THIN LINE SOFTWARE
CJIS AUDIT READINESS

Preparing for a CJIS audit shouldn't start when the auditor calls.

Originally published: September 2026 · Last reviewed: September 2026

If a Texas agency were asked to demonstrate its CJIS security practices today, could it produce the people, policies, records, and evidence that show those responsibilities are actually operating?

If a Texas law-enforcement agency were asked to demonstrate its CJIS security practices today, could it produce the people, policies, configurations, records, and evidence that show those responsibilities are actually being carried out?

> *CJIS readiness is not having a folder of policies. It is being able to demonstrate that the required security practices are actually operating.*

This is a practical readiness guide for smaller Texas agencies. It is not a substitute for the current FBI CJIS Security Policy, the Texas Security Policy Supplement, Texas DPS CJIS guidance, the CJIS Security Addendum, or the instructions from the agency's auditor. Completing this page does not determine CJIS compliance.

Know which policy Texas is auditing

As of September 17, 2026, Texas DPS states that all Texas CJIS audits through March 31, 2027, are conducted against FBI CJIS Security Policy version 5.9.5. Texas agencies also need to account for the Texas Security Policy Supplement and other applicable Texas-specific requirements. Thin Line does not decide which version governs a particular agency's audit.

CJIS Security Policy v6.1 was released June 25, 2026. DPS says agencies should begin gap assessments for that modernized policy. That work belongs on the separate 6.1 guide. This page is about demonstrating the security program Texas is auditing today.

For what changed in v6.1 and how to start a gap assessment, read the Texas CJIS 6.1 Guide.

Use requirement, implementation, and evidence

For each applicable area, ask three questions: What applies? How do we satisfy it? How can we demonstrate that?

- A CJIS or Texas DPS requirement is something supported by the current authoritative policy or guidance.
- Implementation is how the agency actually performs that work.
- Evidence is the record, configuration, log, roster, agreement, or other material that can show the work occurred.

A tracking sheet, folder structure, or matrix on this page is a Thin Line practical recommendation unless a cited source requires that particular artifact. Do not treat a recommended method of documenting compliance as the requirement itself.

Start with the CJIS environment

Before assembling an audit binder, the agency needs to know what it is accounting for. Where does Criminal Justice Information enter the agency? Which systems access, process, transmit, or store it? Which employees or contractors have relevant access? Which workstations, mobile devices, networks, remote-access paths, vendors, and storage locations are involved?

The purpose is scope, not a network-engineering manual. If someone unfamiliar with the agency cannot follow how CJI moves, the later evidence will be hard to explain.

Make responsibilities known

In a small department, several security functions may belong to the same person. That is fine. The problem is when everyone assumes somebody else owns the work.

v5.9.5 requires the designation of a Terminal Agency Coordinator in agencies with devices accessing CJIS systems and a Local Agency Security Officer in each agency with access to CJI. The agency should also know who maintains policies, coordinates with DPS, manages access, reviews logs, handles incidents, and works with vendors. The matrix below is an organizational aid, not a CJIS-mandated form.

Who owns the work

Assign a primary and identify a backup where practical. If no backup exists, make that dependency visible rather than leaving it assumed. Record where the evidence lives.

Responsibility	Primary	Backup	Evidence / location
CJIS / security coordination (LASO, TAC, or applicable role)			
Personnel screening and access			
Security awareness training			
Account and access review			
Incident response			
Media handling and disposal			
System / network documentation			
Vendor and Security Addendum documentation			
Log review			
Policy maintenance			

Distinguish a written policy from an operating practice

Written documentation matters. It is not enough. For each important policy area, the readiness questions are: Do we have the required policy or process? Is it current? Do the people who need it know what to do? Can we show that it is followed?

Texas DPS publishes sample policy templates covering areas such as access control, awareness and training, auditing and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, and personnel security. DPS cautions that templates are starting points that must be customized and formally adopted-not used unchanged. A renamed template does not establish compliance.

Texas DPS sample agreements and policy templates

Show who has access and why

The agency should be able to show who currently has access to CJI or to systems that handle it, why they have it, when it was granted, whether required screening and training are complete, and what happens when someone leaves or changes roles.

Access review is recurring work. A common gap is access that remains after a person no longer needs it.

Do not merely ask whether everyone has taken CJIS training. Ask whether you can produce current completion records. Texas DPS currently provides CJIS policy training resources in areas including incident response, access control, and identification and authentication. A spreadsheet is one practical way to track dates and upcoming retraining; memory is not.

Show how people authenticate

The readiness question is whether the agency can show how applicable users authenticate and how access is controlled-individual accounts, credential requirements, privileged accounts, remote access, and advanced authentication or multi-factor authentication where the current policy and Texas guidance require them.

These rules have changed across CJIS policy versions. Use the current v5.9.5 text and Texas materials. Do not carry forward older "advanced authentication" or password language from an earlier resource without checking the current source.

Know the systems and devices that touch CJI

Include more than the dispatch desktop: RMS, CAD, mobile computers, laptops, servers, file storage, backups, email, printers, removable media, cloud services, remote-access tools, and vendor support paths where they can reach CJI.

A current inventory is a practical way to explain the environment. The columns below are a recommended format, not a CJIS-mandated spreadsheet.

Asset / system	User / location	CJI access?	Protection	Last reviewed	Notes
RMS					
CAD					
Mobile / MDT					

File storage / backup					
Other					

A current diagram helps someone unfamiliar with the environment see where CJI enters, which systems matter, where the security boundary is, what external connections exist, and how remote or mobile access works. No particular notation is required. If the drawing cannot be explained, it is not ready.

For remote and mobile access, the agency should be able to say whether the method is authorized, how the user authenticates, whether CJI is stored locally, how lost-device and revocation procedures work, and whether personally owned devices are permitted. The FBI publishes guidance for personally owned devices that access, process, store, or transmit CJI.

Show how CJI is protected

Where the current policy requires encryption or other protection for data in transit, at rest, on mobile or removable media, in backups, or in cloud storage, the agency should be able to show how that protection is implemented. Do not generalize a requirement beyond its actual scope.

Useful evidence may include configuration, architecture notes, vendor documentation, or device-management settings. Those are examples of how an agency might demonstrate implementation-not automatically required audit artifacts.

Show that logging is more than a file that exists

Distinguish three things: applicable logs exist; someone reviews relevant activity; and the agency can demonstrate that the review occurred.

v5.9.5 AU-6 states that system audit records are to be reviewed and analyzed weekly for indications of inappropriate or unusual activity. Confirm with current Texas DPS audit materials which markings are sanctionable for the agency's review. A dated review record is a practical way to show that the review happened. The policy names the review; it does not name a particular spreadsheet.

Show what happens when something goes wrong

v5.9.5 includes an incident-response plan control. The readiness questions are whether there is a current usable plan, whether responsibilities are assigned, whether relevant staff know how to report an incident, whether DPS and other escalation contacts are current, and whether required testing, exercise, or review has occurred where applicable.

Use the current DPS incident-response instructions rather than an old copy saved locally. A DPS sample plan is a starting template. It does not, by itself, satisfy the requirement.

Texas DPS sample incident-response and related policy templates

Media, continuity, and physical security

The current policy addresses protection of electronic and physical media containing CJI, including storage, transport, sanitization, and destruction. The agency should be able to show how printed CJI, discarded paper, old drives, and retired devices are handled-not only that a media policy exists.

If a CJI system becomes unavailable, who is responsible, where is the recovery or continuity information kept, and is it current enough to use? Do not turn this page into a disaster-recovery manual. Confirm applicable continuity requirements against the current policy and DPS materials.

Walk the building as though seeing it for the first time. Can visitors reach screens displaying CJI? Are workstations left unlocked? Who can enter areas with systems or media that contain CJI? How are visitors handled? Physical security belongs in the demonstration, but this page does not reproduce the full physical-protection section of the policy.

Keep vendor responsibility visible

CJIS security is shared work. Buying a product, outsourcing IT, or hearing that a vendor is "CJIS compliant" does not transfer the agency's responsibilities to the vendor.

The agency should know which third parties can access, process, store, transmit, administer, or otherwise affect CJI-managed IT, cloud, backup, network contractors, repair shops, dispatch arrangements, integrations, and the RMS or CAD vendor. Texas DPS says the CJIS Security Addendum is required for contractors and vendors with access to CJI, and that contractor employees with such access must sign it before access is granted.

For each relevant vendor, know the service, the applicable agreements, where information is stored, how access is controlled, how incidents are reported to the agency, and what happens when the relationship ends.

Create evidence as the work happens

The easiest audit evidence is evidence created by the normal security process. Do not reconstruct a year of activity the week before a review.

Examples of useful evidence include training records, access lists and reviews, screening documentation, diagrams, inventories, configuration reports, policy approval or review records, incident-response exercises, log-review records, vendor and addendum files, media-destruction records, and vulnerability or patch evidence where applicable. Not every example applies to every agency.

If the agency has been audited before, start with prior findings. A corrective action that quietly stopped happening is still a gap.

One practical way to store the material is a single current folder. The names below are a recommended organization, not a required filing system:

```
01 - Agency & CJIS Contacts
02 - Policies
03 - Personnel & Screening
04 - Training
05 - Access & Account Reviews
06 - System & Device Inventory
07 - Physical Security
08 - Vendors & CJIS Addenda
09 - Incident Response
10 - Audit & Security Logs
11 - Media & Disposal
12 - Network & System Documentation
13 - Prior Audit Findings
14 - Remediation Evidence
```

> *If an auditor asked us to show this today, could we produce it-or would we start searching?*

A practical evidence map

This is a readiness worksheet, not an official CJIS form. Use it to find gaps: what applies, how the agency implements it, what evidence exists, who owns it, and what is missing.

Area	Requirement / source	Agency implementation	Evidence	Owner	Last reviewed	Gap
Scope / environment						
Roles and responsibility						
Personnel and screening						
Training						
Accounts and access						
Authentication						
Devices and inventory						
Network / diagram						
Encryption / data protection						
Logging and review						
Incident response						
Media protection						
Vendors / addenda						
Continuity						
Physical security						
Prior findings						

CJIS readiness checklist

Verify that the item can be produced or demonstrated. This checklist does not determine compliance. Items that organize work rather than restate a named requirement are practical readiness recommendations.

Scope and responsibility

- ☐ Current description of where CJI enters and which systems handle it can be produced
- ☐ LASO, TAC, and other applicable CJIS roles are identified
- ☐ Staff know who to contact with a CJIS or security question
- ☐ Primary owners are named; a backup is named where practical, or the single-person dependency is visible

Policies, people, and access

- [ ] Required policies can be produced and show agency-specific procedures
- [ ] Required policy reviews or approvals can be produced where applicable
- [ ] Current authorized-user list has been compared with active accounts
- [ ] Required personnel screening documentation can be produced
- [ ] Current security-awareness training records can be produced
- [ ] Former users and role changes have been removed or adjusted
- [ ] How applicable users authenticate can be demonstrated

Systems, network, and protection

- [ ] Current inventory of systems and devices that handle CJI can be produced
- [ ] Current network or system diagram can be produced and explained
- [ ] Remote and mobile access methods can be explained
- [ ] Applicable encryption or data-protection implementation can be shown
- [ ] Applicable logs can be produced
- [ ] Evidence that required log review occurred can be produced

Incidents, media, vendors, and the building

- [ ] Current incident-response plan can be produced
- [ ] Staff reporting and DPS/escalation contacts are current
- [ ] Incident-response testing, exercise, or review can be shown where applicable
- [ ] Media storage, transport, and destruction procedures can be demonstrated
- [ ] Vendors that can affect CJI are identified
- [ ] Required Security Addenda and vendor agreements can be produced
- [ ] Continuity or recovery information can be produced if a CJI system is unavailable
- [ ] Physical control of relevant areas, visitors, and displayed or printed CJI can be explained
- [ ] Prior findings and remediation evidence can be produced

An audit drill

These are practical readiness exercises, not a representation of the exact questions a CJIS auditor will ask. Pick several items and have someone who did not assemble the folder ask:

- What applies?
- Who owns it?
- How do we implement it?
- Show me the evidence.
- Show me who has access.
- Show me their required training.

- Show me the network path.
- Show me what happens when someone leaves.
- Show me how a security incident gets reported.
- Show me evidence that a recurring security process actually occurred.

Every time the answer begins with "I think that's in...", write it down. That is the gap to close before a real review.

Demonstrate the program you already operate

> *Do we know how CJI is protected? Are we doing the work? Can we show it?*

If those three answers are yes, a review is less about assembling paperwork and more about showing the security program the agency already runs.

Official Texas and FBI resources

Current FBI and Texas DPS publications control. DPS currently provides the policy versions, Texas supplement, audit material, incident-response resources, Security Addendum, companion spreadsheets, and sample policy templates. Future v6.1 gap assessment is covered in the Texas CJIS 6.1 Guide.

Texas DPS CJIS Policy Components & Documents

Texas DPS CJIS Security Office

Texas DPS sample agreements and policy templates

Texas DPS CJIS training resources

FBI CJIS Security Policy Resource Center

For v6.1 gap assessment and future readiness, read the Texas CJIS 6.1 Guide.

Generated from the Thin Line Software resource library. Read this guide online: https://thinline.software/resources/texas-cjis-audit-readiness-checklist