imprivata®

EBOOK

Eight considerations for achieving CJIS 6.0 compliance

The U.S. Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division outlines the required security policies for any agencies, vendors, or individuals that access CJIS information and systems. While law enforcement officials require near-instant access to CJIS data, maintaining its security is imperative to prevent unauthorized access and misuse. Improper access to criminal justice information can result in penalties, including denied access to databases, fines, and criminal charges.

The FBI published its latest update, CJIS 6.0, on December 27, 2024. It raises expectations for how agencies operationalize identity and access management to protect Criminal Justice Information (CJI). While CJIS has long required strong identification, authentication, and auditing controls, CJIS 6.0 put a greater emphasis on applying those controls consistently in real-world environments — reinforcing that multifactor authentication (MFA) is not optional, strengthening expectations for auditability with detailed, tamper-proof logs of who accessed what, when, and from where, and elevating the need to manage risk for third-party/vendor access and shared devices like mobile data terminals (MDTs).

The latest policy updates are designed to strengthen security while supporting operational efficiency for law enforcement and related agencies. This guide reflects the latest requirements and lessons learned from agencies seeking CJIS compliance.

CJIS Security Policy requirements for identification, authentication, and auditing: What you need to know

Key provisions of the CJIS Security Policy are focused on identification, authentication, and auditing. CJIS 6.0 also raises expectations for how agencies manage access in practice (especially for third-party users and shared devices/MDTs) to ensure access is appropriately scoped, traceable, and separated between users on shared endpoints. Functionalities like session persistence, fast user switching with session isolation, and reliable session termination at end-of-shift helps protect CJI on shared workstations and MDTs without slowing officers down.

Authentication requirements

In line with fundamental security best practices, the CJIS Security Policy requires advanced authentication (or multifactor authentication) when an individual is accessing CJIS data. To satisfy MFA requirements, agencies must use two factors from different categories to authenticate users: something a user knows (e.g., a password), something a user has (e.g., a token), or something a user is (e.g., biometrics). Acceptable methods include factors like biometrics, smart cards, or tokens.

What are the CJIS multifactor authentication requirements?

- Multifactor authentication must be enforced for both privileged and non-privileged accounts
- Authentication mechanisms must be resistant to replay attacks
- Authenticators must reach authenticator assurance level 2 (AAL2), including minimum cryptographic strengths, FIPS 140 validation and secure binding procedures
- Biometrics if used as an authentication factor must meet strict performance, anti-spoofing and transmission security requirements

Who is multifactor authentication a requirement for?

Multifactor authentication is a requirement for the following:

- All mobile systems, including laptops (removed from squad cars) and all mobile devices, such as cell phones and PDAs, that run National Crime Information Center (NCIC) access transactions
- Any device that uses the Internet, wireless, or dial-up connections to run or process NCIC transactions

What is CJIS' auditing requirement?

The CJIS policy requires auditing to provide integrated reporting capabilities that track data access, network authentication, and application activity at the individual user level. CJIS 6.0 requires agencies to maintain detailed, tamper-proof logs of who accessed what, when, and from where. Login attempts, password changes, privilege escalations, data access attempts and other security-related events must be securely logged as part of the agency's auditability and accountability controls. Not only must these events be logged, but agencies must review them regularly (think weekly).

Identify misuse

A core goal of the CJIS Security Policy is to ensure that access to Criminal Justice Information (CJI) is appropriate and authorized. Officers need access to these systems to do their jobs safely and effectively. But access that is unrelated to a person's duties or casework is a violation. For example, accessing records on a family member without a legitimate work-related reason would constitute misuse under CJIS policy. Agencies need a way to detect misuse as it happens or soon after. They also need a clear process for reviewing suspected misuse and recording the outcome. Misuse can result in loss of access and may create legal exposure for the individual or the agency. Audit logs must be reviewed weekly, and consider controls like behavioral anomaly detection, insider threat monitoring, and documented disciplinary workflows to help identify and manage potential misuse.

AUDITABLE EVENTS

The following events shall be logged:

- Successful and failed system log-ons and any attempts (and enforce a limit of 5 unsuccessful login attempts)
- Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resource
- Successful and unsuccessful attempts to change account passwords
- Successful and unsuccessful actions by privileged accounts
- Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file
- Logs must capture event type, time, source, outcome and related identities
- Logs must be retained for a minimum of 1 year, though many jurisdictions have longer retention mandates

Least-privilege and role-based access control (RBAC)

CJIS compliance also depends on limiting access to only what each user needs. Least-privilege and role-based access control (RBAC) help agencies align permissions with job responsibilities and operational needs. That matters across all user types, from officers to civilian staff to outside vendors. When access is too broad, risk increases. Clear roles help keep permissions as narrow as possible, and make user activity easier to attribute.

Account lifecycle management

Access control does not stop once an account is created. Agencies need clear processes for granting access, updating permissions when roles change, and removing access when it is no longer needed. This is especially important for temporary users and third parties. Accounts should not remain active beyond their purpose. Permissions should also be reviewed regularly to ensure access remains aligned with current job needs.

Incident response

Audit logs are only useful if agencies are prepared to act on what they show. CJIS compliance requires a defined process for responding to suspicious activity or a possible compromise. Logs help agencies understand what happened and who was involved. They also support follow-up once an incident has been identified. In that sense, auditing is not just about compliance. It is part of how agencies respond effectively when something goes wrong.

Importance of CJIS training

Technology alone is not enough to support CJIS compliance. Users also need to understand their responsibilities and how to handle CJI appropriately. Training should explain what constitutes authorized use and when suspicious behavior must be reported. It should also reinforce secure habits in day-to-day work. Regular training helps reduce preventable mistakes and supports more consistent compliance over time.

An approaching deadline

The deadline to implement MFA has already passed: agencies must have MFA in place for all users. Many agencies may have scrambled to find a solution quickly without due diligence. They may have stopped at “check the box” MFA but didn’t fully consider how it would impact productivity and user experience.

The larger deadline is approaching rapidly. The FBI has mandated that all agencies must be fully compliant with the CJIS Security Policy by October 1, 2027. Ultimately, unique IDs, strong passwords, multifactor authentication, and audit controls are best practices that every organization should adopt. Implementing a solution built for the dynamics of public safety should not only help meet CJIS requirements but should also enable agencies to improve their cybersecurity posture and, just as importantly, streamline access, keeping first responders focused on their mission, not technology.

Seek advice from your peers

Agencies need expert advice — not from a vendor, but from actual peers who have successfully complied with CJIS at their own agencies—from those who have measured the results against the investment and can share their experiences. We asked some of our customers for advice on how other agencies can comply with CJIS.

What follows are eight considerations for ensuring success based on their experiences.

1 Factor in CJIS-approved authentication methods

The CJIS Security Policy requires that MFA requirements must be supported by authorized authentication methods. These methods include smart cards, FIDO2 security tokens, and biometrics. Selecting the best form of multifactor authentication to implement will depend heavily on the organization's specific needs. It's important to keep in mind that those needs can vary over time and across the organization, and deploying a solution with limited authentication options will likely not serve all users and use cases well.

2 Consider how multifactor authentication will affect officer workflows

When choosing a solution, agencies must consider how implementing multifactor authentication will affect user workflows. In the fast-moving, demanding environment of law enforcement, it is imperative that MFA does not disrupt officer workflows or productivity. Choose a solution that eliminates the need to enter a complex password or carry additional hardware.

3 Consider your existing infrastructure and core (legacy) applications

The last thing an IT department needs on top of meeting CJIS requirements is to further disrupt the IT environment with changes to its infrastructure. Choose a solution that integrates easily with existing IT infrastructure and legacy applications, such as your CAD and RMS systems, without disrupting workflows.

---

4 Require end-to-end compliance with the FIPS 140-3 data encryption standard

CJIS requires FIPS 140-3 compliance for biometric systems and criminal justice information stored or transmitted outside physically secured locations. Ensure that the biometrics you choose comply with the FIPS 140-3 Standard. All data in transit and at rest must be encrypted with FIPS 140-3 modules.

---

5 Consider passwordless authentication methods and self-service password reset to reduce the helpdesk load

CJIS' password requirements are lengthy and complex. While this enhances security, it creates a poor user experience. At best, these complex passwords are frustrating and inconvenient; at worst, they create a safety issue because officers get locked out and can't get the access they need. Consider passwordless authentication to improve the user experience while maintaining security. Also consider self-service password reset options to minimize reliance on IT and reduce administrative overhead.

6 Evaluate the benefits of single sign-on to all applications

With single sign-on, agencies can profile an application's sign-on behaviors and enable application profiling without scripting or modification of application code. While it's relatively easy to mandate longer, expiring passwords, personnel will have a more difficult time remembering passwords for the many applications they need to access. The result will be increased password reset requests to the helpdesk. Choose a single platform solution that supports Single Sign-On to all critical applications, including legacy systems like CAD and RMS.

---

7 Engage with peers who have successfully addressed these CJIS requirements

Agencies who have already started on their CJIS compliance journey can share valuable insights and learnings from their experience.

---

8 Rethink third-party access: Eliminate shared logins and enforce time-bound, traceable vendor access

Avoid shared vendor logins. Under CJIS 6.0, third-party access should be individually attributable, verified, and auditable. Implement temporary, least-privilege (tightly scoped), and automatically expiring access to reduce risk and simplify offboarding.

Thinking beyond the audit: CJIS as an ongoing mission

CJIS compliance will always be mandatory. Rather than simply trying to survive and pass the next audit and implement the latest requirements, **shift your perspective to view CJIS compliance as another ongoing mission for the agency.** Successful agencies tend to look beyond whether they are technically compliant today. They think about whether their controls will still make sense after staff turnover, system changes, or future CJIS updates. They look for ways to simplify enforcement rather than layering on more manual processes.

They also consider how to optimize controls to help them implement and manage them with their unique workflows in mind. The right controls increase operational efficiency, making compliance easier for users without encouraging risky workarounds.

The goal is CJIS compliance that holds up as environments grow more complex. It makes audits more predictable. It supports the mission instead of getting in the way. Meeting the requirements is the baseline. Building lasting, durable CJIS compliance is what really matters.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

3874-2026_CJIS-ebook-8-considerations