THIN LINE SOFTWARE
READINESS CHECKLIST

Texas CJIS 6.1 Readiness Checklist

Originally published: August 2026 · Last reviewed: September 2026

Printable take-away from What changed in CJIS Security Policy 6.1, and what Texas agencies need to know.

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.