

A Practical Guide to Criminal Justice Information Services Password & MFA Compliance

What State and Local Agencies Need to Know
Before Their Next Audit



Specops, an Outpost24 company,
is the leading provider of identity
management and authentication
solutions.

What's Inside?

Executive Summary

Chapter One - CJIS: Origins, Scope and the Stakes of Non-Compliance

Chapter Two - CJIS Requirements and Best Practices

Chapter Three - A Practical Roadmap to CJIS Compliance

Chapter Four - Beyond Compliance

Chapter Five - Securing the Identity Lifecycle



Executive Summary

Password security has changed more in the last five years than in the previous twenty. For decades, the standard advice was complexity and frequent rotation: more character types, changed on a schedule. That advice is now considered weak practice, since complexity does little against credential-stuffing and breach-list attacks, and rotation on its own does not stop reuse.

Specops' 2026 [Breached Password Report](#) backs this up. It analyzed more than six billion credentials stolen by malware over twelve months. Over 4.4 billion of them were between eight and twelve characters long, the exact range most password policies treat as secure. Length and complexity did not protect them. It is clear, the traditional model of what counts as a strong password is outdated.

Artificial intelligence (AI) has exacerbated the problem. [Microsoft's 2025 Digital Defense Report](#) found AI-powered phishing campaigns achieve a 54% click-through rate, more than four times the roughly 12% rate for traditional phishing. The same report recorded a 195% year-over-year rise in AI-generated identities used to bypass verification systems. Identity, not the network perimeter, is now where most attacks land.

Regulators are responding accordingly, and not only in law enforcement. [PCI DSS 4.0's](#) expanded multi-factor authentication requirements became mandatory on March 31, 2025, and the EU's [Digital Operational Resilience Act](#) (DORA) has imposed strong authentication requirements on financial-sector firms and their ICT providers since January 17, 2025. [NIST](#), [HIPAA](#), and [GDPR](#) have moved in the same direction. Within US law enforcement, that shift shows up in the Criminal Justice Information Services (CJIS) Security Policy, which sets the security requirements for any organization that accesses or supports Criminal Justice Information (CJI).

Under CJIS 6.0 and 6.1, Priority 1 controls, including multi-factor authentication (MFA) and password and authenticator management, are already sanctionable. The remaining controls must be in place before the current compliance cycle, known as the zero cycle, ends on September 30, 2027. Together, this signals that CJIS's cybersecurity expectations are rising now, with more to come, particularly around access and identity.

This white paper gives state and local agencies what they need to know to be ready for their next CJIS audit, covering:

- This white paper walks through what state and local agencies need to know to be ready for their next CJIS audit, including:
- What CJIS 6.0 and 6.1 require, and what changed between the two versions
- Who is subject to CJIS standards, and the consequences of non-compliance
- A practical roadmap to compliance, and how to reduce risk across the entire identity lifecycle



Chapter One

CJIS: Origins, Scope and the Stakes of Non-Compliance

1.a The Origins of CJIS

CJIS traces back to 1924, when the FBI began centralizing fingerprint records submitted by police agencies nationwide, the first coordinated national effort of its kind. The CJIS Security Policy itself followed decades later, established in 1998 to set minimum security standards for accessing that data as it moved onto networked systems.

That 1998 policy held largely unchanged for over twenty-plus years, while the world around it did not. Broadband, widespread internet access, and cloud computing gave agencies far easier ways to reach CJI remotely, and cybercrime scaled right alongside that access.

In 2020, the CJIS Advisory Policy Board acknowledged the need to modernize CJIS policy, empowering the FBI CJIS Division's Information Security Officer, Chris Weatherly, to lead a full re-evaluation and rewrite of the then-current CJIS Security Policy, version 5.9. Weatherly, who joined the FBI in 1994 and has led the CJIS Division's information assurance function since 2017, has since described the resulting policy as "roughly 50% new." It was this largely new iteration that became CJIS Security Policy 6.0, finalized in December 2024.

CJIS 6.0 restructured the policy around the NIST SP 800-53 Revision 5 control catalog, giving agencies a ready-made, NIST-aligned baseline to build from. It marked a distinct shift away from a checklist approach and toward continuous risk management, governance, and accountability. [Version 6.1](#), released in June 2026, refines that same framework rather than radically altering it.



1.b Who Does CJIS Apply To?

CJIS applies to every individual, agency, and private company that creates, stores, transmits, or otherwise processes CJI. Each authorized entity is identified through a unique, nine-character Originating Agency Identifier, the mechanism the FBI uses to track exactly who has access to CJI and hold them accountable for protecting it.

In practice, that reaches well beyond sworn law enforcement. It covers police departments, sheriffs' offices, courts, and corrections facilities directly, along with federal and civil agencies, social services, and motor vehicle departments that run background checks against CJI.

Education and health services organizations fall in scope wherever their own background check processes touch CJI. The private sector is included as well: companies hosting public safety software, such as AWS GovCloud and Microsoft Government Cloud, and software developers building dispatch tools, records management platforms, or evidence tracking systems for criminal justice customers.

Enforcement runs through each state's own CJIS Systems Agency, so specific requirements and audit timing can vary from state to state. Texas DPS, for example, states in its own [CJIS documentation](#) that all Texas CJIS audits through March 31, 2027 are conducted against version 5.9.5, not 6.0 or 6.1, with 6.1 recommended only for gap assessment planning at this stage.

Organizations concerned about CJIS requirements should confirm with their own state's CJIS Systems Officer which policy version their next audit will be measured against.

1.c The Consequences of Non-Compliance

The most immediate consequence is a technical one, though not always an instant one. A CJIS audit finding does not automatically mean an agency loses access to CJIS systems. Agencies are expected to respond with a corrective action plan, and findings stay under review until remediation is sufficient. But that runway is not indefinite. Continued failure to close the gap can lead to further sanctions, including suspension or termination of access to systems like the National Crime Information Center.

Washington State Patrol (WSP) experienced exactly this in June 2025, when an [FBI audit](#) conducted against version 6 of the CJIS Security Policy identified compliance issues. The gaps were under IA-2(1) and IA-2(2), covering multi-factor authentication for privileged and non-privileged accounts. WSP subsequently confirmed that it was preparing its response to the FBI and developing a plan to resolve the findings.

Vendors face a different kind of exposure: not access loss, but the contract itself becoming impossible to fulfill. Louisiana's own vendor management program states that a vendor's CJI access will be terminated and they will be removed from the approved vendor list if they fail a compliance audit, miss required response timelines, or mishandle a security incident without adequate remediation. [Michigan State Police](#) applied that same standard in practice in 2025, dropping its media disposal vendor, Vital Records Control, after an assessment found the vendor out of compliance.

Beyond access and contracts, there is a financial and reputational dimension as well. Public agencies found in willful violation risk losing federal grants and state public safety funding tied to CJIS compliance, and audit findings can escalate to the CJIS Advisory Policy Board, compounding the damage of a failed audit.

CJIS compliance is not a routine paperwork exercise. It decides whether an agency can operate its own systems, whether a vendor keeps the contract they already have, and whether the funding behind either of them stays intact. That makes it a business imperative as much as an operational one, and a foundation for a genuinely proactive identity security strategy, not just a compliant one.



Chapter Two

CJIS Requirements and Best Practices

2.a What are the CJIS Policy Requirements?

CJIS's 20 policy areas span more than passwords and MFA. Access controls and authentication sit alongside incident response, system security, and supply chain risk, covering the full range of how an agency handles CJI, not just how someone logs in. Across those areas, the core responsibilities break down into a few consistent themes:

Controlling who can access CJI by managing accounts (including applying least privilege), and removing access when it is no longer required.

- Identifying and authenticating users, including using MFA for both privileged and non-privileged accounts.
- Managing personnel security and training, ensuring that users understand their responsibilities and providing role-based training.
- Protecting CJI wherever it is handled, stored, accessed, and transmitted.
- Securing and maintaining systems by using secure configurations, managing vulnerabilities, and carrying out maintenance securely.

- Preparing for disruption with robust contingency and recovery plans, as well as reporting incidents correctly.
- Managing third-party and supply chain risk with formal agreements and expectations in place for service providers and contractors.

Password and MFA requirements are one piece of a much larger policy, and it is easy to feel a false sense of security about this particular piece. Often, organizations assume that AD already has it covered, or that Microsoft Entra Password Protection closes whatever gap is left. This white paper shows where that assumption breaks down, and what actually meeting IA-2 and IA-5 requires.

2.b What is New in CJIS 6.1

Unlike the leap from version 5.9 to 6.0, which rebuilt the policy from the ground up around a new NIST-aligned control structure, 6.1 is a cleanup of 6.0, not a new baseline.

Where 6.0 restructured the policy into 20 policy areas, 18 of them mapped directly onto [NIST SP 800-53](#) control families, 6.1 mainly updates terminology within that same structure. Although the refinements to 6.1 are minimal in terms of impact, they are a signal that organizations should treat CJIS compliance as an ongoing discipline requiring continued attention.

Whatever version governs an agency's next audit, whether that is 6.1, 6.0, or an earlier release still in force in their state, the goal should be the same: sustained readiness, not reactive compliance.

2.c Best Practices for CJIS Compliance

Acknowledge Your Gaps

Most organizations assume their existing password rules are close enough. That assumption is where many agencies fall short during an audit. The only way to know for certain is a baseline assessment of current password policy against CJIS requirements.

Once gaps are identified, document them against the specific control each one maps to: IA-5 for password and authenticator management, IA-2 for MFA. That way, the evidence already exists before the audit letter arrives, rather than being assembled under pressure afterward.

Move From Reactive to Proactive Identity Management

A compromised credential rarely gets used the moment it is stolen. It is more likely to sit for sale on the dark web first, then surface in an attack months later. [Verizon's 2026 Data Breach Investigations Report](#) found that 73% of ransomware victims had an infostealer infection or credential leak in the prior year, half of those surfacing within 95 days of the attack.

That gap is exactly what CJIS IA-5 is built to close. Blocking compromised or commonly used passwords only works if it happens continuously, catching a credential the moment it turns up breached and prompting an immediate reset rather than waiting for the next scheduled check. A password confirmed safe once is not the same as a password kept safe.

Balance Access, Risk, and UX

Extend MFA to every login point, not just the one that is easiest to secure. IA-2 requires coverage across privileged and non-privileged accounts alike, including Windows logon, remote access, and offline scenarios, and a gap at any one of them is a gap in the



requirement itself. But full coverage carries its own risk if it ignores the user experience. A control people find ways around stops functioning as a control at all. The practice that holds both truths at once is pairing full coverage with clear, real-time guidance at the point of authentication, so users understand what is being asked of them and why, rather than looking for a way past it.

Automate What You Can't Afford to Forget

Manual processes are the ones that fail under pressure. A policy that depends on someone remembering to check it, update it, or enforce it consistently will eventually lapse, usually at the worst possible time. Automating identification, enforcement, and documentation wherever possible is what keeps the practices above working when nobody is actively watching them. None of the four practices above need to live in separate tools, chased down individually by an already stretched team. The right platform brings password policy, continuous breach screening, and MFA coverage together in one place, which is worth keeping in mind before building this out piece by piece.

Chapter Three

A Practical Roadmap to CJIS Compliance

1. Get Visibility Over Your Risk

You cannot fix what you cannot see, and without visibility, an organization cannot fully understand its own risk. Visibility is what turns remediation from guesswork into something structured and targeted, with issues addressed in order of actual risk rather than whatever surfaces first.

IA-5, Authenticator Management, specifically requires organizations to identify and assess weak, outdated, or non-expiring authenticators across their environment, not just confirm a policy exists on paper.

Specops Password Auditor supports that requirement with a free, read-only scan of your AD, surfacing compromised, blank, and non-expiring passwords. Because it runs from any domain-joined workstation, there is no new infrastructure to stand up before that first scan can happen.

The report Specops Password Auditor produces ranks findings by severity and maps each one to the specific requirement it fails to meet, giving security teams a clear picture of where the highest-risk exposures sit at no cost, and giving leadership evidence they can take to a board conversation about risk management.

2. Screen Every Password Against Live Breach Data

IA-5 does not actually require complexity in the way most legacy policies still enforce it. The requirement is length and a blocklist: memorized secrets must be at least eight characters, agencies must allow much longer passphrases, and new and existing passwords alike must be checked against a list of commonly used, expected, or compromised values before they are accepted. That is a different problem to solve than the one most password policies were built for.

Specops Password Policy applies those rules directly in AD, enforcing length requirements and passphrase support beyond what native Microsoft tooling offers, with password changes triggered on expiration or on evidence of compromise rather than a fixed schedule alone. Its Breached Password Protection feature is what actually closes the blocklist requirement: it checks AD continuously against a database of more than 6 billion compromised credentials, not only at the moment a password is created or reset, so a password that looks safe today does not get to stay unchecked once it is not.



3. Beyond MFA, Secure Access at Every Point of Entry

IA-2 requires MFA for both privileged and non-privileged accounts under IA-2(1) and IA-2(2), aligned to Authenticator Assurance Level 2 (AAL2) under NIST's digital identity guidelines. Specops Secure Access delivers that with phishing-resistant MFA on Windows logon, Remote Desktop Protocol, and offline and remote logons. These are the access points a single cloud sign-in screen never touches.

For an officer working out of a patrol vehicle, MFA has to hold up on intermittent connectivity and still be fast enough to use mid-shift. Flexible authentication methods, rather than one fixed factor, are what make that possible without asking the officer to trade speed for security. Specops Secure Access supports offline MFA through one-time password codes generated on an authenticator app or a YubiKey, so a dead zone does not mean a locked-out officer or a workaround that skips the control entirely.

Specops Secure Access also supports Single Sign-On and Software as a Service applications via OIDC and SAML, and integrates with SIEM, SOC, and analytics platforms through its Event API, giving security teams visibility into authentication events without adding a separate system to manage.

Chapter Four

Beyond Compliance

Reducing Risk Across the Entire User Lifecycle

CJIS sets a genuinely strong security foundation. Meeting its password and MFA requirements is real progress toward securing an entire agency's identity infrastructure. But a foundation is a floor, not a ceiling, and CJIS itself keeps expanding to close whatever gaps remain. Organizations that build beyond today's requirements, rather than waiting for the next version to mandate them, are the ones best positioned when it does.



Extending Trust to the Device, Not Just the Credential

A verified user is not the same as a secure one. CJIS's password and MFA requirements confirm who is logging in, but not what device they're logging in from, and that distinction is exactly what attackers have started exploiting instead of trying to beat authentication directly.

CJIS's own trajectory points the same way. Version 6.0 and 6.1 have both tightened how identity is verified and closed access gaps further with each release, and the device an identity operates from is the natural next extension of that same emphasis. As zero trust principles take hold more broadly across cybersecurity, the device itself is increasingly treated as part of the perimeter, not just the credential presented from it.

Verified Identity, Unverified Device

Bybit's 2025 breach shows exactly why that matters. In February 2025, attackers compromised the device of a developer at Safe{Wallet}, a third-party wallet provider Bybit relied on for transaction approvals. From that single compromised device, they altered what Bybit's own signers saw on their screens, making a fraudulent transaction appear routine. The signers were legitimate, verified users acting exactly as their MFA and credentials confirmed they should. It was the device presenting the transaction to them that could not be trusted, and it cost Bybit roughly \$1.5 billion, the largest crypto theft on record.

Specops Device Trust is built for exactly this pattern: it binds identity to an organization's own approved devices and checks their posture continuously, not just once at login, so trust in

a device or session isn't assumed to hold indefinitely once it's been granted. None of this is required by CJIS today, but building toward continuous device verification now is a reasonable way to stay ahead of policy updates, rather than catch up once it becomes mandatory.

Chapter Five

Securing the Identity Lifecycle

Why Organizations Choose Specops

Most organizations meet CJIS requirements the hard way: one tool for password policy, another for MFA, a third added later for service desk verification, each bought at a different time to solve a different problem. That approach is manageable day to day, but it falls apart at audit time, when someone has to pull evidence from three or four disconnected systems and present it as a single, coherent story. Consolidation is not a nice-to-have here, it is what makes an audit something an agency can walk into with confidence rather than apprehension.

Specops solves that by covering the full identity lifecycle, password, MFA, self-service reset, service desk verification, and device trust, from a single vendor built specifically around AD. One point of contact, one relationship to manage, no gaps between vendors for an attacker or an auditor to find.

That consolidation matters beyond any single audit. CJIS has been revised six times since its 2020 modernization began, and there is no reason to expect version 6.1 is the last word. Agencies juggling several vendors have to track several roadmaps every time the policy shifts. Agencies working with one vendor do not.

Meeting CJIS's Priority 1 controls, IA-2 and IA-5, should be treated as a good starting point, not a finish line. Specops is built for that reality, designed to help an agency's identity strategy move at the same pace as the threats and requirements it is meant to outlast.



Get Started With Specops

If you are ready to find out more about how Specops can support CJIS compliance, download Specops Password Auditor for a free baseline report of exactly where your AD stands today, book a demo to see how Specops can help your organization succeed at its next CJIS audit, or talk to an expert about what a full identity security strategy looks like for your agency, beyond the audit.

[Book a Demo](#)[Download Specops Password Auditor](#)

Specops

Specops Software, an Outpost24 company, is the leading provider of identity management and authentication solutions. Specops protects your business data by blocking weak passwords and securing user authentication. With a complete portfolio of solutions natively integrated with Active Directory and Entra ID, Specops ensures that sensitive data is stored securely, either on-premises or within your Entra ID tenant, and remains under your control. Specops Software was founded in 2001 and is headquartered in Stockholm, Sweden with additional offices in the US, Canada, the UK, and Germany.