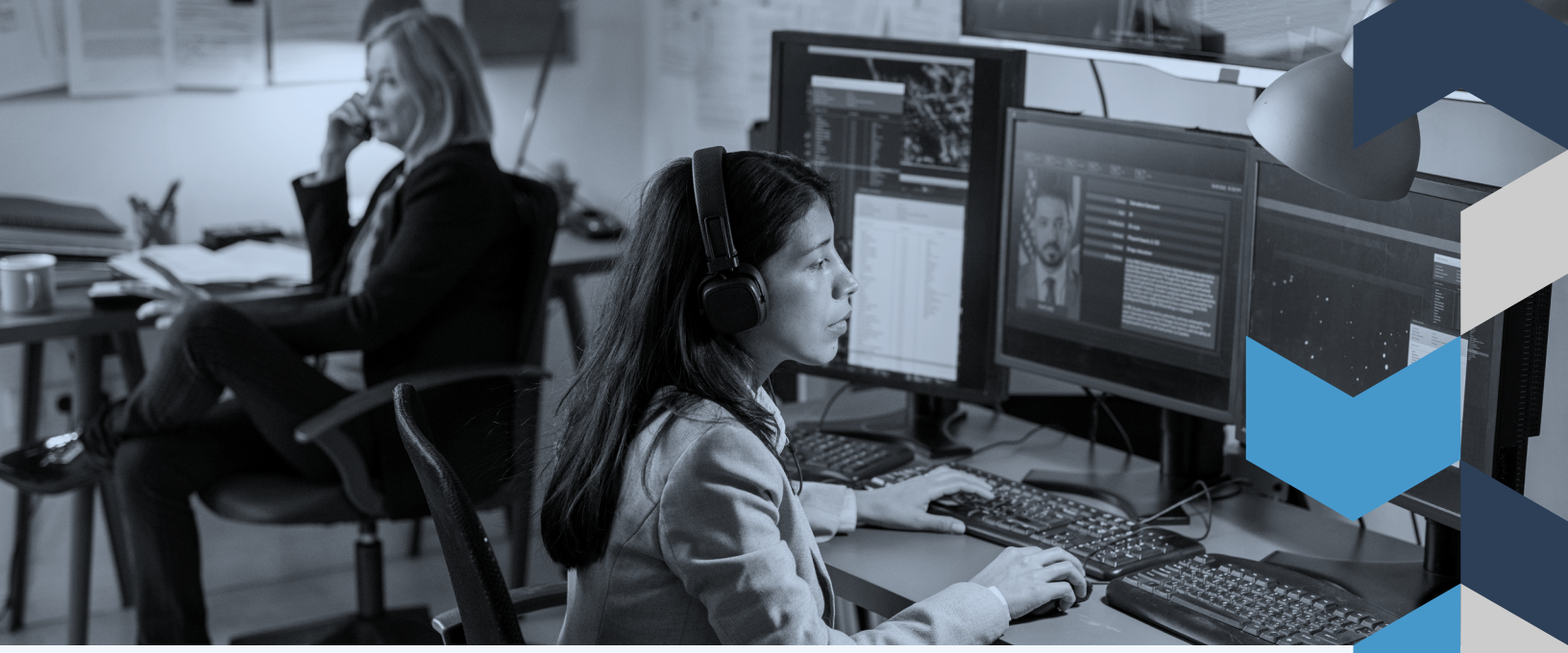
imprivata®

WHITEPAPER

Criminal Justice Information Services (CJIS) 6.0 compliance made practical

Modern access and authentication for law enforcement agencies and their partners



Executive Summary

Criminal justice information is among the most sensitive data any public agency manages. Failing to protect it can compromise investigations, endanger personnel, and erode public trust. The stakes are high, and the expectations for protecting that data are rising.

To keep pace with evolving threats and technologies, the FBI has updated its Criminal Justice Information Services (CJIS) Security Policy twice in the past year. Version 5.9.5, issued in July 2024, introduced a firm mandate for multifactor authentication. Agencies must now require at least two forms of identity verification for anyone accessing criminal justice data. In December, version 6.0 expanded those rules further by introducing new requirements for continuous monitoring, supply chain and third-party risk, and access management policies that apply across the entire lifecycle of a system.

These updates create new challenges for law enforcement. Many depend on shared computers and mobile data terminals (MDT). Some still rely on record management systems or computer-aided dispatch that do not support modern authentication methods. Almost all work with third-party contractors or consultants who need access to sensitive information. They are expected to meet these new standards without slowing down operations or increasing the administrative burden.

This white paper explains what has changed with CJIS 6.0, how those changes affect your access management responsibilities, and what it takes to comply. It also shows how Imprivata helps agencies meet these expectations in a practical, sustainable way. With modern access management tools, flexible authentication options, and full visibility into user activity, agencies can secure their systems without sacrificing efficiency.

01

Introduction to CJIS 6.0

The CJIS Security Policy was created to set clear, enforceable standards for how law enforcement agencies protect criminal justice data. It applies to every agency or department that creates, stores, accesses, or transmits this information. That includes state and local law enforcement agencies, regional task forces, third-party vendors, contractors, and anyone else who touches systems that handle sensitive criminal data.

22%

of breaches in the public sector were due to credential abuse (the most common attack vector).

Source - Verizon 2025 DBIR Public Sector snapshot

In recent years, the way law enforcement agencies operate has changed dramatically. Agencies now rely on a mix of mobile devices, legacy systems, remote users, and external partners. Threats also continue to grow and evolve. In 2024, **the FBI's Internet Crime Complaint Center (IC3)** reported 4,878 complaints from organizations within critical infrastructure sectors (including state and local government and law enforcement) affected by cyber threats. The most reported threats among these sectors were ransomware and data breaches. According to **Verizon's 2025 Data Breach Investigations Report,** 30% of compromised systems were enterprise-licensed devices, while 46% of the systems with corporate logins in their compromised data were personal devices. In response to the continued evolution and frequency of cyberattacks, the FBI released two major updates to the CJIS Security Policy in 2024.

Version 5.9.5 made multifactor authentication a requirement for every agency accessing criminal justice information. This marked a shift from recommended best practice to mandatory control. Agencies must now use at least two authentication factors for each user. These can include something the user knows, such as a password or PIN, something the user has, such as a smart card or mobile token, or something the user is, such as a fingerprint or other biometric marker.

Version 6.0 added further structure and raised the expectations around secure access and monitoring. It introduced a requirement for continuous monitoring. Agencies must now be able to detect suspicious behavior and access attempts in real time. While this does not necessarily mean proactive monitoring around the clock, it does require that agencies have tools in place to support incident detection and investigation when needed.

The policy also introduced a stronger focus on third-party and supply chain risk. Agencies must formally assess and manage the risk introduced by outside partners, including contractors, consultants, and software vendors. Lastly, version 6.0 introduced security planning requirements that span the full system lifecycle. From system design to decommissioning, security considerations must be integrated every step of the way.

These updates reflect the real-world conditions and challenges that agencies face. They acknowledge the complexity of modern operations and the growing reliance on technology partnerships. And they expect agencies to secure every access point, regardless of how or where the connection happens.

02

CJIS requirements related to access management

CJIS 6.0 places access management at the center of its compliance framework. Every user, every session, and every system interaction must now meet clearly defined standards.

Identity assurance is the foundation. Agencies must have a way to confirm that the person requesting access is who they say they are. This is not just about authentication. It also involves provisioning accounts based on least-privilege principles. Access is periodically reviewed to ensure the user still needs that access, and access is swiftly removed when the user is no longer working for the department or when nefarious activity is detected. Multifactor authentication is required for all access to criminal justice information. Passwords are no longer enough. Agencies must implement a second factor that cannot be easily guessed, stolen, or reused. This may involve a physical token, a biometric input, or a trusted mobile device.

Auditability is another key pillar. Agencies must keep detailed logs that track who accessed what, when, and from where. These records must be retained, tamper-proof, searchable, and available for review during audits or incident investigations.

Agencies must also ensure secure access for non-agency personnel. Third-party users must meet the same standards as internal staff. Their access must be controlled, time-bound, and traceable. And for shared devices, such as kiosks or MDTs, the system must isolate user sessions to prevent unauthorized viewing or data crossover.

These requirements create a strong foundation. But they also highlight the need for practical tools that can enforce policy without overwhelming IT teams or slowing down operations.

03

Challenges in securing access for internal and third-party users

Meeting CJIS 6.0 requirements is not as simple as installing a new piece of software or turning on a setting. Agencies must work around real constraints. They are tasked with managing risk across people, systems, and environments that were not designed with modern security in mind.

One of the most common challenges is managing shared workstations and fleet laptops. Officers often use the same device across shifts. These systems must support secure user switching without making logins slow or frustrating. Session data must be isolated so that one user cannot see what another was working on. And the system must be able to log every action with accuracy.

Third-party access presents another hurdle. It's common for agencies to provide vendors and other third parties supporting their operations with shared credentials or broad access to systems and data. It can be difficult to know exactly what a vendor will need access to. However, these methods do not allow law enforcement agencies to uniquely identify individual third-party users, limit access to only what is needed for their job function, and track all access activity – which are all required by CJIS.

Unlike internal identities, law enforcement agencies may not have clear visibility into the employment status and access needs of individual third-party representatives supporting their operations. This can make it difficult for agencies to adhere to least-privilege principles and revoke access in a timely manner when it is no longer needed.

Many agencies also struggle with legacy systems. These applications often predate the concept of multifactor authentication or identity federation. Replacing them may not be feasible in the short term. Still, they must be secured in a way that meets CJIS requirements.

Remote work adds another challenge. External users and off-site personnel need to connect through secure channels. That access must be traceable and enforce all authentication controls. At the same time, agencies need to avoid adding friction that slows down investigations or delays field operations. This can indirectly encourage workers to skirt security protocols.

Finally, limited resources are a constant concern. IT staff are often stretched thin. Onboarding a temporary user or setting up secure remote access can take hours that agencies do not have. Any solution must be easy to manage and work with existing infrastructure.

These challenges are not unique. Agencies across the country face the same constraints. What matters is how they are addressed.

04

How Imprivata enables CJIS 6.0-compliant access control

Imprivata offers a set of solutions that helps agencies meet CJIS 6.0 standards without adding complexity. These solutions are designed to secure access, manage identity, and provide full visibility into user activity.

For authentication, Imprivata supports a wide range of methods. Agencies can use fingerprint scanners, facial biometrics, identification badges, smart cards, one-time passcodes, PIN numbers, and mobile push verification. Even third-party users without domain accounts can be brought into compliance with flexible, secure MFA options.

Shared device support is built in. Imprivata enables fast user switching and session isolation on laptops, desktops, and kiosk systems. This ensures that every user has a secure, private session without slowing down workflow.

Legacy applications can also be secured. Imprivata provides tools that layer authentication on top of older systems, bringing them into compliance without requiring costly replacements. These applications can also be secured when offline as well when internet access is unavailable.

For third-party access, Imprivata Vendor Privileged Access Management enables secure, temporary access with full logging and policy-based expiration. Agencies can grant access quickly to only the systems, ports or hosts that are needed for their job function. They can also automatically deprovision accounts that no longer need access, reducing risk and saving time.

All activity is logged in detail. Imprivata Analytics for Enterprise Access Management provides visibility into who accessed what, when, and from where. These records are available for audit, reporting, and forensic investigation.

Together, these solutions allow agencies to secure every access point, meet CJIS expectations, and keep users productive.

05

Deployment best practices

Rolling out access controls that meet CJIS 6.0 standards can become disruptive if user experience and impact to the current workflows are not considered early in the planning. Agencies must plan carefully to ensure success without disrupting operations. While there is no one-size-fits-all approach, there are practical steps that can make deployment smoother and more effective.

Existing infrastructure such as identification badges, Active Directory, and other identity systems should be integrated into the access control solution.

One important consideration is starting with the systems and user groups that pose the highest risk. These might include shared devices in patrol cars, applications that contain sensitive investigative data, or systems used by third parties. Focusing on these areas first can help build momentum and demonstrate value quickly.

Agencies should also look for ways to use what they already have. Existing infrastructure such as identification badges, Active Directory, and other identity systems should often be integrated into the access control solution. This avoids duplication and reduces costs.

Many agencies are also in different stages of maturity with regard to their cloud adoption. It is critical to find a solution that meets the agency's current needs – whether they are running everything on-premises or mostly in cloud – and can move with them along their maturity curve at a pace determined by them. This will ensure that the agency does not have to look for multiple solutions to solve the same problem.

Training is another key factor. Users need to understand how the new system works and why it matters. Clear communication from leadership can help build support and reduce resistance to change.

Implementation should be phased and measured. Rolling out new access controls in stages allows the agency to test policies, refine workflows, and adjust settings without causing widespread disruption. IT teams can gather feedback, respond to concerns, and ensure the system is working as expected before expanding it further.

For many organizations that are short-staffed, working with a vendor with the teams, capabilities, and expertise to help rollout is key. They'll also want a vendor who can provide continuous ongoing patching and upkeep with comprehensive managed services.

Throughout the process, it is important to balance security with usability. If a solution is too slow or too complicated, users will find workarounds. The goal is to implement strong security controls that fit naturally into daily operations and do not create unnecessary obstacles.

06

Real-world use case: The City of Marietta, Georgia

A real-life example of how one community is meeting CJIS 6.0 requirements is the City of Marietta, Georgia. The City partnered with Imprivata to enhance its security and workflows with a specific focus on CJIS compliance.

Marietta faced a critical challenge: ensuring its law enforcement personnel could continue accessing essential federal crime databases while complying with the FBI's CJIS requirements. One of the most daunting mandates was the need for advanced authentication when accessing national crime databases from unsecure locations, such as patrol cars.

To meet these stringent requirements, the City of Marietta implemented Imprivata Enterprise Access Management (EAM). This solution not only enabled the City to comply with CJIS advanced authentication standards, but also revealed additional benefits. During the implementation process, the City's IT staff discovered that EAM could support several long-term goals.

Specifically, EAM provided robust authentication management and single sign-on (SSO) capabilities, enhancing information security, streamlining workflows, and boosting productivity across various City departments.

As a result, EAM was deployed on a majority of the PCs within the City's IT infrastructure, spanning departments such as police, fire, municipal courts, power and water, and others. City employees were highly enthusiastic about the productivity enhancements EAM provided.

Maintaining CJIS 6.0 compliance is challenging – but achievable

CJIS 6.0 raises the bar for access control, identity assurance, and third-party risk management. Agencies are now expected to apply consistent security practices across every user, every session, and every system. This is not a small task, especially for agencies with limited resources or complex operational needs.

Imprivata offers practical tools that help law enforcement agencies meet these standards without sacrificing efficiency. From flexible authentication options to secure third-party access and full audit reporting, Imprivata provides the foundation for secure, CJIS-compliant operations.

To take the next step, schedule a compliance readiness workshop or request a personalized demo. Protecting sensitive data is essential. With the right tools, it can also be manageable.

imprivata®

Imprivata delivers simple and secure access management solutions for mission-critical industries to ensure every second of crucial work is both frictionless and secure. Imprivata's platform of innovative, interoperable access management and privileged access security solutions enable 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

3110-2025_EAM-WP-CJIS-6.0-compliance