THIN LINE SOFTWARE
TEXAS CJIS 6.1 GUIDE

What changed in CJIS Security Policy 6.1, and what Texas agencies need to know.

Originally published: August 2026 · Last reviewed: September 2026

What Texas is auditing today under v5.9.5, why v6.1 matters now, and a readiness checklist covering people, access, vendors, cloud, policies, incident response, technical security, recovery, and evidence.

If your Texas law-enforcement agency is preparing for a CJIS audit, you may be hearing about policy versions 5.9.5, 6.0, and 6.1. Texas agencies currently need to pay attention to two versions for two different reasons.

What applies today is the standard Texas DPS is auditing. What you should prepare for is the modernized policy already released for gap assessment. What to do next is keep current audit evidence in order while you identify where v6.1 will require different people, policies, systems, vendors, or procedures.

The short version

CJIS Security Policy v5.9.5 is still the Texas audit standard. Texas DPS states that Texas CJIS audits through March 31, 2027, will be conducted against v5.9.5.

CJIS Security Policy v6.1 is the preparation standard. Released June 25, 2026, it should be used now for gap assessments and future readiness.

> **Texas audit timing**
> Through March 31, 2027, Texas DPS continues auditing against CJIS Security Policy v5.9.5. Use CJIS Security Policy v6.1 now for gap assessment and future readiness.

> *5.9.5 = what Texas is auditing today*
> *6.1 = what your agency should be preparing for*

Preparing for the current Texas audit standard? Use the Texas CJIS Audit Readiness Checklist.

Why CJIS 6.1 is different

Version 6.1 is not a routine wording update. The modernized policy is organized around security controls aligned more closely with NIST SP 800-53 Rev. 5.

That change shows up as control families covering a wide operating surface: access control, training, audit, configuration, contingency planning, authentication, incident response, personnel, physical protection, risk, acquisition, communications protection, and system integrity. The point is not to memorize the family names. The point is that the modernized policy reaches people, systems, vendors, and recovery-not only the login screen.

The practical question for a Texas agency is whether your people, policies, systems, vendors, and procedures satisfy the controls that will eventually apply to your agency. A v6.1 gap assessment should answer that question.

Understand Existing, Priority 1, and zero-cycle controls

The v6.1 Requirements Companion identifies requirements carried forward from earlier policy as Existing and phases in modernized controls through priority and sanction designations. Priority 1 controls are treated as immediately sanctionable in the FBI implementation framework; other modernized controls may be in zero-cycle.

Texas agencies should not assume that an FBI designation alone determines how a Texas audit will be conducted. DPS currently says v5.9.5 remains the Texas audit policy through March 31, 2027. Use v6.1 priorities to plan gap work and confirm audit expectations with the Texas CJIS Security Office.

Know who can reach CJI

The first transition question is about people and access. Who has access? How are they authenticated? What can they do? Why do they need it? Are they trained? What happens when their role changes? When does access disappear? Identity, authentication, permissions, training, and personnel processes are related controls, not separate administrative exercises.

Multi-factor authentication

MFA is one of the most visible modernized areas. Review both privileged and non-privileged access, and do not limit the inventory to office desktops. The work is to identify every path through which users can reach CJI and show how each path is authenticated.

- RMS and CAD
- mobile computers
- administrative access
- remote access
- VPN
- cloud-hosted applications
- web applications
- connected systems
- vendor support paths
- elevated accounts

> **Question to ask**
> Can we identify every path through which users can access CJI and demonstrate how each is authenticated?

Manage the entire account lifecycle

Agencies should be able to identify authorized users, roles, group membership, privileges, and other access attributes-and show how that picture changes over time. Access is a lifecycle: creation, approval, role assignment, privileges, periodic review, responsibility change, separation, and revocation. If asked today, how quickly could you produce a current list of everyone with CJI access and what each person can do?

Users should receive only the access required for their responsibilities. Administrative activity should be separated from ordinary work where practical. Look especially at role and group membership, privileged and administrator accounts, shared credentials, vendor administrative access, application roles, database access, and the ability to change security settings.

> **Question to ask**
> Are we granting access because the job requires it, or because the user has always had it?

Connect personnel security and training to access

Personnel security and training belong in the same lifecycle as the account. Before access: screening, authorization, and initial training. During service: recurring and role-specific training, including contractor training where applicable, and training after major policy or system changes, with completion evidence. After a transfer, responsibility change, or separation: credential revocation and recovery of devices and tokens. Can you show that the people who can reach CJI understand the policy they must follow?

> **Question to ask**
> When someone leaves at 5:00 p.m., when does their access actually disappear?

Know who shares responsibility outside the agency

Modern public-safety systems rarely exist entirely inside the police department. An agency may rely on RMS and CAD vendors, cloud and backup providers, managed IT, outside technicians, dispatch providers, consultants, and remote-support personnel. Those relationships create security responsibilities that need to be identified explicitly. Using a provider does not make the agency's security responsibility disappear.

Vendors and contractors

Third-party access deserves special attention. Contractors with CJI access may require the CJIS Security Addendum, screening, and other agreements. The first job is to know who those parties are-not only the primary software vendor.

- CAD and RMS vendors
- cloud and backup providers
- managed IT and outside technicians
- dispatch providers and consultants
- remote-support personnel

> **Question to ask**
> Do we know every third party that can potentially touch CJI, why access is necessary, and how access is removed?

Cloud services and shared responsibility

The Requirements Companion includes a cloud responsibility matrix for IaaS, PaaS, and SaaS. Those labels matter only enough to understand who owns which duty. Responsibilities may sit with the agency, the provider, CJIS, or multiple parties, but the agency remains accountable for its environment.

For each hosted service, classify the service, document agency, provider, and shared duties, obtain evidence for provider responsibilities, and define who owns access, logging, incidents, and data return when the contract ends.

> **Question to ask**
> Do contracts and procedures clearly establish who owns each security requirement?

Turn security requirements into operating practice

A security requirement becomes meaningful only when the agency can connect it to a policy, a procedure, a responsible person, a system or process, and evidence. The gap-assessment work is finding where that chain is missing.

Policies and procedures

Modernized CJIS emphasizes documented policies and procedures. DPS templates are useful starting points, not finished agency policies. Compare the policy set against applicable v6.1 control families, customize templates to actual operations, adopt them through the agency process, set review and update triggers, and retain evidence that procedures are followed.

> **Question to ask**
> Do our written policies describe what we actually do, and can we demonstrate it?

Incident response

Texas DPS guidance instructs agencies to report a confirmed security incident within one hour of discovery, notify the LASO, TAC, or OPSR, preserve evidence, and contact DPS ETOC for TLETS or CJIS incidents. The plan has to be usable under pressure: who identifies and escalates, who contacts DPS and vendors, who has evidence-preservation and isolation authority, how the process is documented and tested, and what after-hours contact looks like.

- Current DPS ETOC numbers: 512-424-2139 and 1-888-377-6420
- Current vendor and after-hours contacts
- Assigned evidence-preservation and isolation authority

> **Question to ask**
> If an incident were found at 2:00 a.m., would the person on duty know exactly what to do?

Audit logging and accountability

Agencies need records that allow them to determine what occurred, by whom, and when. That means knowing what is logged, how logs are protected and retained, who reviews them, how alerts are handled, and whether vendor and agency records can be correlated. Logging is useful only if the agency can use the resulting evidence to understand what occurred.

> **Question to ask**
> Could we investigate questionable access from three months ago?

Configuration, vulnerability, and system security

In a smaller agency, the person implementing a control may be city IT, a managed-service provider, a software vendor, or another provider. The agency therefore needs to know both who implements the control and what evidence exists. Review secure configuration, patching, vulnerability management, malware protection, network and endpoint controls, encryption, remote access, production changes, unsupported systems, and security monitoring.

> **Question to ask**
> Can the responsible provider explain how each applicable control is implemented and prove it?

Make ownership explicit

CJIS security is not solely an IT responsibility. Operational, technical, and administrative roles must be named and understood-typically the TAC, LASO or OPSR, agency leadership, IT personnel, and contract or vendor administrators.

> **Question to ask**
> Does everyone involved know which CJIS responsibilities belong to them?

Protect CJI beyond normal operations

Security planning cannot stop at the application login screen. CJI can exist physically. Devices can disappear. Systems can fail. Providers can have outages. Backups can fail to restore.

Physical and media protection

CJIS security covers locations, devices, printed information, and removable media as well as servers. Walk the places CJI can physically exist: secure areas, workstations, mobile computers, removable media, printed CJI, storage, transport, disposal, repair, and lost equipment.

> **Question to ask**
> Where can CJI physically exist outside the server room?

Contingency planning and recovery

Cyber incidents, hardware failure, disaster, and provider outages can interrupt operations. Protected backups are not the same thing as demonstrated recovery. The agency also needs disaster-recovery and continuity procedures, vendor recovery responsibilities, alternate operating procedures, and emergency contacts.

> **Question to ask**
> Have we demonstrated that our backups can actually be restored?

Do not wait until the audit to find gaps

Continue maintaining the requirements Texas DPS currently audits under v5.9.5. At the same time, compare your people, systems, vendors, policies, and procedures against v6.1 so the transition does not become an emergency later.

The checklist below is the gap-assessment worksheet. The article explained how the controls relate. The worksheet is where the review becomes specific.

Texas CJIS 6.1 Readiness Checklist

A practical gap-assessment worksheet for TAC, LASO, OPSR, leadership, and IT. Use it to organize your review. It does not replace the official policy, the Requirements Companion, or guidance from the Texas CJIS Security Office.

> **A worksheet, not a score**
> This checklist helps an agency organize a v6.1 gap assessment. It does not store answers, assign a pass/fail rating, or determine CJIS compliance.

Work through each area. Unchecked items are starting points, not findings.

People

- [ ] Confirm TAC and applicable security-responsibility designations.
- [ ] Identify backups for critical security responsibilities.
- [ ] Verify personnel and contractor screening procedures.
- [ ] Review security training records.
- [ ] Establish prompt access removal when personnel leave or change roles.

What to have ready

Role designations, backup assignments, screening records, training reports, and termination procedures.

Accounts and access

- [ ] Inventory every system that processes, stores, or transmits CJI.
- [ ] Inventory every user with access to those systems.
- [ ] Separately identify privileged and administrator accounts.
- [ ] Review roles and permissions for least privilege.

- [ ] Identify shared or generic accounts.
- [ ] Document account creation, modification, review, and termination.
- [ ] Review MFA for privileged and non-privileged CJI access paths.

What to have ready

System inventory, user and role exports, approval records, MFA settings, access-review results, and termination evidence.

Vendors and contractors

- [ ] Inventory vendors with direct or indirect CJI access.
- [ ] Verify applicable CJIS Security Addenda.
- [ ] Verify required contractor screening.
- [ ] Review applicable Management Control Agreements and contracts.
- [ ] Document vendor remote-support access.
- [ ] Define how vendor access is granted, reviewed, and removed.
- [ ] Confirm vendor incident-notification responsibilities.

What to have ready

Vendor list, signed Security Addenda, applicable MCAs, screening records, contracts, and remote-access records.

Cloud systems

- [ ] Inventory cloud systems processing, storing, or transmitting CJI.
- [ ] Classify SaaS, PaaS, and IaaS where applicable.
- [ ] Document agency, provider, and shared responsibilities.
- [ ] Determine what security evidence the provider can supply.
- [ ] Document logging, incident response, data return, and contract-end procedures.

What to have ready

Cloud inventory, responsibility matrix, contracts, security reports, incident terms, and data-return provisions.

Policies and procedures

- [ ] Compare agency policies against v6.1 control families.
- [ ] Identify missing or outdated policies.
- [ ] Make written policy match actual practice.
- [ ] Document procedures that implement each policy.
- [ ] Establish approval, review, and update triggers.

What to have ready

Approved policies, procedures, revision history, ownership assignments, and evidence of implementation.

Incident response

- [ ] Verify the incident-response plan.
- [ ] Verify LASO, TAC, OPSR, vendor, and DPS contact information.
- [ ] Address the Texas one-hour reporting guidance.
- [ ] Establish after-hours escalation procedures.
- [ ] Assign evidence-preservation and system-isolation authority.
- [ ] Verify current DPS ETOC numbers and instructions.
- [ ] Test and document the response process.

What to have ready

Incident plan, call tree, ETOC contact details, reporting forms, exercise results, and after-action records.

Technical security

- [ ] Review patch and vulnerability management.
- [ ] Review endpoint and malware protection.
- [ ] Review encryption and network protection.
- [ ] Review remote and administrative access.
- [ ] Review audit logging, retention, and monitoring.
- [ ] Identify unsupported systems and software.
- [ ] Document configuration and production-change controls.

What to have ready

Patch and vulnerability reports, configuration baselines, encryption evidence, log settings, access records, and remediation plans.

Physical and media protection

- [ ] Identify all locations where CJI can exist.
- [ ] Review secure-area and workstation controls.
- [ ] Review mobile computers and removable media.
- [ ] Review printed CJI storage, transport, and disposal.
- [ ] Document lost, stolen, repair, and disposal procedures.

What to have ready

Facility procedures, device and media inventories, access records, disposal certificates, and incident procedures.

Recovery and continuity

- [ ] Verify protected backups.
- [ ] Test restoration and retain results.
- [ ] Document disaster-recovery and continuity procedures.
- [ ] Understand vendor recovery responsibilities.
- [ ] Maintain alternate operating procedures and emergency contacts.

What to have ready

Backup reports, restoration-test evidence, recovery plans, vendor commitments, and emergency contacts.

Documentation and evidence

- [ ] Maintain current network and system documentation.
- [ ] Maintain current access and training records.
- [ ] Maintain contractor screening, agreements, and Addenda.
- [ ] Maintain policy approvals, review records, and exceptions.
- [ ] Maintain incident and exercise records.
- [ ] Collect evidence instead of relying on verbal assurances.

What to have ready

A dated evidence folder organized by control area, with an owner and review date for each item.

Review notes

Use these prompts to turn the worksheet into a plan. This worksheet does not store answers.

> **Highest-priority gaps**
> Which gaps matter most for your agency, and why?

> **Assigned owners**
> Who owns each priority gap?

> **Target dates**
> When should each priority gap be addressed?

> **Questions for the Texas CJIS Security Office**
> What do you need to confirm with the Texas CJIS Security Office before you proceed?

Official resources

Current Texas audit preparation is covered in the Texas CJIS Audit Readiness Checklist.

Texas DPS CJIS Policy Components and Documents

Texas CJIS Security Office

Texas DPS CJIS Security Policy Training

FBI CJIS Security Policy Resource Center

Preparing for the current Texas audit standard? Use the Texas CJIS Audit Readiness Checklist.

> **Important notice**
>
> This guide is provided by Thin Line Software for general informational purposes. It is not legal advice, an official interpretation of the FBI CJIS Security Policy, or a determination of CJIS compliance. Requirements vary by system, access method, relationship, and operating environment. Agencies should verify decisions against current FBI and Texas DPS publications and consult the Texas CJIS Security Office and appropriate legal or technical advisors.