those attempting to access CJIS data are who they say they are. According to this policy area:

- Strong passwords must be used on all systems used to access CJIS data. They must be at least eight characters long and not a dictionary word or proper name.
- Passwords must expire after 90 days.
- Passwords must not be transmitted outside of secure locations.
- "Advanced authentication" must be enforced for those accessing CJIS data from locations that are not physically secure and do not meet the FBI's technical guidelines for security. In the language of the Security Policy, advanced authentication is at least two-factor authentication: a password plus another factor unique to the user, like a smart card, a software token, or a fingerprint.

The FBI initially planned to put the new policies into effect as of Sept. 30, 2013. Because so few agencies were on track for compliance, however, the FBI pushed the deadline back a year to September 2014. Even that date may be ambitious; law enforcement agencies and their IT teams will be scrambling to comply throughout the next year, hoping to complete their projects before they become the target of an FBI audit.

The Risks of Noncompliance

When it comes to compliance with the new CJIS Security Policy, large city police departments and statewide law enforcement agencies have the advantage over smaller police departments and county sheriff's offices. While larger agencies will have their own dedicated IT team, smaller departments often share IT resources with other county or municipal departments. At this level, too, officers and chiefs tend to be less progressive in their understanding of technology. IT personnel often find themselves having to fight for increases in their budget and reassuring veteran officers that new systems will help them get their jobs done, not get in their way.

As you plan and budget for CJIS compliance at your department, consider sharing these points with your superiors:

- While the FBI's year-long postponement offers a temporary reprieve from compliance, the grace period will not last forever. Sooner or later, the FBI will want all agencies to comply with the new policies and deny CJIS access to those that don't.
- Even the smallest police department would be hampered without access to the valuable information stored in CJIS databases. Veteran investigators know that crime doesn't occur in a vacuum; they can't constrain their investigations to their own town or county borders.
- Even if compliance weren't an issue, the FBI's new guidelines are in line with the latest best practices for data security. Enforcing strong passwords and multi-factor authentication, for example, are just good—and highly recommended—ways to protect computer systems from unauthorized access.
- If an unauthorized user were to access your department's systems, he would be able to modify or remove arrest records, compromise ongoing investigations, and access information that could be used for fraud, blackmail, or intimidation.
- Criminal justice information in the wrong hands could jeopardize public safety and the safety of law enforcement officers and risk embarrassment for law enforcement and government officials and agencies.
- When implemented correctly, many of the solutions required for CJIS compliance will actually improve your agency's efficiency and simplify the workflow for your officers in regards to accessing information systems and the data it makes available within them.

TWO CJIS USE CASES

Clearly, complying with the new CJIS policy is in the best interest of all law enforcement agencies, as well as public safety in general. Compliance is difficult, though, because of the many different ways officers and officials access and use CJIS data—even within the same police department. For example, here are two different use cases.

Use Case #1: On the Street

Situation: A detective leaves his police station to conduct an investigation. He's equipped with a laptop with a 3G or 4G radio receiver for connecting back to the station computer system via VPN (usually using software tools like NetMotion or Cisco AnyConnect).

CJIS requirement: If the detective is traveling and accessing CJIS data from within an official police vehicle that is secured, advance authentication isn't required. For the time being, the FBI considers police vehicles to be secure locations (that is expected to expire in September 2014). However, when the detective stops at a coffee shop for a working lunch or takes the laptop with him to interview a witness, advanced authentication is required if he wants to access CJIS information.

Use Case #2: Back at HQ

Situation: The same detective returns to his police station and continues to work from the desktop computer in his office.

CJIS requirement: If all the necessary technical controls are in place, a police station is considered a secure environment and, therefore, the detective does not have to go through an advanced authentication process to access CJIS data. His login must still be logged, however, to create an auditable record.

SIMPLIFYING CJIS COMPLIANCE WITH A PASSWORD MANAGEMENT SYSTEM

Implementing different solutions for compliance with different CJIS requirements is going to result in complex, disjointed, expensive systems that annoy users and decrease efficiency. In the examples above, the detective might have to remember a different strong password to log into the VPN than he does to log into the system locally. He'll have to be sure to change both passwords every 90 days (or be forced to somehow). Further complicating the situation, both his remote and local logins will have to be recorded somewhere for auditing purposes—even if they were done using different systems.

Password security needn't be so complicated for end users or system administrators. A better solution would combine password management functions with single sign-on portals made secure by multi-factor authentication. Before discussing how these three solutions can work together, let's look at how law enforcement agencies can benefit from using each one:

Password Management

A password management system is a centralized solution where your entire department's passwords can be safely stored and managed, in sync with the sites and applications the passwords protect, including those that access CJIS data. This meets most of the requirements of Policy Area 5, Access Control. The most effective and secure password management systems grant different levels of access to passwords (and the ability to add, remove, or modify them) to different individuals based on their roles and level of authority. If an officer leaves, changes roles, or is terminated, an administrator can use a centralized password management system to quickly identify and change any passwords that officer used.

A password management system also acts as a central, auditable database for information on password use. When sites and systems are synced with a password management system, every login attempt, successful or unsuccessful, can be recorded by username, date and time, and many other identifying factors.

Because of the sensitive nature of their systems and the disastrous consequences of unauthorized access, law enforcement agencies should consider password management systems that store password information in a locally controlled server, rather than off-premise or in the cloud.

Single Sign-On

As the phrase implies, single sign-on (SSO) refers to the ability to access multiple password-protected sites and systems by logging in only once. This is usually accomplished through a web portal. In the example above, our detective could use a single sign-on portal on the go or sitting at his desk. It makes no difference.

Here is how it might work: When the detective starts up his laptop's web browser, he's greeted by an online portal where he will see links to all the different web applications, sites, and systems he uses to communicate with other officers, access criminal justice information, share information with other law enforcement agencies, and so on. While all of these sites and systems might require a different username and password, the detective only has to log in once. Clicking on one of those links will provide him instant access to get right to work on his chosen site. No password required; the password management system provides login credentials behind the scenes.

You can see where technology-averse officers might actually be interested in using a system like this. Single sign-on would allow them to:

- Reduce the amount of time they spend at login prompts.
- Access systems and services without having to remember a URL or host name.
- Access multiple applications, websites, and systems without needing to know or remember their passwords—and good single sign-on systems make new sites easy to add.

Single sign-on also makes password security simpler for system administrators. Enforcing strong passwords—like those required by CJIS—and changing them every 90 days is much easier when end users don't even have to know their passwords. Single sign-on also provides a way to generate auditable login records for systems in which multiple users share the same credentials.

Multi-Factor Authentication

Multi-factor authentication (MFA) is more than a CJIS requirement; it's the function that makes single sign-on secure. Single sign-on portals are great conveniences, but what would happen if a cybercriminal gained access to a police officer's SSO credentials? That individual would then be able to access all the same sites and systems as the officer, without having to know the strong passwords that protect them. Multi-factor authentication gets around this serious security lapse by requiring a password along with a second authentication factor.

If a website or system requires a username and password for access, that's just one factor—something the user knows. Other recognized identification factors are something the user is, something the user has, or somewhere a user is at. In practice, the knowledge factor and the possession factor are most commonly used for multi-factor authentication, but biometrics like fingerprints or iris scans are sometimes used to provide the inherence (something the user is) factor. More recently, some systems use the location of the user to reduce risk to an acceptable level, depending on the sensitivity of the information being accessed.

One-time-use codes sent to a user's smartphone are becoming a frequent second authentication factor. For law enforcement officers that don't like carrying smartphones on the job or need a more reliable, less "high-tech" form of authentication, small USB-based YubiKeys or hardware keyfobs might be preferred.

Returning one more time to our detective on the streets, if he attempts to access his SSO portal during lunch at his favorite diner, the only way he'll get in is if he plugs his YubiKey into the laptop or types in a one-time-use PIN that was generated by an app on his cell phone. If he leaves his laptop in his car, forgets to lock up, and a thief makes off with it, that thief and his associates will be out of luck without the YubiKey or smartphone, even if they can somehow crack the detective's password.

Tying Them Together: The Power of Three

Technically, CJIS compliance can be achieved without a solution that combines password management, single sign-on, and multi-factor authentication into a single system. But as anyone involved in law enforcement knows, it's often necessary to look beyond the letter of the law. The spirit of the new CJIS policy is to encourage security best practices that will protect law enforcement officers and, more importantly, the communities they serve from those who would use criminal justice information against them.

We have already shown how each system builds on the strengths of the others. Password management makes single sign-on possible and multi-factor authentication makes single sign-on secure. Working together, these three components allow law enforcement agencies to eliminate the need for passwords entirely in many situations, while simultaneously strengthening their security practices and lessening the headache of managing hundreds of different credentials across an ever-changing force. Working together, password management, single sign-on, and multi-factor authentication eliminate most of the barriers to the level of security called for by the FBI's new regulations and open the door to improved law enforcement collaboration in a connected world.

AuthAnvil for Law Enforcement

AuthAnvil is a full-featured all-in-one credential management solution that combines the power of password management, multi-factor authentication, and single sign-on. AuthAnvil is an effective tool for complying with the new CJIS Security Policy and improving the efficiency and security of law enforcement agencies of any size. To learn more about how modern law enforcement agencies use AuthAnvil, download our free guide, "Using AuthAnvil in Law Enforcement."

Free eBook!
Using AuthAnvil in
Law Enforcement
Learn more about using AuthAnvil in Law Enforcement - Click Here