John Keel, CPA
State Auditor

An Audit Report on

The Criminal Justice Information System

February 2006
Report No. 06-022

State Auditor's Office
John Keel, CPA
State Auditor

An Audit Report on

The Criminal Justice Information System

SAO Report No. 06-022
February 2006

Overall Conclusion

The Department of Public Safety (DPS) and the Texas Department of Criminal Justice (TDCJ) have made significant improvements to their portions of the Criminal Justice Information System (CJIS) since the State Auditor's Office's December 2001 audit of CJIS (see *An Audit Report on the Accuracy of Criminal Justice Information System Data at the Department of Public Safety and the Department of Criminal Justice*, SAO Report No. 02-013). However, more improvements are needed at both agencies to ensure that the data in CJIS is complete, timely, and accurate.

Specifically, DPS should strengthen and monitor access to its secure Web site so that unauthorized individuals do not have access to confidential criminal history data. There are 7,488 entities that use this Web site to conduct criminal background checks with data from CJIS. Auditors contacted 42 of those entities and found that 11 (26.2 percent of the sample) had unauthorized users. In total, 17 (21 percent) of the 81 listed users at these entities were no longer employed by the entities.

The Criminal Justice Information System

The Criminal Justice Information System (CJIS) includes information systems at two state agencies:

- The Computerized Criminal History system and the Automated Fingerprint Identification System are maintained by the Department of Public Safety. The Computerized Criminal History system contains data on arrests and dispositions, and the Automated Fingerprint Identification System contains fingerprints associated with arrests or with noncriminal background checks.
- The Corrections Tracking System is maintained by the Texas Department of Criminal Justice. This system contains data on prison inmates, probationers, and parolees.

Arrest records are maintained in the Computerized Criminal History system for all felonies, Class A misdemeanors (such as unlawful carrying of a weapon), and Class B misdemeanors (such as driving while intoxicated). Individual counties have discretion in entering Class C misdemeanors (which are punishable by a fine only; for example, public intoxication) into the system.

Chapter 411 of the Texas Government Code specifies which types of entities have access to CJIS data and what their level of access is. See Appendix 2 for more information on the entities that use CJIS data.

DPS also needs to perform background checks that are based on fingerprints (instead of just on names) on the users of this Web site before granting them access. The Federal Bureau of Investigation's (FBI) CJIS policy requires fingerprint checks of all individuals who have access to the FBI's CJIS system. The state CJIS system is linked to the FBI's CJIS system and contains the same type of data. Although the users of DPS's secure Web site do not have direct access to the data in the FBI or state CJIS systems, background checks are important because they help ensure that people with criminal backgrounds do not have access to confidential criminal history information. In addition, DPS should revise its disaster recovery plan and ensure that the plan adequately provides for the continued operation of its Automated Fingerprint Identification System and

This audit was conducted in accordance with the Texas Code of Criminal Procedure, Article 60.02.

For more information regarding this report, please contact Nicole Guerrero, Audit Manager, or John Keel, State Auditor, at (512) 936-9500.

complies with Texas Administrative Code (TAC) requirements and standards recommended by the Department of Information Resources.

TDCJ needs to strengthen its approval processes for changes made to its automated systems. It should also develop controls to ensure that programmers do not have access to live (production) data or that their access is closely monitored. It is a good management policy to prevent or restrict system development programmers' access to live data and to hold programmers accountable for changes so that the integrity of the live data is not compromised.

In addition, TDCJ should improve the timeliness with which criminal records for individuals who are on probation are identified in CJIS. To do this, TDCJ should encourage local probation departments to submit updated probation information on a more timely basis. Currently, local probation departments update information monthly. State law requires probation departments to submit this data within 30 days of a probation status change, but more frequent updates would help ensure that when someone on probation is arrested, the individual's probation officer is notified immediately.

The disaster recovery planning deficiencies at DPS and the programmers' access to live data at TDCJ were previously identified in the State Auditor's Office's December 2001 audit report on CJIS and remain uncorrected.

Key Points

DPS and TDCJ have made significant improvements in the completeness, timeliness, and accuracy of CJIS data.

Both agencies have adjusted their processes to improve the reliability of data in CJIS. Since the State Auditor's Office's December 2001 audit of CJIS, DPS has increased the number of dispositions matched to arrests to ensure that criminal records are complete. In addition, TDCJ has begun collecting and requiring incident tracking numbers before it will accept an inmate, which helps ensure that each offender's criminal history record reflects all criminal activity.

DPS needs to improve its security controls and disaster recovery planning.

DPS maintains a secure Web site through which thousands of entities perform criminal background checks. However, DPS does not adequately monitor user access to this Web site to prevent unauthorized users from obtaining confidential information. In addition, DPS's disaster recovery plan does not adequately address its Automated Fingerprint Identification System, which is critical to its processes.

TDCJ should make improvements in its change management processes and the timeliness of probation data.

TDCJ's change management processes do not comply with several requirements in the TAC. TDCJ allows programmers to access live data but does not consistently monitor the changes that are made to data to ensure that these changes are necessary and authorized. Also, most probation departments report their

probation information to TDCJ on a monthly basis, resulting in a delay between the time that individuals are placed on or removed from probation and the time their probation officers can be notified of their arrests.

Summary of Management's Response

DPS and TDCJ management generally agree with the recommendations in this report.

DPS chose to respond specifically to the Key Points section of this report, as well as to the individual recommendations in Chapter 2. With regard to the Key Points, DPS stated:

> *The "Key Points" of the audit report state that "DPS and TDCJ have made significant improvements in the completeness, timeliness, and accuracy of CJIS data." We agree with that assessment and appreciate the notation of that success in the report. The document also states "DPS needs to improve its security controls and disaster recovery planning." The findings regarding security controls focus on access to CJIS and resultant use by non-criminal justice licensing and employment agencies. Again, we concur with the conclusions. We have recognized that the ever increasing use of the criminal history data for licensing, employment, volunteerism, and other "non-criminal justice" purposes naturally creates a corresponding responsibility for controls over those entities. Our limited resources have prevented an adequate response to this rising need.*

Summary of Information Technology Review

In addition to the audit work described in this report, auditors performed wireless network security scans and internal network scans at DPS to review access security over the agency's information technology systems. We discussed the results of these scans with DPS. We did not perform any scans at TDCJ.

Summary of Objective, Scope, and Methodology

The audit objective was to determine whether controls over data in CJIS provide reasonable assurance that data in this system is complete, accurate, and timely. The audit scope covered information in CJIS from December 2001 to December 2005.

The audit methodology consisted of conducting interviews; collecting and reviewing information; and performing tests, procedures, and analyses against predetermined criteria for DPS and TDCJ relating to CJIS.

Recent SAO Work		
Number	**Product Name**	**Release Date**
02-013	An Audit Report on the Accuracy of Criminal Justice Information System Data at the Department of Public Safety and the Department of Criminal Justice	December 2001

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1

DPS and TDCJ Have Made Significant Improvements in the Completeness, Timeliness, and Accuracy of CJIS Data

Both the Department of Public Safety (DPS) and the Texas Department of Criminal Justice (TDCJ) have made adjustments in their processes that are helping to improve the completeness, timeliness, and accuracy of the data in the Criminal Justice Information System (CJIS). DPS is providing counties with data and resources that will enable them to identify and correct errors and to review their performance in submitting data. In addition, the completeness of the data in CJIS is improving slightly due to more timely submissions of court dispositions, and the number of errors in fingerprint records is decreasing. TDCJ is collecting data that will help ensure the accuracy of inmate records and is developing infrastructure that will aid in the automation of the CJIS data collection process.

Costs of CJIS

Due to the size and complexity of CJIS, which was implemented in May 1994, it is difficult to calculate the total cost associated with the systems involved. An approximate cost is $58.8 million. This includes:

- $3.2 million for the Computerized Criminal History system rewrite at DPS
- $31.4 million for the Offender Management Information System at TDCJ
- $11.9 million for the Corrections Tracking System at TDCJ
- $12.3 million for the Automated Fingerprint Identification System at DPS

DPS generated approximately $7.5 million in revenues from the use of CJIS data in fiscal year 2005 through fees charged for performing criminal records checks via DPS's secure Web site, its public Web site, fingerprint checks, and sales of its public database of criminal records.

Size of CJIS

As of December 2005, there were:

- 30.4 million records in the Computerized Criminal History system
- 6.3 million records in the Automated Fingerprint Identification System
- 1.6 million records in the Corrections Tracking System

These records included information on:

- 151,477 inmates who were incarcerated
- 266,811 active probationers
- 76,163 active parolees

In fiscal year 2005, 757,431 new arrests and 770,176 new court dispositions were submitted to DPS for inclusion in the Computerized Criminal History system.

Source: Unaudited information provided by TDCJ and DPS

DPS has made improvements in the completeness of CJIS data. The December 2001 State Auditor's Office audit of CJIS (see *An Audit Report on the Accuracy of Criminal Justice Information System Data at the Department of Public Safety and Department of Criminal Justice*, SAO Report No. 02-013) found that information in DPS's Computerized Criminal History system was incomplete because DPS was not always able to match court dispositions with arresting events and complete the criminal history records. These records did not match because court dispositions were sometimes submitted before the arresting agency had submitted the arrest information. Other records could not be matched because disposition information submitted by the court did not match the specific arrest information.

To improve the completeness of criminal records by improving the ability to match dispositions to arrests, House Bill 776 (77th Legislature, Regular Session) charged DPS with creating a name-based, searchable database to house unmatched court disposition records. DPS developed the database and, as of November 2005, the database had 224,255 records. In addition, DPS maintains a return file that sends counties information on which transactions

have processed correctly and which have not, as well as information on what the errors are so that these errors can be corrected and the data resubmitted.

DPS also developed a compliance report that details the number and percent of matching arrests and dispositions by county so that each county can review its performance and correct any errors. The most recent compliance report published by DPS in April 2005 (for data reported in 2003) showed that 71 percent of adult arrest records had matching disposition records in the system.

The timeliness and accuracy of data in the Computerized Criminal History system is improving. Auditors requested compliance data from DPS for 2001, 2002, and 2003 and performed a trend analysis to determine whether arrests were being matched to dispositions at a faster rate. As of November 2005, the matching rates for arrest records and dispositions were 74 percent, 73 percent, and 73 percent for 2001, 2002, and 2003, respectively.

In addition, after 22 months, the 2003 matching rate was almost equal to (1) the 2002 matching rate after 34 months and (2) the 2001 matching rate after 46 months. This indicates that the timeliness of the data in the Computerized Criminal History system is slowly improving.

Electronic submissions from local jurisdictions represented 72 percent of the total arrest and disposition reports processed by DPS in fiscal year 2005 (79 counties report electronically). Auditors evaluated electronic reporting data provided by DPS and determined that in fiscal year 2005, 94 percent of the 594,875 arrest reports, 72 percent of the 1,301,786 prosecution dispositions, and 91 percent of the 686,023 court dispositions submitted to DPS did not contain errors. Generally, electronic reporting is more accurate than manual (paper) reporting. The increase in electronic reporting is resulting in more accurate data in CJIS.

The accuracy of fingerprint data has improved. In the past, information in the Computerized Criminal History system was not completely accurate because some offenders had more than one state identification number (state ID). The December 2001 State Auditor's Office audit of CJIS found that there was a backlog of 3,300 of these duplicate state IDs, called "misraps" (see text box), that were waiting to be manually resolved. DPS has instituted policies and procedures to identify and immediately resolve misraps, and there is no longer a backlog of misraps waiting for resolution. In fiscal year 2005, 16,445 misraps were identified and corrected.

What Is a Misrap?

Although each offender in the Computerized Criminal History system should have one unique state ID, for various reasons arrest fingerprints of persons with prior criminal histories do not always match the fingerprints already on file. This causes some offender criminal history files to be incomplete. When a fingerprint search erroneously fails to match an existing record and a new state ID is created, this is referred to as a misrap.

TDCJ has made efforts to improve the accuracy and completeness of its CJIS data. The December 2001 audit of CJIS found that TDCJ was not always collecting incident tracking numbers in the Corrections Tracking System as required by

the Texas Code of Criminal Procedure. The state ID and the incident tracking number are unique identifiers for a particular individual and a particular offense. Without incident tracking numbers, there is a risk that TDCJ would not be able to ensure that complete and accurate offender information is reported from the time an offender is arrested until the time the offender is released.

In addition, some of the final judgments that TDCJ received from the courts did not contain incident tracking numbers. House Bill 967 (79th Legislature, Regular Session), which became effective in September 2005, clarifies the need to report the incident tracking number with the final judgment. Therefore, TDCJ will start requiring the incident tracking number before accepting an inmate.

Improvements in its telecommunications infrastructure enable TDCJ to electronically transmit data to DPS. During the December 2001 CJIS audit, TDCJ did not have the infrastructure to electronically transmit offender fingerprints and demographic information to DPS. This infrastructure is now in place at the TDCJ intake units that have the ability to electronically scan fingerprints. TDCJ has automated fingerprint equipment at 11 of 24 intake units.

In addition to the improvements discussed above, TDCJ has made improvements to the process for providing to DPS information about which individuals with criminal records in the Corrections Tracking System are on probation or parole. Information regarding these individuals is flagged in DPS's Computerized Criminal History system so that if these individuals are arrested again, their probation or parole officers will be notified of the arrest. More information on this process can be found in Chapter 3-B.

Chapter 2

DPS Should Make Improvements in Security Controls and Disaster Recovery Planning

DPS should more closely monitor user access to its secure Web site (see text box). Monitoring would help DPS ensure that only authorized users access and obtain information from that Web site. In addition, DPS performs only limited checks before granting users access to this Web site. More extensive background checks that include fingerprints would help ensure that users are who they claim to be and that they do not have criminal records.

DPS's Secure Web Site

DPS developed a secure Web site to make it easier for entities with access authorized by Chapter 411 of the Texas Government Code to perform criminal background searches on prospective employees or licensees. (See Appendix 2 for a complete list of authorized entities.)

As of December 2005, 7,488 entities had access to the secure Web site. These entities include state licensing agencies, school districts, daycare facilities, and nursing homes, as well as home service businesses such as plumbers, electricians, and movers. At the time of audit testing, these entities employed 16,446 authorized users of the Web site.

In addition, DPS's disaster recovery plan does not adequately address one system that is critical to its processes: the Automated Fingerprint Identification System. The plan also does not meet all of the requirements of the Texas Administrative Code (TAC) or standards recommended by the Department of Information Resources. (The State Auditor's Office also identified this issue in the December 2001 audit report on CJIS.) Incorporating all systems and adhering to guidelines would help DPS ensure that it could continue operations with little or no interruption in the event of a disaster.

Chapter 2-A

DPS Should Improve Controls over Its Secure Web Site

DPS does not adequately monitor user access to its secure Web site. In addition, when granting access, DPS performs a name-based background check but does not perform a fingerprint check to ensure that individuals are who they say they are and that they do not have criminal records in another state or under another name. These background checks are important because they help ensure that people with criminal backgrounds do not have access to confidential criminal history information.

DPS should monitor the access of users who perform criminal background checks. DPS grants access to its secure Web site after users complete a user agreement. However, after granting initial access, it does not periodically verify whether users are still employed by the same entities and should continue to have access to the confidential information available on the Web site. DPS also does not automatically deactivate user IDs that have not been used for a certain period of time.

Auditors contacted 42 randomly selected entities with a total of 81 secure Web site users to determine whether their registered users should still have access. Eleven (26.2 percent) of those 42 entities have unauthorized users. In

total, 17 (21 percent) of the 81 listed users were no longer employed by these entities. These individuals still retain access to the secured Web site and to the confidential information it provides. Nine of the 11 entities with unauthorized users had a level of access that allows them to obtain all criminal history information except restricted juvenile records. In addition, 59 (73 percent) of the 81 users we reviewed did not have user agreements on file with DPS.

Furthermore, some of the entities, including some of those with users who were no longer employed there, allow people to log on to the secure Web site by sharing the user IDs and passwords of former employees. For example, one entity uses the IDs and passwords for two employees who are no longer employed by that entity to access the secure Web site. Another entity has IDs and passwords for each authorized user, but the employees all use the same ID and password. Another entity volunteered its log-on ID and password to auditors over the phone.

Based on conversations with staff at these entities, auditors concluded that some entities do not know how to contact DPS to update their current user lists to add or remove a user. The signed user agreement that DPS obtains prior to granting access does not contain this information, nor is the user provided with rules about appropriate access or password security.

The security issues discussed above increase the risk that individuals without proper authorization could access DPS's secure Web site and obtain confidential criminal history information. However, access to the secure Web site does not give users the ability to add, delete, or change information, and it does not allow users to access national criminal history records.

DPS should perform fingerprint checks on users who have access to criminal history information. DPS performs a name-based background search on the individuals who apply for access to its secure Web site, but it does not perform a full background check that includes fingerprint checks. DPS also does not perform background checks on law enforcement employees (including probation and parole officers) who have access to the Web site; instead, it relies on those individuals' employers to perform these checks. Of the 16,446 individuals with access to the Web site, 80.6 percent have access to confidential data that is not available to the general public. This creates a risk that someone with a criminal record under another name or in another state could potentially gain access to confidential information on warrants, arrests, and court dispositions.

Because state criminal history systems are linked to the federal criminal history system, the Federal Bureau of Investigation (FBI) implemented a CJIS security policy in April 1999. The policy requires state and national fingerprint records checks for all staff with CJIS access, as well as signed written agreements for all criminal justice and non-criminal justice users and private contractors. Although the users of the secure Web site do not have

direct access to the FBI or state CJIS systems, background checks are important because they help ensure that people with criminal backgrounds do not have access to confidential criminal history information. In addition, the FBI's CJIS security policy requires compliance audits of all criminal justice and non-criminal justice end user agencies that have access to state CJIS systems at least once every three years.

Recommendations

DPS should:

- Perform periodic reviews of the users of its secure Web site to ensure that these individuals' access to the Web site is needed and that their level of access is still appropriate given their job duties and positions.

- Automatically deactivate Web site user IDs and passwords that have not been used after a set period of time.

- Require users of its secure Web site to sign a security agreement that contains:

  - Rules about logging on and password sharing.

  - Information on how to set up and delete user accounts.

  - Information on how to contact DPS with questions or changes to account information.

- Perform full background checks, including fingerprint checks, on all individuals who request access to nonpublic information on the secure Web site.

Management's Response

- *We concur with this recommendation. Limited resources have prevented such reviews. Pending our ability to apply greater resources, we will mail the user access lists to each user entity and require them to respond in writing with appropriate changes, additions, and deletions.*

- *We concur with this recommendation and we will make programming changes to deactivate user accounts that have not been used for 30 days.*

- *We concur with this recommendation and will develop and distribute the revised user agreements.*

- *We concur with this recommendation, but we caution that it will take significant time to implement. In addition to communicating the updated*

security policy data, we will advise that users must submit fingerprints to DPS for appropriate background searches. The gathering of fingerprints, performing the criminal history searches, making suitability determinations, and correlating those to users and user entities will be a lengthy process.

Chapter 2-B

DPS Should Revise Its Disaster Recovery Plan to Adequately Address the Automated Fingerprint Identification System and Make Other Improvements

DPS should revise its disaster recovery plan to help ensure the recovery of its Automated Fingerprint Identification System (see text box) in the event of a disaster. Although the plan addresses that system, it does not contain several important elements. In addition, DPS's overall disaster recovery plan does not contain 45 percent of the elements required by the TAC and recommended by the Department of Information Resources' standards. The plan has not been updated since July 2003.

Automatic Fingerprint Identification System

The Automated Fingerprint Identification System electronically stores fingerprint records for individuals who are arrested, as well as for individuals who apply for jobs for which fingerprint checks are required.

Law enforcement agencies and other entities use this information to determine whether individuals are wanted for crimes and to run background checks on applicants for certain types of jobs.

DPS should develop a specific disaster recovery plan for the Automated Fingerprint Identification System. DPS does not have an adequate disaster recovery plan for the Automated Fingerprint Identification System. The overall disaster recovery plan for DPS mentions this system, but it does not include several elements that are needed to ensure that this system can be recovered in case of a disaster. For example, the plan does not identify the resources needed to recover the system, and it lacks a testing schedule. Furthermore, DPS has not performed testing on the backup tapes for the Automated Fingerprint Identification System, which are maintained at the State Library. This means that in the event of a service interruption, DPS has no assurances that the system could be successfully restored using the backup tapes.

The Automated Fingerprint Identification System is a proprietary system, and the vendor does not have a contractual obligation to provide a disaster recovery plan for the system. Title 1, TAC, Section 202.24, requires state agencies to (1) maintain a written disaster recovery plan for information resources, (2) update the plan with information learned from periodic testing, and (3) test the plan annually.

DPS's disaster recovery plan should comply with TAC requirements. DPS's current disaster recovery plan does not meet 45 percent of the requirements in TAC or the standards recommended by the Department of Information Resources. For example, the plan is not based on a current business impact analysis, nor does it include necessary elements such as identification of the agency's mission-critical systems and critical business processes. It also contains outdated plans and contact information.

The State Auditor's Office recommended in its December 2001 report that DPS base its disaster recovery plan on a business impact analysis to assess the potential impacts of a loss of business functions due to an interruption of computer or infrastructure services. DPS's Information Management Services Division completed a business impact analysis in November 2001, but that analysis has not been updated. Since that time, at least one of the individuals listed as a contact on the plan has left the agency. However, DPS is testing the plan at least once a year as required.

The Department of Information Resources' *Business Continuity Planning Guidelines* (revised December 2004) indicate that business impact analysis results "are the foundation and cornerstone of the plan and strategies selected to use in the event of a disaster." Because DPS has not completed this analysis, it risks (1) not identifying potential impacts on its business operations if there was an interruption of computing or infrastructure support services and (2) being unable to recover from such interruptions.

Recommendations

DPS should:

- Consider amending its contract with its vendor to require the vendor to develop and maintain an adequate disaster recovery plan for the Automated Fingerprint Identification System and to test the plan regularly.
- Develop a current business impact analysis and revise its disaster recovery plan based on that analysis.
- Ensure that the disaster recovery plan contains all of the elements required by the TAC and complies with standards recommended by the Department of Information Resources
- Update the disaster recovery plan when changes occur.

Management's Response

- *We agree that a more formalized disaster recovery plan should exist for AFIS. Management is now working with the AFIS vendor (NEC) to*

develop a plan that will outline the roles and responsibilities of DPS and NEC in the disaster recovery process. Our experience is that regular testing of such a plan would prove impractical without the existence of another AFIS in a separate location. Because of the prohibitive cost of such a configuration, we do not anticipate that model for the disaster recovery plan.

- *We concur with this recommendation.*

- *We concur with this recommendation, except to the degree that the impracticality of purchasing a redundant AFIS limits our ability to ensure a full "continuity of information resources supporting critical services" function. The continuity plan involves use of FBI's AFIS search capability, which at present includes a subset of all Texas AFIS data. We are in the process of updating the FBI AFIS to include all Texas AFIS data, but that is a long term project. In addition, without the redundant AFIS, the TAC annual testing requirements exceed the plan's anticipated capability. The disaster recovery methodology has been tested, albeit in a production environment. That test demonstrated the disaster recovery methodology's ability to move the archived AFIS data to a different platform. That test was performed as part of a major system upgrade. Because of the complex nature of AFIS data storage, to restore the files from archive is a time consuming and expensive process, and we would not anticipate repeating that demonstration outside of a system upgrade.*

- *We concur with this recommendation.*

TDCJ's change management processes do not provide adequate assurance that unauthorized changes to its automated systems and applications will be prevented or detected. In addition, TDCJ's current policy of allowing programmers to access live (production) data without close monitoring exacerbates the lack of controls. Although TDCJ has made significant improvements in the accuracy of the information used to update the Computerized Criminal History system at DPS, auditors identified areas for further improvement to increase the timeliness of this information.

Chapter 3-A

TDCJ Should Improve Its Change Management Processes and Ensure that Programmers Do Not Have Access to Live Data

TDCJ's approval process for changes to its automated systems does not comply with change management requirements in the TAC. TDCJ's change management policies and procedures have not been updated since 1997. An updated and detailed change management policy and procedure would mitigate the risk that unauthorized changes could be made to automated systems and applications.

In addition, TDCJ has granted 29 of its programmers access to live data and applications in the Corrections Tracking System so that they can make minor or emergency changes. However, TDCJ does not have sufficient mitigating controls to prevent these programmers from making unauthorized changes to the data. Currently, staff enter changes to TDCJ's computer applications into an automated change management system, and these changes are only occasionally reviewed by a manager. Because some of the applications do not have audit trails that record who made which change, it is possible that unauthorized changes to live data could be made without detection. It is a good management policy to prevent or restrict system development programmers' access to live data and to hold them accountable for changes so that the integrity of live data is not compromised.

Furthermore, although TDCJ requires and maintains adequate documentation to support the request, review, approval, and implementation of major changes, it does not require adequate documentation for minor changes or for moving programs from the test environment to the production environment. In addition, TDCJ's information technology division does not have a formal quality control process and does not require supervisory review of changes made by staff in that division. As a result, unauthorized changes could be made to data without detection.

Recommendations

TDCJ should:

- Update its change management processes to comply with the TAC.
- Implement controls to prevent unauthorized changes to production programs and data, or remove programmers' access to the production environment.
- Require additional information in the automated change management system—such as the name of the individual who reviewed the code, testing information, and the date the change was submitted— to increase accountability.
- Improve documentation required for moving programs from the test environment to the production environment.

Management's Response

- *TDCJ agrees to update the Change Management Standards and Procedures to comply with TAC. The Change Management Standards and Procedures will be updated to include standards and procedures to be followed in the Request for Services "RQ00" system which inventories and documents all Information Technology Division request for services. Target date: February 1, 2007*
- *TDCJ agrees and will remove individual programmers' access to the production environment to prevent unauthorized changes to production programs. Access to the Adhoc and Override libraries will be limited to teamleaders. Individual programmers will no longer have the access to move programs directly to the production environment.*

  TDCJ will research and evaluate tools for auditing changes made by teamleaders to production data. Target date: February 1, 2007
- *TDCJ agrees, and will comply with adding the additional information to the change management documentation. Target date: May 1, 2006*
- *TDCJ agrees, and will create formal documentation for moving programs from the test environment to the production environment. Target date: August 1, 2006*

Chapter 3-B

While TDCJ Has Made Significant Improvements, It Should Take Additional Steps to Ensure that the Data Used to Identify Probationers in CJIS Is Current

Information for 89 percent of individuals identified as being on probation in TDCJ's Corrections Tracking System was correctly flagged in DPS's Computerized Criminal History system. This is a significant improvement since 2001, when the Criminal Justice Policy Council reviewed TDCJ's Flash Notice System (see text box) and found that information for 46 percent of the individuals placed on probation and 49 percent of the individuals whose probation was revoked was not correctly flagged in the Computerized Criminal History system (see the Criminal Justice Policy Council's report entitled *Texas Criminal Justice Information System Audit*). As of November 2005, there were 605,229 records flagged in the Computerized Criminal History system.

Flash Notice System

TDCJ provides information to DPS about which individuals with criminal records in the Corrections Tracking System are on probation or parole. Information for these individuals is flagged in DPS's Computerized Criminal History system so that if these individuals are arrested again, their probation or parole officers will be notified of the arrest. The notices TDCJ sends to inform officers of individuals' status are called flash notices.

DPS is responsible for adding and removing flags for individuals on probation and parole based on the information TDCJ provides. The flags reside in the Computerized Criminal History system that DPS maintains.

However, the timeliness of this information could be improved to further increase its accuracy. In some cases, information on individuals who are placed on or removed from probation may not be correctly identified in the system for up to a month. State law requires probation departments to submit this data within 30 days of a probation status change, and certain provisions in contracts that some probation departments have with a vendor require only monthly reporting of probation information (the vendor reports information regarding individuals who are on probation to TDCJ on the probation departments' behalf). However, more frequent updates would help ensure that when someone on probation is arrested, their probation officer is notified immediately.

The vendor with which some probation departments contract electronically reports information regarding individuals who are on probation to TDCJ's Community Justice Assistance Division, which then reports the information electronically to TDCJ's Corrections Tracking System and, ultimately, to DPS. TDCJ staff update that agency's system and send the information to DPS on a weekly basis, but because of the delay in probation departments' reporting, the information on some individuals may not be accurate. Therefore, probation officers will not receive flash notices on probationers until the information on those individuals is updated.

The delay presents a problem when a probationer is arrested in another county and his or her probation officer is not notified promptly. When probationers are arrested in the same counties in which their probation officers work, probation officers learn about these arrests because they regularly review jail bookings.

TDCJ has improved the Flash Notice System by implementing recommendations from the December 2001 State Auditor's Office audit of CJIS. Specifically, TDCJ now captures incident tracking numbers and sends flash notices only to the specific office in which the probationer or parolee is under supervision.

Recommendations

TDCJ should:

- Consider requesting that probation departments update information on probationers' status more frequently than once per month.
- Use the information from the probation departments to update its system on a daily basis.
- Periodically reconcile the data in the Corrections Tracking System with DPS's Computerized Criminal History system data to identify any records that may not have been updated.

Management's Response

- *TDCJ agrees, and will review the timeliness of updated information to determine if more frequent submissions will be beneficial to the system. Target date: May 1, 2006*
- *TDCJ agrees, and will work with DPS to initiate a process for daily updates for Flash Notice reporting. Target date: February 1, 2007*
- *TDCJ agrees, and will work with DPS to initiate a process for periodically reconciling the Flash and ER5 data. Target date: February 1, 2007*

Appendices

Appendix 1

Objective, Scope, and Methodology

Objective

The audit objective was to determine whether controls over data in the Criminal Justice Information System (CJIS) provide reasonable assurance that data in this system is complete, accurate, and timely.

Scope

The audit scope included data in CJIS from December 2001 to December 2005, as well as the controls over the data.

Methodology

The audit methodology consisted of conducting interviews; collecting and reviewing information; and performing tests, procedures, and analyses against predetermined criteria for the Texas Department of Public Safety (DPS) and the Texas Department of Criminal Justice (TDCJ) relating to CJIS.

Information collected and reviewed included the following:

- Interviews with management and staff of DPS, TDCJ, the Community Justice Assistance Division, and the Department of Information Resources
- Documentary evidence such as:
  - Policies and procedures for DPS and TDCJ
  - Applicable state and federal statutes and guidelines
  - Prior reports from the State Auditor's Office and the Criminal Justice Policy Council
  - Internal audit reports from DPS and TDCJ

Procedures, tests, and analyses conducted included the following:

- Tested the entire population of the Community Supervision Tracking System to determine whether the data used to track offenders were complete and accurate.

- Tested the entire population of the Flash Notice System to determine whether information for all individuals on probation and parole was correctly flagged in the Computerized Criminal History system.

- Tested data from the Corrections Tracking System to the Computerized Criminal History system to ensure that the data was complete and accurate.

- Analyzed DPS's name-searchable database to determine the number and age of records included in the database.

- Analyzed DPS's return file to determine the number of records and the age of the data.

- Analyzed data provided by DPS to determine the number of "misraps" that were identified, resolved, and consolidated for fiscal year 2005.

- Tested a random sample of individuals with access to the Computerized Criminal History system to determine what access levels they were assigned.

- Tested and analyzed a random sample of DPS's secure Web site user list to determine whether:

  - Secure site users were still active users and employed by their current entities.

  - Entities and users had signed agreements as required by DPS.

  - There were users who were not listed on the list of active secure site users provided by DPS.

- Analyzed the DPS disaster recovery plan to determine whether it contained the required or recommended provisions needed to bring DPS back online in the event of a disaster or data processing disruption.

- Analyzed the contract between DPS and its fingerprinting vendor to determine whether the contract contained the required or recommended provisions needed to protect the State's interests.

- Visited the Holliday Unit (intake facility) located in Huntsville, Texas, to observe and document TDCJ's intake processes.

Criteria used included the following:

- Texas Code of Criminal Procedure, Chapter 60

- Title 37, Texas Administrative Code (TAC), Part 1, Chapter 27, Subchapters A and H
- Title 1, TAC, Part 10, Sections 202.24 and 202.25
- Texas Government Code, Chapter 411, Subchapter F
- Texas Government Code, Chapter 499
- Title 28, Code of Federal Regulations, Parts 20 and 22
- The Federal Bureau of Investigation's *Criminal Justice Information System Security Policy*
- Department of Information Resources' *Business Continuity Planning Guidelines*
- Texas Building and Procurement Commission's *State of Texas Contract Management Guide*, Version 1.1
- House Bill 967 (79th Legislature, Regular Session)
- DPS's and TDCJ's internal policies and procedures

Project Information

Auditors conducted fieldwork from August 2005 through December 2005. This audit was conducted in accordance with generally accepted government auditing standards. The following members of the State Auditor's staff performed this audit:

- Sandra Q. Donoho, MPA, CISA, CIA, CFE (Project Manager)
- Wei Wang, MSAS, MSCS, CIA, CPA (Assistant Project Manager)
- Nicole Elizondo
- Tracy Gilliam, MA
- Juan R. Sanchez, MPA, CGAP
- Sherry Sewell, CGAP
- Phatsavinh B. Somsith
- Leslie Ashton, CPA (Quality Control Reviewer)
- Nicole Guerrero, MBA, CGAP (Audit Manager)

Appendix 2

Access to CJIS

Chapter 411 of the Texas Government Code specifies what kinds of entities are allowed access to CJIS and what levels of access they have. Specifically, the entities and positions that may access CJIS are listed below.

Entities and Positions with Access to CJIS	
▪ Criminal Justice Agencies	▪ Texas Department of Mental Health and Mental Retardation[6]; Local Authorities; Community Centers
▪ State Board for Educator Certification[1]	▪ Organization Providing Certain Nurse Aides
▪ Texas Alcoholic Beverage Commission	▪ Texas Rehabilitation Commission[2]
▪ Banking Commissioner	▪ Employer at Residential Dwelling Project
▪ Texas Department of Licensing and Regulation	▪ Applicants for Employment - In Home Service Companies, Residential Delivery Company
▪ Institution of Higher Education	▪ Commercial Nuclear Power Plant Licensees
▪ Consumer Credit Commissioner	▪ Texas Commission on Private Security [7]
▪ Texas Racing Commission	▪ County Judge; Certain Applicants
▪ School District, Charter School, Private School, Regional Education Service Center, Commercial Transportation Company, or Education Shared Services Arrangement	▪ Adjutant General
▪ Texas School for the Blind and Visually Impaired	▪ Texas Appraiser Licensing and Certification Board
▪ Texas Commission for the Blind[2]	▪ Texas Board of Architectural Examiners
▪ Texas State Board of Medical Examiners[3]	▪ State Board of Barber Examiners[8]
▪ Board of Law Examiners	▪ Texas Board of Chiropractic Examiners
▪ State Bar of Texas	▪ Texas Cosmetology Commission[8]
▪ Texas Structural Pest Control Board	▪ State Board of Dental Examiners
▪ McGruff House Program	▪ Texas Board of Professional Engineers
▪ Child Watch Program	▪ Texas Funeral Service Commission
▪ Texas Workforce Commission	▪ Texas Board of Professional Geoscientists
▪ Texas State Board of Public Accountancy	▪ Texas Department of Health[4]
▪ Texas Department of Insurance	▪ Texas State Board of Examiners of Dietitians[4]
▪ Receiver	▪ Texas State Board of Examiners of Marriage and Family[4]
▪ Texas Lottery Commission	▪ Midwifery Board[4]
▪ Comptroller of Public Accounts	▪ Texas State Board of Examiners of Perfusionists[4]
▪ Texas Department of Health[4]	▪ Texas State Board of Social Worker Examiners[4]
▪ Texas Commission on Alcohol and Drug Abuse[4]	▪ State Board of Examiners for Speech-Language Pathology and Audiology[4]
▪ District Court; Name Changes	▪ Advisory Board of Athletic Trainers[4]
▪ Commission on Law Enforcement Officer Standards and Education	▪ State Committee of Examiners in the Fitting and Dispensing of Hearing Instruments[4]
▪ Texas School for the Deaf	▪ Texas Board of Licensure for Professional Medical Physicists[4]
▪ Texas Commission for the Deaf and Hard of Hearing[2]	▪ Texas Board of Orthotics and Prosthetics[4]
▪ Department of Protective and Regulatory Services[5]	▪ Texas Board of Professional Land Surveying
▪ Texas Youth Commission	▪ Texas Commission on Environmental Quality
▪ Interagency Council on Early Childhood Intervention[2]	▪ State Preservation Board
▪ Agencies Operating as Part of Medical Assistance Program	▪ Texas Board of Physical Therapy Examiners

Entities with Access to CJIS	
▪ Texas Board of Occupational Therapy Examiners	▪ Texas Optometry Board
▪ Texas State Board of Pharmacy	▪ Domestic Relations Office
▪ Texas State Board of Plumbing Examiners	▪ County Commissioners' Courts; County Child Welfare Board Members
▪ Texas State Board of Podiatric Medical Examiners	▪ Employment by Municipality
▪ Polygraph Examiners Board	▪ Employment by County
▪ Texas State Board of Examiners of Psychologists	▪ Employment by Appraisal District
▪ Texas Real Estate Commission	▪ Crime Victims' Institute
▪ Board of Tax Professional Examiners	▪ Safe Houses
▪ Texas Department of Transportation	▪ State Auditor
▪ State Board of Veterinary Medical Examiners	▪ Regional Tollway Authorities
▪ Board of Vocational Nurse Examiners[9]	▪ Texas State Library and Archives Commission
▪ Texas Department of Housing and Community Affairs	▪ Public
▪ Secretary of State	▪ Certain Hospitals and Hospital Districts
▪ State Fire Marshal	▪ Texas Juvenile Probation Commission
▪ Texas Education Agency	▪ Juvenile Board or Juvenile Probation Department
▪ Department of Agriculture	▪ Savings and Loan Commissioner
▪ Municipal Fire Department	▪ Court Clerk; Guardianships
▪ Volunteer Fire Departments	▪ Facility, Regulatory Agency, or Private Agency
▪ Texas Commission on Fire Protection	▪ Interagency Council on Sex Offender Treatment[4]
▪ County Fire Marshals	▪ State Securities Board
▪ Political Subdivisions; Public Transportation Drivers	▪ State Commission on Judicial Conduct
▪ Volunteer Centers	▪ Programs Providing Activities for Children
▪ Applicants for Employment and Contractors	▪ State Agencies; Information Technology Employees
▪ Person Seeking to Adopt Child	

[1] Services consolidated under the Texas Education Agency

[2] Services consolidated under the Department of Assistive and Rehabilitative Services

[3] Name changed to the Texas Medical Board

[4] Services consolidated under the Department of State Health Services

[5] Services consolidated under the Department of Family and Protective Services

[6] Mental health services consolidated under the Department of State Health Services; mental retardation services consolidated under the Department of Aging and Disability Services

[7] Services consolidated under the Department of Public Safety

[8] Services consolidated under the Department of Licensing and Regulation

[9] Services consolidated under the Board of Nurse Examiners

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable David Dewhurst, Lieutenant Governor, Joint Chair
The Honorable Tom Craddick, Speaker of the House, Joint Chair
The Honorable Steve Ogden, Senate Finance Committee
The Honorable Thomas "Tommy" Williams, Member, Texas Senate
The Honorable Jim Pitts, House Appropriations Committee
The Honorable Jim Keffer, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

Public Safety Commission

Mr. Ernest Angelo, Jr., Chairman
Mr. Carlos H. Cascos, Member

Department of Public Safety

Colonel Thomas A. Davis, Jr., Director

Texas Board of Criminal Justice

Ms. Christina Melton Crain, Board Chairperson
Mr. Adrian A. Arriaga
Mr. Oliver J. Bell
Mr. Greg S. Coleman
Ms. Patricia A. Day
Reverend Charles Lewis Jackson
Mr. Tom Mechler
Mr. Pierce Miller
Mr. Leopoldo Vasquez III

Texas Department of Criminal Justice

Mr. Brad Livingston, Executive Director