CJIS compliance in focus: The identity security challenges facing public safety agencies

A survey of more than 300 public safety professionals shows CJIS compliance is a top priority. But many agencies are still working through user experience challenges related to access management that make full compliance difficult in real-world operations.

EXECUTIVE LETTER

Efficiency is mission-critical

For a long time, public safety agencies' responsibility for maintaining compliance with the FBI's Criminal Justice Information Services (CJIS) Security Policy rested with IT. The auditor scheduled a visit, someone in IT pulled out a binder, and everyone else stayed out of it. But that's not how it works anymore.

CJIS compliance has become part of the day-to-day job of keeping systems secure and making information available the moment someone in the field needs it. And the conditions for getting it right keep getting harder. Your agency is probably running a mix of legacy systems and newer tools, with workstations getting shared across shifts and officers depending on mobile devices that the IT team doesn't fully control. You might also have vendors who need their own access to the network.

On top of that, cyber threats are becoming more frequent, more automated, and harder to predict, especially as attackers use artificial intelligence (AI) to scale phishing, credential theft, and other attacks against government and public sector organizations. Add in the fact that CJIS requirements are always evolving, and that's a lot to manage at once.

But in public safety, security cannot come at the expense of speed. During an emergency response, seconds matter. Identity security controls cannot slow access to CAD, RMS, dispatch, or field systems when officers, dispatchers, and command staff need information right away. Secure access must operate at mission speed: strong enough to support CJIS compliance and cyber resilience, but seamless enough for the realities of public safety work.

To get a clearer picture of how agencies are managing, Imprivata surveyed public safety professionals nationwide. Most agencies know CJIS compliance matters. Far fewer have figured out how to make it stick in daily operations. Identity security is where those two truths come together.

That's what this report is about. It covers where agencies stand today, what's holding them back, and how the agencies actually closing the gap are thinking about secure access.

We hope you find this data useful, no matter where you are on your CJIS compliance journey. CJIS compliance is not about checking a box. It is an ongoing, agency-wide mission built on continuous risk management, governance, and accountability. The challenge for agencies is meeting that mission while maintaining security and ensuring the people who serve can access the systems they need without delays that disrupt critical operations.

Policy evolves. Threats change. Your workforce adapts. The agencies that get it right design for that reality, balancing rigorous security with the operational agility required to protect the public.

Nick Stohlman

VP of CJIS Program Strategy, Imprivata

Contents

CJIS compliance: from checkbox to strategic imperative

How seriously is your agency taking CJIS compliance? If you're like most of the public safety professionals we surveyed, the answer is "very." Nearly 8 in 10 respondents called it a top or high cybersecurity priority.

Now the harder question: are you actually compliant today? Only 32% say yes. That gap is what this report digs into.

CJIS compliance isn't a contained IT project anymore. It runs straight through how you secure mission-critical systems and maintain accountability in environments where multiple users share the same workstations around the clock. It also affects whether daily operations keep moving when the systems your people need are slow or cumbersome to access.

Here's where it can get challenging. Stronger security controls are essential, but so is fast access in the field. Add repeated logins, authentication delays, legacy systems that don't integrate easily with modern technologies, and devices that need to operate beyond the agency perimeter, and agencies face a constant tug-of-war between efficiency and security.

The good news is that most agencies are taking action. Investment is flowing into multifactor authentication (MFA), single sign-on, identity governance, audit logging, and passwordless authentication. Progress is underway, but many agencies still have gaps to close in building sustainable, long-term security and compliance programs.

Key findings at a glance

- 79% of respondents rate CJIS compliance as a top or high priority within their cybersecurity strategy
- Only 32% report being fully compliant today
- Top barriers include competing agency priorities (67%) and aging infrastructure and legacy systems (61%)

About the survey

Lexipol and Imprivata surveyed 336 public safety professionals across the United States. Respondents came from law enforcement agencies at every level (local, county, state, and federal) along with broader public safety organizations. Their roles span IT, security, compliance, and public safety leadership.

What this report covers

- The current state of CJIS compliance
- Barriers preventing full CJIS compliance
- The role identity security plays in public safety operations
- Identity and access management priorities and future investment plans

Key findings

Knowing what to do isn't the same as getting it done. Most agencies know that CJIS compliance matters. But achieving full compliance means running multiple workstreams in parallel: identity, access, auditability, workflow design, and the operational processes that trust it all to happen. The CJIS Security Policy reflects exactly this tension - **79% of respondents call it a top priority, yet only 32% are fully compliant today.**

CJIS compliance is a strategic priority, but full compliance remains unfinished

Agency size makes the problem worse, not better. Among smaller agencies, 27% report full compliance. Among larger ones, only 21% do. Another 59% land in the 'mostly compliant' zone with minor gaps remaining.

If you're at a bigger agency, wondering why this keeps getting harder, you're not imagining it.

CJIS compliance is increasingly an identity and access management challenge

At its core, CJIS compliance depends on an agency's ability to answer a fundamental question: who is accessing what, from where, on which device, and at what level of trust? In public safety, that visibility is essential.

While the security implications are clear, the operational and accountability requirements are equally important. Agencies must not only protect access to sensitive systems and data, but also ensure they can verify, monitor, and audit access across users, devices, and locations.

That's why identity security has moved to the center of the conversation.

79%

OF RESPONDENTS CALL CJIS COMPLIANCE A TOP OR HIGH PRIORITY

Only 21%

OF LARGER AGENCIES REPORT FULL CJIS COMPLIANCE

59%

MOSTLY COMPLIANT

Report minor gaps still remaining in compliance coverage

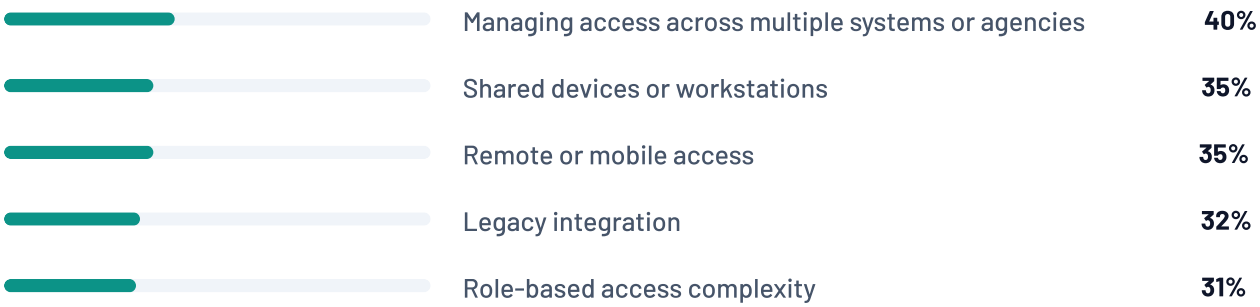
The toughest access challenges

Survey respondents identified cybersecurity risk (67%) and CJIS compliance (64%) as the two leading drivers of identity and access management investments, underscoring how closely security and compliance objectives are now linked.

These problems are more than simple IT or compliance issues. Identity security directly impacts operational continuity and the effectiveness of responders. In modern public safety environments, secure access can't create delays that impact critical emergency response workflows. In short: compliance can't distract from the mission-critical priority of saving lives.

Top access challenges

Percentage of surveyed respondents citing specific barriers to security compliance.

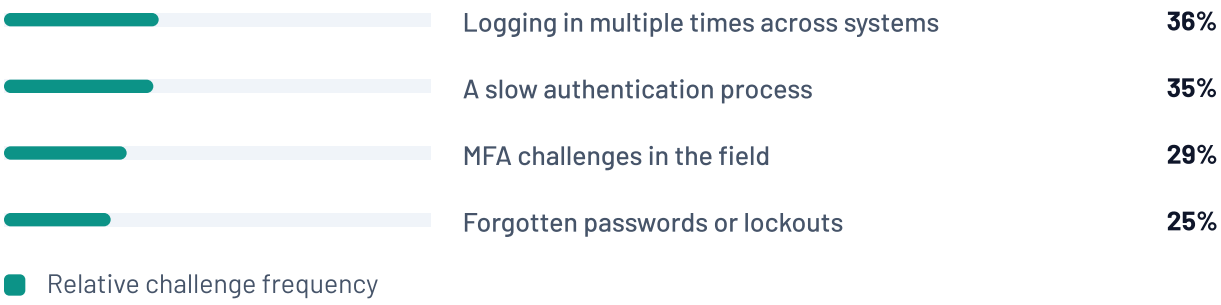


Relative challenge frequency

Operational friction is a security and public safety issue

In public safety, seconds matter. Picture this: an officer logs in for the third time in 20 minutes because three different systems each want their own authentication. The dispatcher across the room is waiting for an MFA prompt before she can pull up a record. Out in the field, a deputy watches the patrol car laptop time out again before he can finish a search. They're all facing the same challenge: security controls designed to protect sensitive information also introduce friction into workflows where every second is critical.

These are common, everyday problems. Nearly all respondents (95%) report some form of access or security friction. The most common pain points are:

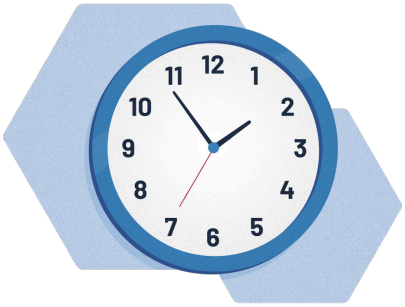


For an officer in the field or a dispatcher handling a call, a login delay is not just frustrating. It can slow access to CAD, RMS, dispatch, or field systems at the exact moment information is needed.

When that happens often enough, people adjust. They may leave a session open longer than they should. They may ask someone else to look something up. They may delay logging out because getting back in is a hassle. These choices are usually made to keep work moving, not to ignore policy. But over time, they still make it harder to prove who accessed what, when, and from where. They can also result in CJIS violations.

That is the challenge for agencies. If access is secure but too slow or awkward to use, it will not hold up in daily operations.

Agencies are navigating real barriers to full compliance



Achieving compliance is often more difficult than simply understanding the requirements. When agencies aren't fully compliant, it's almost never because they decided not to be. The reality is messier than that.

Budgets are tight. The infrastructure is old. The IT team is doing twice the work with half the people it needs. At the same time, CJIS Security Policy requirements continue to evolve, adding new layers of complexity. For many agencies, most of these problems show up in the same agency at the same time, overlapping and compounding one another.

47%

CITE COMPETING AGENCY PRIORITIES AND AGING INFRASTRUCTURE AND LEGACY SYSTEMS AS A TOP BARRIER TO FULL CJIS COMPLIANCE

Among respondents who aren't fully compliant, the top barriers are:

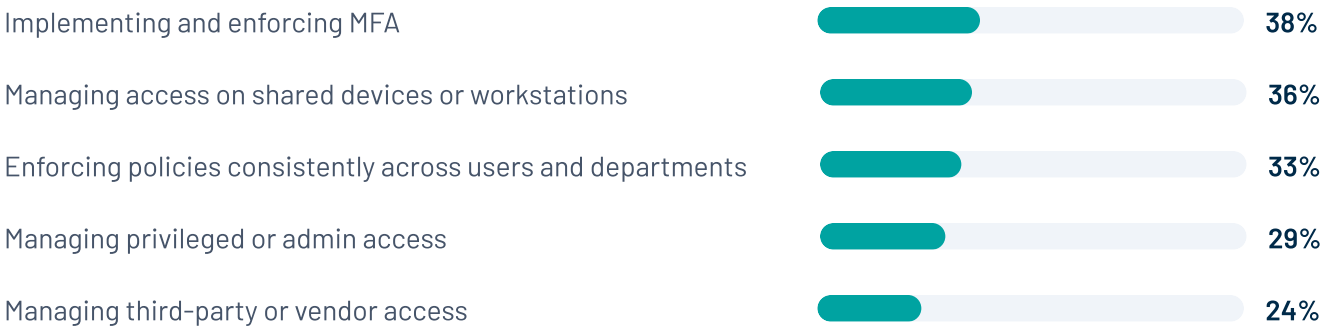
Compliance becomes even more challenging when responsibility is distributed across multiple stakeholders. While a CJIS compliance officer often serves as the primary owner, the day-to-day work typically spans public safety leadership, IT, and security teams. Without clear accountability and coordination, even well-intentioned compliance efforts can lose momentum.

MFA is widely adopted, but not yet universal or easy enough

MFA isn't optional anymore. Most agencies have embraced it as a core security control. The harder question is whether you've deployed it in a way that actually works in your environment, across every user and every device, without creating friction that disrupts daily operations. For most agencies, the answer is "not yet."

Only 38% of respondents say MFA is fully implemented for all applicable users and devices. Smaller agencies are slightly ahead of larger ones (42% versus 36%). Another 39% have rolled it out for most users or devices, but not all.

Most challenging areas for MFA



The data suggests that MFA maturity is less about awareness or deployment and more about coverage, consistency, and usability.

Modernization is already underway

Despite the challenges, agencies are making modernization a priority. Investment is flowing into identity governance, AI-driven detection, and a broader push to modernize how people log in and prove who they are. Over the next 12 to 24 months, agencies plan to invest in:

- Identity governance and role-based access controls (33%)
- Single sign-on (28%)
- New or expanded MFA deployment (27%)
- Audit and logging improvements (25%)
- Privileged access management (24%)
- Passwordless authentication (23%)

These findings reinforce a recurring theme throughout the survey. Agencies are seeking solutions that strengthen security and compliance while making access faster and more efficient for the people who rely on these systems every day.

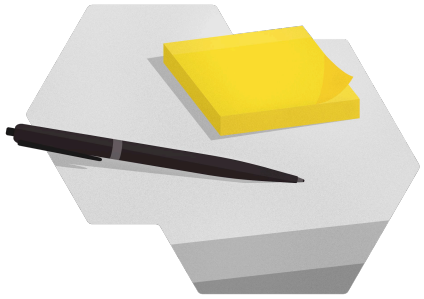
The cost of failure is operational

51%

CITE OPERATIONAL DISRUPTION AS THE TOP CONCERN FROM A CJIS-RELATED BREACH

What actually goes wrong if a CJIS-related breach happens tomorrow? For public safety agencies, the consequences extend far beyond compliance.

When sensitive systems or data are compromised, the impact is not limited to audits, fines, or regulatory scrutiny. The more immediate concern is the potential disruption to the operations that personnel depend on every day.



The respondents we surveyed had several concerns surrounding a CJIS-related data breach, including:

- Operational disruption (51%)
- Loss of public trust (42%)
- Legal or regulatory penalties (38%)

These findings reinforce an important point. For public safety agencies, identity security is what enables the people who answer the call to be effective. The ability to provide secure, reliable access to systems and information helps ensure personnel can continue doing their jobs when every second counts.

Everyone plays a role in CJIS compliance

Most agencies understand what CJIS requires. Most are actively working toward it. But the gap between intent and reality remains, and the responsibility for filling it can be difficult to understand. Regarding who owns CJIS compliance across agencies, the results varied:

- CJIS compliance officer (39%)
- Shared responsibility across teams (20%)
- Public safety leadership (19%)
- IT security (18%)

Shared workstations, mobile access, MFA enforcement, legacy integration, audit logging, and third-party access aren't separate IT problems anymore. They're all the same problem, and everyone plays a role in addressing it by keeping the right people connected to the right systems securely, every day.

With the FBI announcing an October 1, 2027, deadline, agencies should shift their attention from preparation to execution, with a defined plan in place for CJIS compliance.

What agencies should prioritize before the October 2027 CJIS deadline

Public safety agencies currently understand and prioritize CJIS requirements, but the gap between confidence and full compliance shows they need identity security that is enforceable, auditable, and built for real-world operations.

Oct. 1, 2027

FBI DEADLINE FOR CJIS SECURITY POLICY 6.0 COMPLIANCE

Here are five priorities for the agencies preparing for October 2027:

1. Treat CJIS compliance as an ongoing mission

While there is a deadline for 6.0, CJIS doesn't cease or have an end date at that time. It will remain an ongoing mission, with new versions and requirements in the future. Identity governance, authentication, access controls, audit logging, and privileged access management all need continuous attention as your environment and the threats around it keep evolving.

2. Close the MFA maturity gap

MFA effectiveness depends on consistency. The next step for many agencies is extending MFA enforcement out across users, devices, locations, and workflows without creating unnecessary friction for the realities of daily public safety operations.

3. Reduce access friction before it creates risk

Your authentication system must work across shared workstations, mobile users, field operations, and shift-based work. When the controls add unnecessary delays, people will invent workarounds. Cutting friction is a win for both usability and security.

4. Modernize around legacy systems

Legacy systems remain a reality for many agencies. Rather than waiting for a complete technology refresh, focus on solutions that integrate with existing infrastructure while creating a clear, achievable path toward modernization.

5. Build audit readiness into daily operations

Audit logging, access reporting, and role-based access controls shouldn't show up the week before an auditor arrives. Build them into how you operate every day. The visibility you get back makes both compliance and security stronger.

CJIS compliance ultimately comes down to accountability. Agencies need to know who accessed what, when, from where, and whether that access was appropriate. As technology environments grow more complex and threats continue to evolve, maintaining that visibility will remain one of the most important challenges and responsibilities facing public safety organizations.

Methodology

This report is based on a survey of 336 public safety professionals across the United States. Respondents represent a cross-section of public safety and law enforcement organizations. They include leaders and practitioners working in cybersecurity, IT, compliance, and operational decision-making.

Respondent Profile

Agency Type

Local (city/county) law enforcement	38%
County law enforcement	24%
State law enforcement	22%
Federal law enforcement	8%
Public safety agencies	6%
Other	2%

Organization Size

101-250 employees	53%
51-100 employees	18%
1-50 employees	14%
251-400 employees	11%
More than 500 employees	4%

336

PUBLIC SAFETY PROFESSIONALS SURVEYED ACROSS THE UNITED STATES

53%

WORK IN AGENCIES WITH 101-250 EMPLOYEES

38%

REPRESENT LOCAL (CITY/COUNTY) LAW ENFORCEMENT

imprivata®

Imprivata delivers access management solutions for healthcare and other 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, visit www.imprivata.com

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: +613 8844 5533