Legislative Requirement:

The Criminal Justice Information System

- DPS had adequate processes and controls to help ensure that most criminal history information is complete, accurate, and reported within required timeframes.
- TDCJ had processes and controls to help ensure that most custody data and probation data were accurate and supported.

Lisa R. Collier, CPA, CFE, CIDA
State Auditor

The Department of Public Safety (DPS) and the Texas Department of Criminal Justice (TDCJ) had processes and controls to help ensure that most criminal history information in the Criminal Justice Information System is accurate, complete, and reported within required timeframes.

However, DPS should improve its process to resolve prosecution and court records that are not matched to an arrest record in the Computerized Criminal History (CCH) System.

In addition, TDCJ should enhance its oversight of incomplete probation data to ensure that missing data is obtained and added to the Intermediate System (ISYS).

- *Audit Objective* | p. 11

This audit was conducted in accordance with Texas Code of Criminal Procedure, Article 66.352, which requires the State Auditor's Office to examine the records and operations of the criminal justice information system every five years.

MEDIUM

DPS CRIMINAL HISTORY DATA

Most of the data in CCH was complete, accurate, and reported within required timeframes. However, DPS should improve its efforts to resolve unmatched prosecution and court disposition records.

Chapter 1 | p. 4

LOW

TDCJ CUSTODY DATA

TDCJ's custody data was mostly accurate and supported. However, it should ensure that programming changes to the State Ready System are tested.

Chapter 2-A| p. 7

LOW

TDCJ PROBATION DATA

TDCJ had effective controls to ensure that offender probation data in ISYS was complete, accurate, and reported within required timeframes.

Chapter 2-B | p. 9

For more information about this audit, contact Audit Manager Kelley Ngaide or State Auditor Lisa Collier at 512-936-9500.

April 2026 | Report No. **26-021**

Note on Confidential Findings

To minimize security risks, auditors communicated details about an audit finding related to a certain security weakness to DPS in a separate report.

MEDIUM

The finding presented in that report is rated Medium because the issue identified presents risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Government Auditing Standards*, certain information was omitted from this report because that information was deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. Under the provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Summary of Management's Response

Auditors made recommendations to address the issues identified during this audit, provided at the end of each chapter in this report. DPS and TDCJ management agreed with the recommendations in this report.

Ratings Definitions

Auditors used professional judgment and rated the audit findings identified in this report. The issue ratings identified for each chapter were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

PRIORITY: Issues identified present risks or effects that if not addressed could ***critically affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

HIGH: Issues identified present risks or effects that if not addressed could ***substantially affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.

MEDIUM: Issues identified present risks or effects that if not addressed could ***moderately affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

LOW: The audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks ***or*** effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

For more on the methodology for issue ratings, see Report Ratings in Appendix 1.

MEDIUM

Chapter 1
DPS Criminal History Data

The Department of Public Safety (DPS) had adequate processes for validating the arrest, prosecution, and court disposition data in its Computerized Criminal History (CCH) system. (See text box for more information on CCH.) For example, if prosecution or court disposition records did not have a matching arrest record in CCH, they were maintained in a separate file until corrected.

However, DPS should work with local entities to resolve and correct unmatched records to help ensure the completeness of criminal history data in CCH.

The Computerized Criminal History (CCH) System

DPS maintains the CCH system that contains arrest, prosecution, and court disposition data. That data is reported by local law enforcement agencies, prosecutor offices, and courts (local entities).

The information in the CCH system is used by various entities for background checks to help determine eligibility for employment, adoption, housing, licensing, and firearm purchases.

Sources: Texas Government Code, Chapter 411; and DPS.

Criminal history data added to CCH was accurate, complete, and reported within required timeframes.

DPS had effective controls to ensure that arrest, prosecution, and court disposition data added to the CCH system was complete and accurate. Specifically, DPS implemented automated controls for criminal history data, evaluated access requests for compliance, validated records submitted by the Federal Bureau of Investigation, appropriately managed user access, and maintained effective backup and recovery processes.

In addition, DPS had an adequate process for updating criminal history information when requested by local entities and monitored whether local entities reported criminal history records within required timeframes. Specifically, for all criminal history information received from September 2024 through August 2025:

- 91 percent of arrest records were reported within the required 7 days.
- 86 percent of prosecution records were reported within the required 30 days.

- 80 percent of court disposition records were reported within the required 35 days.

DPS should improve its efforts to correct unmatched records to ensure CCH is complete.

The majority of criminal history information in the CCH system was complete because DPS had a process to validate that prosecution and court disposition records were matched to an arrest record before being processed into the system. However, 79 percent of the approximately 700,000 unmatched records as of October 2025 were over 10 years old. These records should be researched, corrected, and removed from the unmatched file to ensure that criminal history data is up to date and complete, as required by Texas Code of Criminal Procedure 66.106(c). It is important that criminal history data is accurate and complete because it is used for decisions such as firearm purchases and employment screening.

DPS had a process to share unmatched records with local entities for correction. However, DPS should improve processes to ensure that the number of unmatched records does not continue to grow and become unmanageable.

Recommendation

DPS should continue to work with local entities to research, correct, and remove criminal history records from the unmatched file.

Management's Response

> DPS concurs with the recommendation regarding records within the Non-Fingerprint Supported File of the Computerized Criminal History (CCH) system. While most of the CCH data is complete and accurate, DPS is committed to addressing the volume of records in the Non-Fingerprint Supported File.

Currently, the Non-Fingerprint Supported File holds about 700,000 records (2% of all dispositions), with 79% dating back more than 10 years. Created under House Bill 776 (2001), the file segregates records that lack the fingerprint data required for arrest matching. This separation is vital for maintaining the accuracy of the state's criminal history records and ensuring that the public can trust the fingerprint-backed integrity of the primary CCH system.

To improve data integrity and further reduce the submission of unmatched dispositions in the Non-Fingerprint Supported File, DPS is modernizing the entire CCH system to enhance accessibility, reporting, and automated matching efficiency as appropriate. In the interim, DPS will continue collaborative outreach through coordination with law enforcement agencies, prosecutorial offices, and courts to resolve outstanding unmatched submitted records. DPS will continue to focus on record matching efforts by prioritizing the small percentage (less than 0.5% of all dispositions) of unmatched records that are less than 10 years old. This ceaseless pursuit to address unmatched records demonstrates an active management dedicated to mitigating file growth in alignment with recent legislative actions and executive orders, which demand that submitting agencies comply with defined timeliness and completeness requirements.

DPS will continue transferring records from the Non-Fingerprint Supported File to the CCH system immediately upon receipt of arrest information, per Texas Code of Criminal Procedure, Article 66.106(c).

These initiatives will ensure criminal history data remains accurate for critical operational decision-making by law enforcement and criminal justice agencies.

Title of Responsible Person: Chief, Crime Records Division

Estimated Completion Date: December 31, 2026

LOW

Chapter 2-A
TDCJ Custody Data

Overall, the Texas Department of Criminal Justice (TDCJ) had processes to help ensure that custody data in the State Ready System (SRS) for offenders held in state prisons was complete, accurate, and reported in a timely manner. (See text box for more information on TDCJ's systems.)

In addition, TDCJ had effective review processes to identify and correct data entry errors prior to an offender's release. Those processes were completed for 98 percent of the 65 released offenders tested.

TDCJ Systems and the State Ready System (SRS)

TDCJ maintains the Corrections Tracking System, which includes SRS and other component systems.

SRS contains custody records for offenders convicted and secured in a state prison. Custody data includes sentencing dates, jail credits, and offense codes.

Sources: Texas Code of Criminal Procedure, Articles 66.151-152; and TDCJ.

TDCJ had adequate IT controls for SRS but should ensure that programming changes are tested.

TDCJ had effective IT controls in SRS over user access and automated processes. In addition, TDCJ had adequate backup and recovery controls in place to protect custody data from loss.

While TDCJ had change management controls, it did not have evidence that testing was performed as required for 4 (40 percent) of 10 SRS programming changes tested. TDCJ asserted that it tested these changes but could not provide documentation. Testing system changes helps promote the accuracy and completeness of custody data.

Recommendation

TDCJ should test system changes in SRS in accordance with TDCJ policy.

Management's Response

The Texas Department of Criminal Justice agrees with the recommendation and will follow its documented procedures for fully testing changes to SRS.

Title of Person Responsible: Information Technology Division Director

Implementation Date: Ongoing

LOW

Chapter 2-B
TDCJ Probation Data

TDCJ had effective controls for probation data.

TDCJ had effective controls to ensure that offender probation data in the Intermediate System (ISYS) was complete, accurate, and reported within required timeframes. (See text box for more information on ISYS.) Specifically, TDCJ:

- Monitored the timeliness of probation data submitted by local probation departments.
- Corrected probation data and made requested changes within the required timeframe for a sample of requests tested.
- Implemented automated controls for key data elements to help ensure that probation records were reliable.
- Implemented user access controls for internal users and local probation department users and had change management controls for ISYS.

Intermediate System (ISYS)

ISYS contains community supervision (probation) records. Probation records include the jurisdiction, probation start and end dates, applicable programs, and related information.

Sources: Texas Code of Criminal Procedure, Article 66.152; and TDCJ.

TDCJ should take additional steps to resolve rejected probation records excluded from ISYS.

An Audit Report on the Criminal Justice Information System (State Auditor's Office Report No. 22-017, January 2022) previously recommended that TDCJ work with probation departments to update missing information. TDCJ implemented that recommendation by establishing a monthly process to monitor missing data, such as the state identification number and incident number. That process helped to ensure that more than 98 percent of the probation records submitted in ISYS between January 2024 and August 2025 contained the required key data.

Of the 71,000 rejected records that still require resolution, 80 percent were over 10 years old. Because DPS is the agency responsible for creating state identification numbers and incident numbers, TDCJ should coordinate with DPS to periodically analyze rejected records and obtain the missing information that local probation departments could not originally provide.

Recommendation

TDCJ should coordinate with DPS to resolve rejected ISYS records.

Management's Response

> The Texas Department of Criminal Justice agrees with the recommendation. The Community Justice Assistance Division (CJAD) will coordinate with the Department of Public Safety (DPS) to analyze rejected Intermediate System (ISYS) records that cannot be resolved by the local Community Supervision and Corrections Departments (CSCD).
>
> **Title of Person Responsible:** CJAD Director
>
> **Implementation Date:** March 2026

Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether controls over the Criminal Justice Information System (CJIS) help ensure that data in the system is complete, accurate, and up to date.

Scope

The scope of this audit for the Department of Public Safety (DPS) covered processes performed between September 1, 2024, and August 31, 2025, related to the DPS-managed component of CJIS for arrest, prosecution, and court disposition records in the Computerized Criminal History (CCH) system.

Additionally, the audit covered processes for the Texas Department of Criminal Justice (TDCJ) performed between January 1, 2024, through August 31, 2025, related to TDCJ-managed components of CJIS for offender custody records in the State Ready System (SRS) and probation records in the Intermediate System (ISYS).

The scope also included a review of significant internal controls related to those records at DPS and TDCJ.

The following members of the State Auditor's staff performed the audit:

- Thomas Andrew Mahoney, CFE, CGAP (Project Manager)
- Allison Fries, CFE (Assistant Project Manager)
- Alyssa Alvarado
- Becki Franklin, CISA, CFE, CGAP, CICA
- Kristyn Dempster, CFE
- Kevin Mack, CFE
- Sarai Rivas
- Quang Tran, CFE
- Dana Musgrave, MBA, CFE (Quality Control Reviewer)
- Kelley Ngaide, CIA, CFE (Audit Manager)

Methodology

We conducted this performance audit from July 2025 through April 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. In addition, during the audit, matters not required to be reported in accordance with *Government Auditing Standards* were communicated to DPS and TDCJ management separately for consideration.

Addressing the Audit Objective

During the audit, we performed the following:

- Interviewed staff at DPS and TDCJ to gain an understanding of the controls over CJIS data, including processes to support data in the Computerized Criminal History (CCH) system, State Ready System (SRS), and Intermediate System (ISYS).
- Identified the relevant criteria:
  - Texas Code of Criminal Procedure, Chapters 42 and 66.
  - CCH system specifications, including the *CCH Data Dictionary*, version 1.7, and reporting code appendices.
  - DPS and TDCJ policies and procedures effective during the scope of the audit.
  - The Department of Information Resources' *Security Control Standards Catalog*, version 2.2.

DPS

  - Tested a sample of arrest, prosecution, and court disposition data entered in CCH by DPS for accuracy.
  - Tested a sample of CCH data inquiries requested by the Federal Bureau of Investigation (FBI).

- Performed data analysis of DPS's unmatched prosecution and court records to determine the completeness of the CCH system and the effectiveness of DPS's monitoring process.
- Performed data analysis to determine the timeliness of arrest, prosecution, and court disposition records reported to DPS.
- Reviewed edit checks for key fields in the CCH system to determine whether application controls ensured that data was reliable.
- Tested a sample of change management requests for the CCH system to determine whether changes were properly managed.
- Reviewed user access to determine appropriateness of access to the CCH system and the network for administrative users.
- Reviewed a sample of DPS's assessments of Texas Law Enforcement Telecommunications System (TLETS) access requests from local entities.
- Reviewed DPS's penetration test results to determine whether vulnerabilities were assessed.
- Reviewed DPS's backup and recovery process to ensure that data could be restored.

Figure 1 provides details about the populations and samples at DPS selected for testing.

Figure 1

DPS Populations and Samples Selected

Population	Population Size	Sample Size	Sample Methodology
CCH corrections entered by DPS [a]	141,704	25	Selected a stratified random sample of 25 corrections by type (arrest, prosecution, and court records) and total records using random selections within each record type to ensure coverage of the record types.
FBI inquiries related to CCH data [a]	11,936,096	60	Selected a stratified random sample of 60 inquiries, stratifying transactions by the 15 error types and the number of transactions using random selections from each record type to ensure that all types of inquiries were covered.
TLETS access assessments [b]	29	3	Selected a random sample of 3 assessments to obtain coverage of the population.

Population	Population Size	Sample Size	Sample Methodology

[a] The sample was not representative of the population because it was selected by strata; therefore, it would not be appropriate to project test results to the population.

[b] The sample was representative of the population; therefore, test results may be projected to the population, but the accuracy of the projection cannot be measured.

TDCJ

- Tested a sample of offenders that went through TDCJ intake during the scope to determine whether key information in SRS was accurate and entered within required timeframes.
- Tested a sample of offenders released from TDCJ custody during the scope to determine whether date records were supported and accurate in SRS, TDCJ's audit release checklist was completed, and the release date was correctly calculated.
- Reviewed the process to update National Crime Information Center codes in SRS to determine whether criminal codes were updated and approved.
- Tested a sample of ISYS data correction requests from local probation departments to determine whether they were processed accurately and within required timeframes.
- Performed data analysis on the timeliness of submission of probation data to ISYS to determine whether local probation departments were reporting within required timeframes.
- Tested a sample of ISYS monthly rejected probation files to determine whether TDCJ was monitoring that local probation departments were making corrections within required timeframes.
- Tested a sample of quarterly ISYS user access reviews for external users to determine whether TDCJ managed external access to ISYS appropriately.
- Reviewed all SRS change management requests and reviewed a sample of change management requests for the TDCJ mainframe and ISYS to determine whether changes were properly managed.
- Reviewed user access to SRS, ISYS, and network administrative users to determine appropriateness of user access.

- Reviewed edit checks for key fields in SRS and ISYS to determine whether application controls ensured that data was reliable.
- Reviewed TDCJ's penetration test results to determine whether vulnerabilities were assessed.
- Reviewed TDCJ's backup and recovery process to ensure that data could be restored.

Figure 2 provides details about the populations and samples at TDCJ selected for testing.

Figure 2

TDCJ Populations and Samples Selected

Population	Population Size	Sample Size	Sample Methodology
SRS custody intake records [a]	70,640	66	Selected a sample of 66 intake records: 60 were selected randomly to obtain coverage of the population, and 6 records were targeted based on the risk that data could be inaccurate.
SRS custody release records [a]	64,068	65	Selected a sample of 65 release records: 60 were selected randomly for coverage of the population, and 5 records were targeted based on the risk that data could be inaccurate.
ISYS data correction requests [a]	9,831	30	Selected a sample of 30 corrections requested: 25 were selected randomly to obtain coverage of the population, and 5 records were targeted to review corrections that were rejected and not processed.
ISYS user access reviews (of local probation departments) [b]	122	25	Selected a random sample of 25 local probation departments with ISYS access to obtain coverage of the population. For those 25 departments, selected a random sample of reviews from 3 quarters.
Records from the ISYS monthly rejected files [b]	10,609	25	Selected a random sample of 4 monthly files from the population. From the selected monthly files, selected a random sample totaling 25 records.
TDCJ Mainframe (Micro Focus) changes [b]	401	18	Selected 18 targeted changes that were high-priority requests.

[a] The sample was selected using a combination of random selection and professional judgment, and the report did not identify which items were randomly selected versus risk-based selections. Therefore, it would not be appropriate to project the test results to the population.

[b] The sample was not representative of the population; therefore, it would not be appropriate to project test results to the population.

Data Reliability and Completeness

Auditors determined that the following data sets were sufficiently reliable for the purposes of the audit.

DPS

- **CCH system data sets.** Auditors reviewed query parameters, analyzed key fields for reasonableness, tested user access, and tested application controls to verify that information technology controls were in place for the following:
  - CCH system custody records (including arrest, prosecution, court disposition, and the CCH unmatched records).
  - CCH system corrections entered by DPS.
  - CCH system change management data.
- **CCH system corrections requested by FBI.** Auditors verified that DPS provided the auditors with the original files sent by the FBI and analyzed files to verify all file types were provided.
- **TLETS access assessments.** Auditors compared the list of assessments performed (provided by DPS) to the total number of assessments reported in its monthly audit tracking sheet.

TDCJ

- **SRS and ISYS data sets.** Auditors reviewed query parameters, analyzed key fields for reasonableness and completeness, tested system user access, and tested application controls to verify that information technology controls were in place for the following data sets:
  - SRS custody intake records.
  - SRS custody release records.
  - ISYS transactions.
  - ISYS data correction requests.
- **ISYS monthly rejected files**. Auditors analyzed key fields for reasonableness and completeness, tested system user access, and tested application controls.

- **ISYS user access reviews (of local probation departments).** Auditors compared a list of community supervision and corrections departments provided by TDCJ to the published list on its website.
- **TDCJ's mainframe change management data and ISYS change management data**. Auditors observed the data retrieval and analyzed the data for reasonableness.

Report Ratings

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Auditors also identified and considered other factors when appropriate.

Appendix 2

Related State Auditor's Office Reports

Figure 3

Report Number	Report Name	Release Date
22-017	*An Audit Report on the Criminal Justice Information System*	January 2022
16-025	*An Audit Report on the Criminal Justice Information System at the Department of Public Safety and the Texas Department of Criminal Justice*	May 2016

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair

The Honorable Dustin Burrows, Speaker of the House, Joint Chair

The Honorable Joan Huffman, Senate Finance Committee

The Honorable Robert Nichols, Member, Texas Senate

The Honorable Greg Bonnen, House Appropriations Committee

The Honorable Morgan Meyer, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

Department of Public Safety

Members of the Public Safety Commission

Colonel Freeman F. Martin, Director

Texas Department of Criminal Justice

Members of the Texas Board of Criminal Justice

Mr. Bobby Lumpkin, Executive Director