

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

Overview: The FBI’s *Criminal Justice Information Services (CJIS) Security Policy* Version 6.0 (effective Dec 2024) introduced important updates from Version 5.9.5 (Jul 2024). This white paper summarizes **critical technical recommendations** based on those updates, tailored for city and public safety leaders. Each recommendation is mapped to the relevant CJIS Policy Area, the FBI’s priority level (P1 = highest priority), and what we call a control’s “quick name.”

These changes aim to strengthen cybersecurity and compliance for all agencies handling Criminal Justice Information (CJI). City managers and police chiefs – especially in smaller municipalities – can use this as a checklist for due diligence.

Contents

Key CJIS v6.0 Technical Recommendations (with Policy Mapping).....	2
Multi-Factor Authentication (Privileged & Non-Privileged Accounts)	2
Authenticator Management (Password Policies & Banned Passwords)	2
Cryptographic Protection (Encryption).....	4
Continuous Monitoring (Audit Log Review & Alerts).....	5
Supply Chain Risk Management Plan.....	6
Personnel Screening & Agreements	7
Incident Response Plan – Breaches	9
Additional Guidance for City Leaders	11
Executive Engagement	11
Policy Updates & Training	11
Technology and Budget Considerations.....	12
Shared Risk and Responsibility with Vendors	12
Looking Ahead	13
Legal Disclaimer.....	13

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

Key CJIS v6.0 Technical Recommendations (with Policy Mapping)

Policy Area	Priority	Control (Quick Name)	Summary of Recommendation
Identification & Authentication (IA)	P1	Multi-Factor Authentication (Privileged & Non-Privileged Accounts)	<p>Enforce Multi-Factor Authentication (MFA) for all user access to CJI systems, including both administrative (privileged) and standard accounts. <i>CJIS v6.0 now mandates MFA</i> not only for remote admins but for all users accessing CJI remotely or from unsecure locations^{1 2}. This means users must authenticate with at least two factors (e.g. password + token or biometric) when logging into CJI applications. Ensure your officers and staff are equipped with approved MFA methods (e.g., a hardware token or authenticator app,) and that no CJI access is allowed without MFA. We typically recommend Cisco Duo Authenticator, which can also work with hardware keys for organizations that do want to use smartphones.</p>
Identification & Authentication (IA)	P1	Authenticator Management (Password	<p>Adopt strict password and authenticator policies in line with CJIS v6.0's new</p>

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

		<p>Policies & Banned Passwords)</p>	<p>requirements. Implement a banned password list of commonly-used or compromised passwords and update it at least quarterly³. Configure systems to automatically check new passwords against this list and reject any that are too weak or known to be compromised⁴. Allow and encourage passphrases (long passwords) and avoid arbitrary complexity rules in favor of checking against the banned list. Additionally, require immediate password changes if an account is recovered or there's evidence of compromise^{5 6}. These measures help prevent users from choosing trivial passwords (like "Winter2026!" or "Password123"), thereby reducing the risk of account breaches. Our password manager can assist with tracking and securing maintaining highly complex passwords for all systems and</p>
--	--	---	---

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

			centrally manage when people leave the organization.
Systems & Communications Protection (SC)	P1	Cryptographic Protection (Encryption)	<p>Use strong encryption for CJI data in transit and at rest. CJIS 6.0 reinforces that any transmission of CJI over networks (especially public networks or wireless) must be protected with cryptographic mechanisms that ensure confidentiality and integrity⁷. In practice, this means using FIPS 140-2 approved encryption (e.g., TLS 1.2+ for data in motion, and AES-256 for data “at rest”) for all CJI. For example, emails or database connections containing CJI should use end-to-end TLS encryption, and laptops or USB drives storing CJI should employ full-disk encryption. “Approved encryption” in CJIS is defined as cryptography vetted by NIST/FIPS⁸. Ensure your IT infrastructure (VPNs, Wi-Fi, mobile devices, body cams, cloud services, backups, etc.) complies with this by enabling encryption options and using only CJIS-compliant ciphers. This could mean our email</p>

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

 **Address:** 1670 Keller Parkway, Suite 130, Keller, TX 76248-3769  **Phone:** 817-337-0300

 **Email:** sales@fulcrumgroup.net  **Website:** <https://www.FulcrumGroup.net>

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

			encryption solution that uses AS256.
Audit & Accountability (AU) (and Assessment & Authorization – CA)	P1	Continuous Monitoring (Audit Log Review & Alerts)	<p>Implement a continuous monitoring program for your IT systems that handle CJI. Under CJIS 6.0, agencies are expected to go beyond periodic audits and establish <i>ongoing</i> oversight of security controls⁹. This involves: regularly reviewing audit logs of system and user activity, setting up automated alerts for suspicious events, and conducting periodic security self-assessments. For example, ensure that logins, queries, and data exports in state databases are logged and have an assigned reviewer who checks for anomalies (e.g., logins at odd hours or excessive queries by a single user). Utilize tools or an SIEM to correlate and analyze log data in real-time for threats¹⁰. Continuous monitoring helps catch issues early – such as an account misuse or an external attack – and is now a top-priority control in CJIS (Priority 1). We can provide a third-party service to review security logs</p>

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

			24x7 and alert to attempts at intrusion. The platform also connects to Office 365, a common vulnerability area some organizations do not consider.
System & Services Acquisition (SA) (and new Policy Area: Supply Chain Risk Mgmt (SR))	P2	Supply Chain Risk Management Plan	Establish supply chain security practices for all IT systems and services. CJIS v6.0 added Supply Chain Risk Management (SR) controls, meaning agencies must account for risks posed by vendors, hardware suppliers, software developers, and third-party services. Develop a formal Supply Chain Risk Management Plan (SR-2) ¹¹ that, at minimum, documents how you vet third-party providers for security. For example, require vendors to disclose their security controls, incident history, and to sign the CJIS Security Addendum (for any who may encounter CJI). Notification agreements (SR-8) should be in place – vendors must agree to promptly inform your agency of any cyber incidents or changes that could affect CJI ¹² . Inventory critical components

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

 **Address:** 1670 Keller Parkway, Suite 130, Keller, TX 76248-3769  **Phone:** 817-337-0300

 **Email:** sales@fulcrumgroup.net  **Website:** <https://www.FulcrumGroup.net>

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

			<p>(servers, network gear, cloud software) and ensure you source them from reputable, trusted providers. Also, include security requirements in procurement: e.g., when buying a new records management system, mandate CJIS compliance and perhaps request independent audit results. Finally, plan for component disposal (SR-12)¹³ – have policies for securely wiping or destroying retired devices that held CJI. By treating the supply chain as part of your security program, you reduce the risk of breaches via vendor vulnerabilities or compromised equipment.</p>
<p>Personnel Security (PS)</p>	<p>P2</p>	<p>Personnel Screening & Agreements</p>	<p>Strengthen personnel vetting and agreements. Human factors are critical: CJIS requires that any individual with access to CJI – be it a police officer, IT admin, contractor, or volunteer – undergo proper screening and be bound by security agreements. Ensure your hiring and contracting process includes fingerprint-based background checks (Personnel Screening) for all CJI-access personnel (this is</p>

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

			<p>usually mandated by state law/CJIS policy) and that results are reviewed for suitability. Implement a formal policy for personnel termination and transfer to immediately revoke CJI access when someone leaves or changes roles (CJIS PS-4, PS-5). Additionally, have all staff sign Access Agreements (PS-6) acknowledging their security responsibilities¹⁴. This includes confidentiality/non-disclosure agreements and the FBI’s CJIS Security Addendum for contractors. CJIS v6.0 also introduced External Personnel Security (PS-7) focusing on contractors/third-parties – treat them like your employees in terms of vetting and training. In short, double-down on the “people” side of security: only trustworthy, trained individuals should handle CJI, and they must formally accept that responsibility¹⁵. Our engineers are finger printed as well and must maintain security awareness training in our system at a more advanced</p>
--	--	--	---

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

			level than the standard CJI training.
Incident Response (IR)	P2	Incident Response Plan – Breaches	<p>Develop and drill an Incident Response Plan that meets CJIS expectations, specifically addressing data breaches. CJIS v6.0 places fresh emphasis on <i>prompt reporting</i> of security incidents. Your agency should have a written Incident Response (IR) plan that defines steps to take if CJI is lost, stolen, or hacked. Include notification procedures so that, for example, if a laptop with CJI is stolen or a server is compromised, your LASO or IT lead knows to notify the State CJIS ISO or FBI CJIS Division immediately (typically within 24 hours or as required by your CSA). Train staff on recognizing and reporting incidents (CJIS requires “breach” training for personnel under IR-2(3)¹⁶). We can work with you on details of the plan as well as share some of the DIR resources for plans and tabletops. Regularly test the plan with tabletop exercises – e.g., simulate a ransomware attack on a records system – so that both technical staff and leadership</p>

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

			<p>know their roles. The plan should cover containment (e.g., disconnecting affected systems), eradication (removing malware), recovery (restoring backups), and lessons learned documentation. Being prepared not only meets CJIS IR-8 (1) Breach Response obligations¹⁷, but it also minimizes damage and liability when an incident occurs. Smaller towns and cities can also engage Texas Municipal League as they also have resources designed to help member cities.</p>
--	--	--	---

Notes: “Priority” (P1, P2, P3, P4) corresponds to the FBI’s designation of control importance – P1 controls are most critical¹⁸ ¹⁹. All the above recommendations align with P1 or P2 controls, meaning CJIS and the Advisory Policy Board consider them high priority for implementation. Also, while technical details are cited from CJIS Policy, the implementation in your local environment should be guided by your IT staff or service providers.

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

Additional Guidance for City Leaders

Executive Engagement: City managers, leaders and police chiefs should treat CJIS compliance as an ongoing governance issue, not a one-time or IT only task. You don't have to be technical to manage technical processes. Like other areas, you just want to develop the ability to ask questions or develop basic metrics to measure and manage the process and systems.

Set up regular briefings with your IT director, vendors or IT partners on the status of these controls (MFA deployment, training completion, log monitoring results, etc.). This not only keeps you informed but also signals to all departments that leadership is serious about cybersecurity. There might even be implications related to open records requests via the Texas Public Information Act (PIA).

We'd also recommend you subscribing to threat intelligence feeds where you can get periodic emails about threats and vulnerabilities that are targeting local government. You don't even have to be a technical expert to understand them. You can simply put the threat in front of your technical contact and ask them if that's a concern or if you're protected. Here is our favorite one for local government.

<https://www.cisa.gov/topics/cyber-threats-and-advisories>

Policy Updates & Training: Update your department policies to reflect these CJIS 6.0 changes. For instance, if your current policy manual doesn't mention multi-factor auth or the new password rules, revise it. Then, ensure all users are trained on any new procedures (e.g., how to use the MFA token, how to report an incident). Remember that **CJIS Security Awareness Training (Policy Area 2)** is required every two years for all CJI-authorized personnel; use that training to reinforce these specific updates (like why writing down passwords is now even more risky given new rules, or how to handle suspect phishing emails to avoid breaches).

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

 **Address:** 1670 Keller Parkway, Suite 130, Keller, TX 76248-3769  **Phone:** 817-337-0300

 **Email:** sales@fulcrumgroup.net  **Website:** <https://www.FulcrumGroup.net>

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

Technology and Budget Considerations: Some of these recommendations may require new tools or services:

- If you don't already have an MFA solution, you'll need to implement one (there are government-friendly options like Duo, Microsoft Authenticator, hardware tokens, etc.).
- Complying with log management and continuous monitoring may require a Security Information and Event Management (SIEM) system or Managed Detection and Response (MDR) log monitoring service.
- Verify that all software your city uses (CAD/RMS, court systems, cloud storage, body camera archives, etc.) can meet the encryption and logging requirements. If not, work with vendors on updates or plan for migrations to compliant solutions.
- Consider running assessments of your environment for vulnerabilities. This could be as simple as a vulnerability scan or a little bit more comprehensive and an automated pen test. These are tools that can help you identify concerns before an attacker tries to take advantage of them.

Shared Risk and Responsibility with Vendors: *Many towns, cities, counties and other use third-party vendors, larger entities or cloud services for IT and CJIS-related functions. CJIS Policy **explicitly holds the criminal justice agency (your police or sheriff department) accountable for compliance** – even if a vendor is involved. It's critical to engage your vendors in meeting these requirements.*

For example, if you use a cloud-based dispatch system, ask the provider to confirm in writing that their system enforces MFA (is it even configured), encryption (at what level), audit logging (are logs preserved somewhere), etc., in accordance with CJIS. Ensure that **contracts include CJIS clauses** (like the Security Addendum) and that vendors agree to cooperate with audits and incident response.

Essentially, treat vendors as an extension of your agency: you manage the risk together, but *your agency bears ultimate responsibility* to the FBI. Having a clear understanding

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

 **Address:** 1670 Keller Parkway, Suite 130, Keller, TX 76248-3769  **Phone:** 817-337-0300

 **Email:** sales@fulcrumgroup.net  **Website:** <https://www.FulcrumGroup.net>

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

with vendors will protect the city and align expectations (e.g., who will notify whom if there's a breach, specific points of contacts like who the vendor's Security Officer is, how data is securely returned or wiped at contract end, etc.).

Looking Ahead: CJIS Security Policy will continue to evolve (v6.1, 6.2, etc.). Many of the changes in v6.0 align CJIS with broader federal standards (NIST). City leaders should strive to create a culture of compliance that can adapt to new requirements. This means building flexibility and security consciousness: when new tech or practices emerge (drones, AI analytics, Smart Grids, Self-driving Cars, Green Technologies, etc.), ask "How does this impact CJIS compliance? Do we have controls in place to handle the data securely?"

By baking these questions into planning processes, you'll stay ahead of the curve. Consider designating a **CJIS Compliance Officer** or leveraging your preferred consultant who can periodically review your setup against the latest policy (kind of like a mini-audit) to catch gaps before an official audit does. However, there is currently only one CJIS Auditor for the State of Texas, and so far, he seems to be fairly easy-going on helping diligent towns and cities get up to speed on their gap areas.

Finally, remember that these technical controls not only satisfy CJIS rules but also **reduce the risk of a data breach** that could fundamentally damage public trust or incur liability. Investing in cybersecurity and compliance is investing in the integrity and reputation of your city's justice system and trust of your council and citizens.

Legal Disclaimer

The information provided in this document is intended for general guidance and educational purposes only. It is not legal advice and should not be relied upon as such. Your municipality's obligations under the CJIS Security Policy or other laws may vary based on specific circumstances. Always consult with your agency's legal counsel and security professionals to tailor compliance efforts to your situation.

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

This white paper is provided “**as is**” without any warranties. While we strive for accuracy (with references to official policy sources), The Fulcrum Group, Inc. (author) **assumes no liability** for any errors or omissions or for actions taken in reliance on the information herein. Implementing the recommendations in this document does not guarantee compliance or complete security. *CJIS compliance is ultimately the responsibility of the criminal justice agency.*

By using this document, you agree that The Fulcrum Group, Inc. and its employees shall **not be held liable** for any direct, indirect, or consequential losses arising out of or in connection with the use of or reliance on the content. Always perform due diligence and, where appropriate, seek independent audits or reviews for CJIS compliance. Your agency is encouraged to refer to the official **CJIS Security Policy v6.0** document and any guidance provided by the Texas Department of Public Safety (TxDPS) CJIS Security Office for authoritative requirements.

The Fulcrum Group is a historically underutilized business located in the Dallas-Fort Worth area and providing services in Texas for over 20 years. You Learn more about the Fulcrum Group and our services at our website. Also note our government contracts allow you to easily do business with us.

<https://www.fulcrumgroup.net/local-government/>

Services

- SPOT Managed Services <https://www.fulcrumgroup.net/managed-it-services/>
- Managed Security <https://www.fulcrumgroup.net/managed-security/>
- Cloud Computing <https://www.fulcrumgroup.net/cloud-computing/>
- VoIP Services <https://www.fulcrumgroup.net/voip-services/>
- AI and Automation <https://www.fulcrumgroup.net/ai-and-automation/>
- SPOT Shield Managed cybersecurity bundle for local government
<https://www.fulcrumgroup.net/services/cybersecurity-solutions/spot-shield-for-local-govt-compliance/>

(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

CJIS Security Policy 6.0 Changes

Key Technical Recommendations and Updates (from 5.9.5)

Government Contracts in Texas

- CMBL# 1710899639200
- HUB Vendor ID/# 1710899639200 / 29199
- DIR Contract # DIR-CPO-5031Managed Services
- Software, Commercial Off-The-Shelf (COTS) RFO DIR-CPO-TMP-570
- NCTCOG Artificial Intelligence- Contract # 2025-018



(C) 2025 The Fulcrum Group, Inc., Texas. All rights reserved. This document may be shared for non-commercial use with attribution to the source.

 **Address:** 1670 Keller Parkway, Suite 130, Keller, TX 76248-3769  **Phone:** 817-337-0300

 **Email:** sales@fulcrumgroup.net  **Website:** <https://www.FulcrumGroup.net>