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

An Audit Report on

The Criminal Justice Information System

January 2022

Report No. 22-017

An Audit Report on

The Criminal Justice Information System

SAO Report No. 22-017
January 2022

Overall Conclusion

The Department of Public Safety (DPS) and the Texas Department of Criminal Justice (TDCJ) have processes and controls in place to help ensure that information in the Criminal Justice Information System (CJIS) is accurate and complete. In addition, the timeliness and completeness of some data has improved since the State Auditor's Office audit of CJIS in May 2016[1]. However, DPS and TDCJ should strengthen certain controls to help ensure compliance with CJIS-related requirements. CJIS consists of DPS's Computerized Criminal History (CCH) system and TDCJ's Corrections Tracking System (CTS) (see text box and Chapter 1 for more information about those systems).

Background Information

Texas Code of Criminal Procedure established the Criminal Justice Information System (CJIS), which is composed of information systems at two state agencies:

- The Department of Public Safety (DPS) maintains the **Computerized Criminal History** system, which is a database containing arrest, disposition, and supervision information.
- The Texas Department of Criminal Justice (TDCJ) maintains the **Corrections Tracking System**, a collection of applications containing information on offenders under community supervision (on probation), in jail or prison, or on parole.

Sources: Texas Code of Criminal Procedure, Chapter 66; DPS; and TDCJ.

Department of Public Safety

Reporting entities submitted most criminal history information to DPS within required timeframes, and compliance with timeliness requirements for reporting final dispositions has increased since May 2016. Courts reported 94 percent of final disposition records within required timeframes (37 days in 2020 and 35 days in 2021), which was a significant improvement from 69 percent in 2016, when final dispositions were required to be reported within 30 days.

DPS had processes and controls in place to help ensure the accuracy and completeness of information in CCH; however, certain processes and controls should be strengthened. For example, DPS should implement automated controls to help ensure compliance with requirements to report the age of the victim for certain offenses and to identify offenses that involved family violence. DPS also should implement processes for reviewing the data it enters and updates in CCH.

In addition, DPS should strengthen certain general controls, such as controls over user access and authentication.

[1] See *An Audit Report on the Criminal Justice Information System at the Department of Public Safety and the Texas Department of Criminal Justice* (SAO Report No. 16-025, May 2016).

This audit was conducted in accordance with Texas Code of Criminal Procedure, Article 66.352.

For more information regarding this report, please contact Becky Beachy, Audit Manager, or Lisa Collier, State Auditor, at (512) 936-9500.

Texas Department of Criminal Justice

TDCJ had automated controls, internal review processes, and audit and correction processes in place to help ensure the accuracy of information in CTS and its Intermediate System (ISYS). Additionally, the completeness of incident numbers in CTS for offenders admitted to jail and prison significantly increased since May 2016. However, TDCJ should strengthen controls to (1) improve the completeness of state identification numbers and incident numbers in ISYS (see text box for definitions) and (2) ensure that automated calculations in CTS are programmed correctly.

In addition, TDCJ should strengthen its process for implementing changes to ISYS and its user access and authentication controls.

State Identification and Incident Numbers

The **State Identification Number** (SID) is a unique number assigned by DPS to each person whose name appears in CJIS.

The **Incident Number** is a unique number assigned to a specific person during a specific arrest. The incident number is paired with an incident number suffix for each charge resulting from an arrest. Together, those identifiers enable reporting entities to track each charge through the criminal history reporting process.

Sources: Texas Code of Criminal Procedure, Chapter 66; and DPS.

Implementation Status of Prior State Auditor's Office Recommendations

Auditors followed up on 17 of 21 recommendations in *An Audit Report on the Criminal Justice Information System at the Department of Public Safety and the Texas Department of Criminal Justice* (State Auditor's Office Report No. 16-025, May 2016). Five recommendations were fully implemented, eight recommendations were substantially implemented, and implementation of four recommendations was incomplete or ongoing.

Table 1 presents a summary of the findings in this report and the related issue ratings. (See Appendix 2 for more information about the issue rating classifications and descriptions.)

Table 1

Summary of Chapters and Related Issue Ratings		
Chapter	**Title**	**Issue Rating [a]**
1	Overview of the Criminal Justice Information System	Not Rated
2	Most Information Was Reported Within Required Timeframes, but DPS Should Strengthen Controls Over Certain Data Elements and Processes	Medium
3	TDCJ Had Processes and Controls in Place for Ensuring the Accuracy and Completeness of Information in CTS and ISYS; However, Some Controls Should be Strengthened	Medium
4	DPS Had Information Security Controls in Place, but Certain General Controls Should be Strengthened	Medium
5	TDCJ Had Information Security Controls in Place, but Certain General Controls Should be Strengthened	Medium
6	Summary of Status of Prior Audit Recommendations	Not Rated

Summary of Chapters and Related Issue Ratings		
Chapter	**Title**	**Issue Rating [a]**

[a] A chapter is rated **Priority** if the 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.

A chapter is rated **High** if the 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.

A chapter is rated **Medium** if the 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.

A chapter is rated **Low** if 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.

To minimize the risks associated with public disclosure, auditors communicated details about information technology findings separately in writing to DPS and TDCJ management. Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Generally Accepted 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.

Auditors also communicated other, less significant issues separately in writing to DPS and TDCJ management.

Summary of Management's Response

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

Audit Objective and Scope

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

The scope of this audit covered activities performed between January 1, 2020, and April 30, 2021, including processes and controls performed during that time period and adult criminal history information entered during that time period.

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1
Overview of the Criminal Justice Information System

The Criminal Justice Information System (CJIS) consists of two independent systems maintained by two separate state agencies: the Department of Public Safety (DPS) and the Texas Department of Criminal Justice (TDCJ).

DPS's Computerized Criminal History (CCH) system

DPS maintains the CCH system, which is a database containing arrest, disposition, and supervision information. Specifically, CCH contains:

- **Arrest records.** When a person is arrested, the law enforcement agency reports their identification and arrest information to CCH. This includes the person's fingerprints and physical description, the date of arrest, and the offense(s) they were charged with.

- **Disposition records.** Prosecutors' offices and courts report the results of arrests, referred to as dispositions. For example, district and county attorneys' offices report whether charges were filed with a court or dropped; county, district, and other courts report whether charges were dismissed or resulted in a conviction, along with any associated sentencing information, such as the term of imprisonment or probation.

- **Supervision records.** TDCJ reports information about offenders under its supervision, such as the arrests they were admitted for, their supervision status, and when their sentence will expire.

The information in CCH is used by criminal justice agencies for criminal justice purposes and by legislatively authorized non-criminal justice agencies to help determine eligibility for employment, immigration, adoption, housing, licensing, and firearm purchases. According to DPS, 16,835 agencies and 32,235 users were authorized to obtain criminal history information through the CCH secure website as of November 2021. Certain public information extracted from CCH is available to the general public through the CCH public website.

TDCJ's Corrections Tracking System (CTS)

TDCJ maintains CTS, which is a collection of applications containing information on all offenders under the supervision of corrections agencies and community supervision and corrections departments (CSCDs) in Texas.

CTS includes the following components to manage information on offenders under community supervision (on probation), in jail or prison, or on parole:

- **The Community Supervision Tracking System (CSTS) and the Intermediate System (ISYS).** These two systems include records for offenders under the supervision of the 123 CSCDs in Texas. CSCDs use ISYS to upload community supervision (adult probation) records to CSTS. Records that do not include a state identification number and/or an incident number are suspended in ISYS until that information is obtained and they can be uploaded to CSTS.

- **The State Jail System (SJS) and the State Ready System (SRS**). These two systems include records for offenders who are convicted of felonies and sentenced for terms of imprisonment. Offenders convicted of state jail felonies and sentenced to serve up to 24 months in jail are tracked in SJS, and offenders convicted of all other felonies are tracked in SRS.

- **The Clemency and Parole System (CAPS) and the Offender Information Management System (OIMS)**. These two systems include records for offenders who are placed on parole. Offenders with physical parole files (known as legacy cases) are tracked in CAPS, and offenders with electronic parole files are tracked in OIMS, until they are discharged from TDCJ supervision.

In addition, CCH and CTS are used for notifications, called flash notices, to inform parole and probation officers about offenders on parole or probation who have a subsequent arrest.

Chapter 2

Most Information Was Reported Within Required Timeframes, but DPS Should Strengthen Controls Over Certain Data Elements and Processes

Reporting entities submitted most arrest and disposition information to DPS's CCH system within the required timeframes. DPS had controls in place to help ensure the accuracy and completeness of the information reported. However, DPS should strengthen controls over certain data elements and its data entry and error resolution processes.

Chapter 2 Rating:

Medium [2]

Reporting entities submitted most information to DPS within required timeframes, and compliance with timeliness requirements for reporting final disposition increased.

Law enforcement agencies, prosecutors' offices, and courts submitted most information to CCH within the required reporting timeframes between January 1, 2020, and April 30, 2021 (see text box for additional details about reporting timeframes). Compliance with timeliness requirements has improved since a State Auditor's Office audit report in May 2016.[3] Table 2 summarizes the arrest and court disposition information reported to CCH.

Reporting Timeframes for Arrests and Dispositions

Texas Code of Criminal Procedure, Article 66.252, specifies the timeframes for local entities to report arrest and disposition information to the Department of Public Safety (DPS):

- Law enforcement agencies have seven days to report an offender's arrest to DPS.
- Prosecutors' offices have 30 days to report the action taken on a case to DPS.

In addition, based on an executive order issued by the Governor on September 5, 2019, DPS required courts to report final dispositions within 37 days in 2020 and within 35 days in 2021.

Sources: Texas Code of Criminal Procedure, Article 66.252; Executive Order GA-07; and DPS.

Table 2

Reporting to DPS's CCH System				
Type of Data Reported	Total Reported from January 1, 2020, through April 30, 2021	Total Reported Within Required Timeframes	Percentage Reported Within Required Timeframes	Percentage Reported Within Required Timeframes in 2016 Report
Arrests	922,714	856,868	93%	92%
Court Dispositions	681,719	641,390	94%	69% [a]

[a] At the time of the 2016 report, final court dispositions were required to be reported within 30 days.

Sources: Analysis of data entered into CCH from January 1, 2020, through April 30, 2021, and *An Audit Report on the Criminal Justice Information System at the Department of Public Safety and the Texas Department of Criminal Justice* (SAO Report No. 16-025, May 2016.)

[2] The risk related to the issues discussed in Chapter 2 is rated as Medium because they 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.

[3] See *An Audit Report on the Criminal Justice Information System at the Department of Public Safety and the Texas Department of Criminal Justice* (SAO Report No. 16-025, May 2016).

In addition, from January 1, 2020, through April 30, 2021, prosecutors' offices reported 614,888 (78 percent) of the 790,804 prosecution records that included an action date within 30 days as required by statute.[4] However, prosecutors' offices did not complete the action date field for an additional 93,705 prosecutor records entered into CCH during that time period. Missing action dates affect DPS's ability to monitor the timeliness of disposition reporting. While DPS guidance states that those dates must be entered, the automated controls in CCH did not enforce that requirement for all types of prosecutor actions.

Arrest and Disposition Reporting Processes

Entities have the option to report arrests and dispositions to CCH electronically or by sending paper criminal history reporting forms to DPS for manual entry into CCH. For electronic reporting:

- Law enforcement agencies capture offenders' fingerprints, identification data, and arrest data and transmit it to CCH via the Livescan system.
- Prosecutors' offices and courts submit disposition records through the CCH Web portal, referred to as the CJIS Site or CJIS Website.

According to DPS, 97.3 percent of arrests and 95 percent of dispositions were reported electronically between January 1, 2020, and April 30, 2021.

Source: DPS

DPS should strengthen controls to ensure that certain information is entered into CCH as required.

DPS has implemented automated controls within its electronic arrest and disposition reporting processes to help ensure the accuracy and completeness of information reported to CCH (see text box for more information on those processes). In addition, most data elements analyzed conformed to DPS specifications for most records analyzed. However, controls should be strengthened to help ensure that certain information is entered into CCH as required. Specifically:

Family Violence Reporting Requirements

Historically, reporting to CCH was mandatory for felonies and class A and B misdemeanors, and voluntary for all class C misdemeanors. Effective September 1, 2019, statutory reporting requirements were expanded to include class C misdemeanors that involve family violence as defined by Texas Family Code, Section 71.004.

Reporting entities are responsible for using a field in CCH to identify all offenses that involve family violence. That includes (1) class C misdemeanors which law enforcement agencies determine involve family violence and (2) the 23 offenses which DPS has determined inherently involve family violence (22 of those are class B misdemeanors and above and the other 1 may be any class of misdemeanor).

Sources: Texas Code of Criminal Procedure, Article 66.252; and DPS.

Victim age. Reporting entities did not report the victim age for 29,182 (85 percent) of 34,387 applicable offense records that were required to include that information. Texas Code of Criminal Procedure, Article 66.102(h), requires that CCH include the age of the victim for certain offenses, such as aggravated kidnapping, trafficking, and sexual assault. DPS maintains a list of the offenses that require the victim age on its website and has provided training to reporting entities on the requirement; however, there were not automated controls in the Livescan system or CCH to ensure that the victim age was reported for those offenses.

Family violence offenses. CCH includes a field for reporting entities to identify offenses involving family violence (see text box for additional information on family violence reporting requirements). However, CCH allows that field to remain blank. Without requiring a "yes" or "no" to be entered, there is a risk that family violence is being underreported. For example, DPS

[4] The May 2016 report evaluated only the subset of records that prosecutors rejected; therefore, it would not be appropriate to compare the results from the 2016 report to the results described in this report.

has determined that 23 offenses inherently involve family violence; however, of the 240,304 records associated with those 23 offenses entered during the audit scope, reporting entities did not enter "yes" in that field for 168,582 (70 percent) records. For class C misdemeanors and other offenses, that field may be the only one that identifies whether the offense included family violence.

Data entry of criminal history information. For 5 (20 percent) of 25 criminal history reporting forms tested, DPS did not accurately enter all arrest and disposition information that was reported into CCH. Errors identified included unsupported identification information, an incorrect arrest charge, and failure to enter prosecution information reported. Although automated controls are in place to help ensure the validity of information entered manually, DPS did not have a process in place for reviewing the data entered.

DPS has effective processes in place for correcting records in CCH and made most corrections appropriately.

Error resolution process. DPS has processes in place for updating incomplete and inaccurate criminal history records in CCH to address correction requests and resolve potential errors that are reported by criminal justice agencies, private citizens, and others. This includes processing requests to add, remove, or change information on records; consolidate records; expunge records; and flag records that involve misuse or theft of identity. Of 30 requests reviewed, DPS accurately updated criminal history records for 26 (93 percent) of the 28 requests that required corrections. For the other two requests that required corrections, DPS did not accurately update disposition records based on supporting documentation.

Synchronization process. DPS synchronizes CCH records with Federal Bureau of Investigation (FBI) records on a quarterly basis to identify and correct discrepancies between those two sets of data (see text box for additional information on the process). For 24 (96 percent) of 25 records tested, DPS accurately updated CCH to correct the discrepancies identified.

Interstate Identification Index (III) Program Synchronization Process

The Interstate Identification Index (III) is a national system for the exchange of criminal history records among states and the federal government.

DPS participates in the III program to synchronize Federal Bureau of Investigation (FBI) and CCH data on a quarterly basis. Data elements synchronized include:

- An offenders' FBI universal control number, state identification number, name, sex, race, and date of birth.
- Flags indicating the status of the record (e.g. single or multi-source, deceased, expunged, etc.) and whether the individual is prohibited from purchasing firearms.

The III data is used by the National Instant Criminal Background Check System (NICS) to screen individuals attempting to buy firearms.

Sources: FBI and DPS.

However, DPS had a significant backlog of records that required synchronization to correct discrepancies. As of August 2021, DPS had not completed review of 10 of the 29 synchronization files it received between January 2020 and February 2021. A programming error in the automated

process DPS used to compare records and produce a list of discrepancies that require review significantly contributed to the overall backlog. Because staff received incomplete lists of discrepancies that required review, DPS estimated that 340,563 records related to one type of synchronization report still required review.

Recommendations

DPS should:

- Implement additional automated controls preventing the prosecutor action date, victim age for applicable offenses, and family violence fields from remaining blank.
- Implement review processes to help ensure the accuracy and completeness of the data entered and updated in CCH.
- Develop and maintain monitoring systems for identifying missing and inaccurate information.

Management's Response

DPS agrees with the recommendations and will:

- *Implement mandatory reporting of the Prosecutor Action Date. Implementation Date: 06/30/2022.*
- *Implement mandatory reporting of Victim's Age for applicable offenses. Estimated Implementation Date: 08/31/2023*
- *Enhance training on use of the Domestic Violence Field to be in line with CCP 66.102(f)(7). Implemented 1/31/2022. Implement mandatory reporting for affirmative findings of family violence in the Court reporting section. Estimated Implementation Date: 08/31/2023*
- *Implement a verification process to review manual entries by Quality Assurance Analysts and CCH Quality Technicians. Estimated Implementation Date: 06/30/2022.*
- *Implement verification of court disposition sequence reporting to minimize missed court dispositions. Implementation Date: 06/30/2022.*
- *Enhance training of the web portal functions available to agencies for them to verify their reported data. Estimated Implementation Date: 06/30/2022.*

Title of Responsible Person*: Senior Director, Crime Records Division*

Estimated Completion Date*: See dates above*

Chapter 3

TDCJ Had Processes and Controls in Place for Ensuring the Accuracy and Completeness of Information in CTS and ISYS; However, Some Controls Should be Strengthened

Chapter 3 Rating:

Medium [5]

To ensure the accuracy and completeness of information in CTS and ISYS, TDCJ (1) implemented automated controls within the systems, (2) performed internal reviews, and (3) conducted audit and correction processes. Specifically:

- **Automated controls in CTS and ISYS.** TDCJ designed and implemented automated controls for various data elements to help ensure that offender records are accurately and completely entered into CTS or uploaded to ISYS.

- **Internal reviews of CTS data.** TDCJ had processes for reviewing records within CTS (1) when offenders are admitted to TDCJ and (2) before offenders are released to parole. TDCJ accurately completed 100 percent of those reviews for samples of 25 offenders admitted to prison and 27 offenders released to parole.

- **Audit and correction processes for ISYS data.** TDCJ reviews the data reported to ISYS as part of its audits and evaluations of community supervision and corrections departments (CSCDs) (see text box for additional information on CSCDs). TDCJ accurately performed the data reliability and integrity components of those reviews for all five audits and evaluations tested. TDCJ also had a process in place for CSCDs to request corrections to information in ISYS and accurately processed all 25 requests tested.

Community Supervision and Corrections Departments

The TDCJ Community Justice Assistance Division (CJAD) works with community supervision and corrections departments (CSCDs), which supervise and help rehabilitate offenders who are sentenced to community supervision by local courts (on probation).

There are 123 CSCDs organized within judicial districts that serve the 254 counties in Texas.

Source: TDCJ.

In addition, TDCJ has improved the completeness of incident numbers in CTS. A total of 99 percent of records for offenders who both committed offenses and were admitted to jail or prison for those offenses between January 1, 2020, and April 30, 2021, contained incident numbers. This was a significant improvement since the State Auditor's Office audit report in May 2016,[6]

[5] The risk related to the issues discussed in Chapter 3 is rated as medium because they 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.

[6] See *An Audit Report on the Criminal Justice Information System at the Department of Public Safety and the Texas Department of Criminal Justice* (SAO Report No. 16-025, May 2016).

when only 57 percent of jail records and 88 percent of prison records contained that information.

However, TDCJ should strengthen controls to (1) improve the completeness of state identification numbers and incident numbers in ISYS and (2) ensure that automated calculations in CTS are programmed correctly. Specifically:

State identification numbers and incident numbers in ISYS. As discussed in Chapter 1, probation records that do not include a state identification number and/or incident number are suspended in ISYS. CSCDs are responsible for obtaining the missing information so that records can be transferred from ISYS to CTS, which is important because flash notices are not set up for offenders until their records are in CTS (see text box for additional information on flash notices). However, CSCDs did not obtain missing information that was available in CCH. Specifically, as of July 2021, records associated with 1,222 offenders placed on probation between January 1, 2020, and April 30, 2021, were suspended in ISYS due to missing information. Criminal history records containing one or both of the missing numbers were available in CCH for 113 (9 percent) of those 1,222 offenders on or before April 30, 2021.

Flash Notices

TDCJ provides information to DPS about which individuals with records in CTS are on probation or parole. DPS flags those individuals in the CCH system so that, if those individuals are arrested again, their probation or parole officers will be notified of the arrest. Those notifications, which are required by Texas Code of Criminal Procedure, Article 66.255, are called flash notices.

Source: TDCJ and DPS.

Sentence length in CTS. Offenders' sentence lengths in CTS were correct for 25 (93 percent) of 27 offenders tested who were released to parole between January 1, 2020, and April 30, 2021. However, the remaining two had incorrect sentence lengths in CTS. After auditors brought the errors to its attention, TDCJ determined there was a programming error in CTS, which resulted in a total of 3,415 offenders not receiving the correct amount of credit on their sentences.[7] Those offenders should have received between 1 and 10 additional days of credit, an average of 1.09 additional days. On October 15, 2021, TDCJ updated the sentence lengths of the 3,415 offenders affected.

[7] When offenders spend time in jail between their arrest and sentencing, that time is required to be credited to their sentences.

Recommendations

TDCJ should:

- Work with CSCDs to ensure that they are searching DPS's CCH system for missing information.
- Verify that automated calculations in CTS are programmed correctly before they are implemented.

Management's Response

Recommendation 1

- *The Department should work with CSCDs to ensure that they are searching DPS's CCH system for missing information.*

  The Texas Department of Criminal Justice (TDCJ) agrees with the recommendation. The Community Justice Assistance Division (CJAD) will modify its evaluation criteria for Community Supervision and Corrections Departments (CSCD) to include additional requirements to check the probationer's computerized criminal history and update missing information into their local case management systems. The Director of CJAD shall be responsible for implementing the action. The target date for implementation in February of 2022.

Recommendation 2

- *The Department should verify that automated calculations in CTS are programmed correctly before they are implemented.*

  The Texas Department of Criminal Justice agrees with the recommendation. Once a request to change time calculation is processed by the Information Technology Division (ITD), staff from the Classification and Records Department will review and approve the change before it moves into production. The department will also review a sample of time calculations after it is automated to ensure that the calculation is operating correctly. The Director of the Correctional Institutions Division shall be responsible for implementing the action. The changes were implemented in January of 2022.

Chapter 4

DPS Had Information Security Controls in Place, but Certain General Controls Should be Strengthened

Chapter 4 Rating:

Medium [8]

DPS implemented information security controls to help ensure the reliability of criminal history information in the CCH system. For example, DPS implemented processes for monitoring vulnerabilities of its network resources and followed its processes for implementing changes to CCH for all 10 changes tested.

However, DPS should strengthen certain general controls, such as controls over user access and authentication, to further reduce the risks of loss or inappropriate modification of criminal history information in CCH.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Generally Accepted 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.

[8] The risk related to the issues discussed in Chapter 4 is rated as Medium because they 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.

Chapter 5

TDCJ Had Information Security Controls in Place, but Certain General Controls Should be Strengthened

Chapter 5 Rating:

Medium [9]

TDCJ had controls in place to help ensure the reliability of criminal history information in CTS and ISYS. Specifically, TDCJ:

- Had a formal process in place for managing changes to CTS and effectively managed all eight changes tested.
- Implemented processes for monitoring vulnerabilities of its network resources.
- Had a formally documented disaster recovery plan in place and implemented and tested its backup and recovery processes.

However, TDCJ should strengthen its process for implementing changes to ISYS and controls over user access and authentication to further reduce the risk of inappropriate modifications to its systems or the data within those systems.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Generally Accepted 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.

[9] The risk related to the issues discussed in Chapter 5 is rated as Medium because they 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.

Chapter 6

Summary of Status of Prior Audit Recommendations

Auditors followed up on 17 of 21 recommendations in *An Audit Report on the Criminal Justice Information System at the Department of Public Safety and the Texas Department of Criminal Justice* (State Auditor's Office Report No. 16-025, May 2016).

Table 3 summarizes auditors' determinations about the implementation status of the prior audit recommendations directed to DPS and TDCJ.

Table 3

Summary of Implementation Status of Prior Audit Recommendations				
Implementation Status Determined by Auditors	Implementation Status Definition [a]	DPS	TDCJ	Total Recommendations by Status
Fully Implemented	Successful development and use of a process, system, or policy to implement a prior recommendation.	3	2	**5**
Substantially Implemented	Successful development but inconsistent use of a process, system, or policy to implement a prior recommendation.	4	4	**8**
Incomplete/Ongoing	Ongoing development of a process, system, or policy to address a prior recommendation.	1	3	**4**
Not Implemented	Lack of a formal process, system, or policy to address a prior recommendation.	0	0	**0**
Total Recommendations Reviewed by Auditors		**8**	**9**	**17**

[a] Definitions are from the State Auditor's Office instructions for submitting implementation status of recommendations.

To minimize the risks associated with public disclosure, auditors communicated details about the status of recommendations that were not fully implemented separately in writing to DPS and TDCJ management. Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Generally Accepted 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.

Appendices

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 covered activities performed between January 1, 2020, and April 30, 2021, including processes and controls performed during that time period and adult criminal history information entered during that time period.

The scope also included a review of significant internal control components related to controls over CJIS (see Appendix 3 for more information about internal control components).

Methodology

The audit methodology included conducting interviews and walkthroughs with Department of Public Safety (DPS) and Texas Department of Criminal Justice (TDCJ) management and staff; collecting and reviewing agency policies, procedures, and other guidance; testing agency processes and controls; and analyzing CJIS data.

Data Reliability and Completeness

Auditors obtained data sets from DPS's Computerized Criminal History (CCH) system, TDCJ's Corrections Tracking System (CTS) and Intermediate System (ISYS), and other agency information resources to select samples and perform data analysis.

CCH, CTS, and ISYS. To assess the reliability of the data sets obtained from CCH, CTS, and ISYS, auditors reviewed the data obtained from those systems and the queries used to extract that data for reasonableness and completeness. Auditors determined that the data obtained was sufficiently reliable for purposes of this audit. The following data sets were obtained from CCH, CTS, and ISYS:

- **CCH.** Auditors obtained:
  - The populations of (1) arrest, (2) prosecution, (3) court, and (4) supervision records that were entered into CCH during the audit scope;
  - A log of changes made to CCH records during the audit scope; and
  - Prosecution and court records in the DPS name-based disposition file as of June 7, 2021.
- **CTS.** Auditors obtained the populations of offenders (1) admitted to jail and prison, (2) placed on probation, and (3) placed on parole during the audit scope.
- **ISYS.** Auditors obtained (1) the population of probation records suspended in ISYS as of July 8, 2021, and (2) the log of requests for changes to records in ISYS that were received during the audit scope and completed as of June 28, 2021.

Agency ticketing systems. For the ticketing systems that DPS and TDCJ use to track changes to CCH and CTS respectively, auditors observed the agencies perform queries to identify the populations of changes made to those systems during the audit scope. Auditors determined that those data sets were sufficiently reliable for purposes of this audit.

Agency databases and spreadsheets. Auditors obtained data sets from various databases and spreadsheets maintained by the agencies. For TDCJ, this included the population of audits and evaluations of community supervision and corrections departments (CSCDs) completed during the audit scope. For DPS this included populations of:

- Adult criminal history reporting forms received and entered into CCH during the audit scope;
- Corrections completed during the audit scope; and
- Technical security audits completed during the audit scope.

To determine the reliability of the data sets above, auditors reviewed the data obtained and the queries used to extract that data for reasonableness and completeness. For the correction requests and technical security audits, auditors also traced selected data to supporting documentation. Auditors determined that all of the data sets listed above were sufficiently reliable for purposes of this audit.

Sampling Methodology

Auditors selected the following nonstatistical samples through random selection:

- Twenty-five of the 41,638 adult criminal history reporting forms submitted to DPS during the audit scope, to determine whether DPS accurately entered the reported information in CCH.
- Twenty-five of the 417 technical security audits completed during the audit scope, to determine whether the DPS audit process effectively addresses user access controls at criminal justice agencies.
- Twenty-five of the 25,241 offenders admitted to prison during the audit scope, to determine whether TDCJ's review processes were operating effectively to help ensure the accuracy and completeness of prison offender data.
- Twenty-five of the 5,810 requests for changes to records in ISYS that were received during the audit scope, to determine whether TDCJ accurately processed corrections.
- Five of the 32 audits and evaluations of CSCDs completed during the audit scope, to determine whether TDCJ audit and evaluation processes help ensure the reliability and integrity of probation data.

The samples above were designed to be representative of the populations, so the test results may be projected to the populations, but the accuracy of the projections cannot be measured.

To test DPS processes for correcting discrepancies between CCH and Federal Bureau of Investigation (FBI) records, auditors selected a sample of 3 synchronization reports from the population of 19 synchronization reports that DPS completed during the audit scope. Then, auditors selected a stratified random sample of 25 records from the 898 records among those 3 reports. This directed sample approach was chosen to obtain coverage of discrepancies for a variety of data elements in CCH. The sample items were not necessarily representative of the population; therefore, it would not be appropriate to project the test results to the population.

Auditors used a combination of random and risk-based sampling for two additional samples:

- To determine whether corrections to CCH were processed accurately, auditors selected 30 of the 12,447 correction requests processed by DPS during the audit scope. That sample included 25 correction requests selected at random and 5 selected based on risk.

- To determine whether TDCJ's review processes were operating effectively to help ensure the accuracy and completeness of parole data, auditors selected records for 27 of the 45,278 offenders released to parole during the audit scope. That sample included 25 offenders selected at random and 2 selected based on risk.

The test results as reported do not identify which items were randomly selected or selected using professional judgment; therefore, it would not be appropriate to project the test results to the populations.

To test both agencies' change management processes, auditors selected directed samples to obtain coverage of different types of changes to CCH and CTS, such as routine updates and other enhancements. Specifically, auditors selected (1) 10 of the 85 CCH-related change requests completed during the audit scope and (2) 8 of the 55 CTS-related change requests closed during the audit scope. The sample items were not necessarily representative of the populations; therefore, it would not be appropriate to project the test results to the populations. In addition, auditors relied on TDCJ to identify changes made to ISYS during the audit scope and tested the sole change identified.

Information collected and reviewed included the following:

- Arrest, prosecution, court, and supervision records entered into CCH during the audit scope.
- Prosecution and court records in the DPS name-based disposition file as of June 7, 2021.
- CTS and ISYS records related to offenders (1) admitted to jail and prison, (2) placed on probation, or (3) paroled during the audit scope.
- Probation records suspended in ISYS as of July 8, 2021.
- Criminal history reporting forms received by DPS.
- Checklists used to complete internal reviews.
- Court documents obtained and reviewed by DPS and TDCJ.
- Criminal history reports from CCH.

Procedures and tests conducted included the following:

- Interviewed DPS and TDCJ management and staff.
- Tested DPS's processes for entering and correcting data in CCH.

- Tested TDCJ's processes for reviewing and correcting data in CTS and ISYS.
- Tested automated controls in Livescan devices, the CCH Web portal, CTS, and ISYS.
- Analyzed and compared data in and among CJIS systems.
- Calculated the time that reporting entities took to enter information in CCH.
- Tested the DPS process for sending reports to county commissioners.
- Reviewed password configurations and user access for CCH, CTS, and ISYS resources.
- Reviewed TDCJ's annual user access review process for external ISYS users.
- Tested DPS and TDCJ processes for tracking and implementing changes to CCH, CTS, and ISYS.
- Evaluated DPS and TDCJ cybersecurity and backup and recovery processes and controls.
- Tested DPS and TDCJ processes for auditing law enforcement agencies and CSCDs, respectively.

Criteria used included the following:

- Texas Code of Criminal Procedure, Chapter 66.
- The FBI's *Criminal Justice Information Services (CJIS) Security Policy*, versions 5.8 and 5.9.
- CCH specifications, including the CCH Data Dictionary, version 1.6, and reporting code appendices.
- DPS and TDCJ policies, procedures, manuals, guides, and other guidance.
- Governor's Executive Order No. GA-07 relating to the prevention of mass attacks (September 5, 2019).

Project Information

Audit fieldwork was conducted from February 2021 through January 2022. We conducted this performance audit 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 objective(s). Those standards also require independence in both fact and appearance. During the audit, legislative funding was vetoed. This condition could be seen as potentially affecting our independence in reporting results related to the agencies audited. However, we proceeded with this audit as set forth by the annual state audit plan, operated under the Legislative Audit Committee. We believe this condition did not affect our audit conclusions.

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

- Tessa Mlynar, CIA, CFE (Project Manager)
- Fabienne Robin, MBA (Assistant Project Manager)
- Joe Kozak, CPA, CISA
- Venus Santos
- Quang Tran, CFE
- Tony White, CFE
- Dana Musgrave, MBA, CFE (Quality Control Reviewer)
- Becky Beachy, CIA, CGAP (Audit Manager)

Appendix 2

Issue Rating Classifications and Descriptions

Auditors used professional judgment and rated the audit findings identified in this report. Those issue ratings are summarized in the report chapters/sub-chapters. The issue ratings were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

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.

Table 4 provides a description of the issue ratings presented in this report.

Table 4

Summary of Issue Ratings	
Issue Rating	**Description of Rating**
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.
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.
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.
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.

Appendix 3

Internal Control Components

Internal control is a process used by management to help an entity achieve its objectives. The U.S. Government Accountability Office's *Generally Accepted Government Auditing Standards* require auditors to assess internal control when internal control is significant to the audit objectives. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) established a framework for 5 integrated components and 17 principles of internal control, which are listed in Table 5.

Table 5

Internal Control Components and Principles		
Component	**Component Description**	**Principles**
Control Environment	The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.	▪ The organization demonstrates a commitment to integrity and ethical values. ▪ The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. ▪ Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. ▪ The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. ▪ The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	Risk assessment is the entity's identification and analysis of risks relevant to achievement of its objectives, forming a basis for determining how the risks should be managed.	▪ The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. ▪ The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. ▪ The organization considers the potential for fraud in assessing risks to the achievement of objectives. ▪ The organization identifies and assesses changes that could significantly impact the system of internal control.
Control Activities	Control activities are the policies and procedures that help ensure that management's directives are carried out.	▪ The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. ▪ The organization selects and develops general control activities over technology to support the achievement of objectives. ▪ The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Internal Control Components and Principles		
Component	**Component Description**	**Principles**
Information and Communication	Information and communication are the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.	▪ The organization obtains or generates and uses relevant, quality information to support the functioning of internal control. ▪ The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. ▪ The organization communicates with external parties regarding matters affecting the functioning of internal control.
Monitoring Activities	Monitoring is a process that assesses the quality of internal control performance over time.	▪ The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. ▪ The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Source: Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, May 2013.

Appendix 4

Related State Auditor's Office Reports

Table 6

Related State Auditor's Office Reports		
Number	**Report Name**	**Release Date**
21-002	*An Audit Report on Investigation and Prosecution Processes for Reported Sexual Assaults in Texas*	October 2020
19-040	*An Audit Report on Diversion Program Grants at the Texas Department of Criminal Justice*	July 2019
19-014	*An Audit Report on the Department of Public Safety's Driver License Division*	December 2018
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 Dade Phelan, 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

Texas Department of Criminal Justice

Members of the Board of Criminal Justice
- Mr. Patrick O'Daniel, Chairman
- Ms. Derrelynn Perryman, Vice-Chairman
- Mr. Larry Miles, Secretary
- Mr. Rodney Burrow
- Mr. E.F. "Mano" DeAyala
- The Honorable Molly Francis
- The Honorable Faith Johnson
- Mr. Eric Nichols
- Mr. Sichan Siv

Mr. Bryan Collier, Executive Director

Texas Department of Public Safety

Members of the Public Safety Commission
- Mr. Steven P. Mach, Chairman
- Ms. Nelda L. Blair
- Mr. Steve H. Stodghill
- Mr. Dale Wainwright

Colonel Steven C. McCraw, Director