Table of Contents

Table of Contents

Key Points Of Report

An Audit Report on the Assessment of the Criminal Justice Information System

April 1996

Overall Conclusion

The Criminal Justice Information System (CJIS), the State's summary information system on criminal offenders, is not fully implemented and has control weaknesses that affect data quality. Also, the process used to identify criminal backgrounds for prehiring purposes is ineffective because criminal histories in other states are not routinely searched. CJIS affects public safety through decisionmaking by users such as law enforcement agencies, employers, state leaders, and others.

Key Facts and Findings

- At the Texas Department of Criminal Justice (TDCJ), the agency has not met statutory requirements for completed development of its part of CJIS, the Corrections Tracking System (CTS). Required information on 260,000 probationers is not included as part of CJIS. Recent studies indicate a significant risk that information provided by CTS is not complete, accurate, and timely. Although the Legislature has required TDCJ to report on evaluation of CTS by December 1, 1996, the agency lacks completed plans to resolve a history of automation problems that affect CTS.

- At the Texas Department of Public Safety (DPS), the Computerized Criminal History (CCH) system, the DPS portion of CJIS, is implemented, improving, and in fundamental compliance with statutory requirements. However, weaknesses in controls at DPS indicate the risk that criminal history information on arrests, prosecutions, and court decisions may not be complete, accurate, and timely until controls are strengthened.

- The quality of information in CJIS is affected by limited accountability of local criminal justice agencies that originate the data. DPS is dependent upon the cooperation of local governmental entities to provide timely, accurate, and complete data.

Contact

Charlie Hrncir, CPA, Audit Manager (512) 479-4700

Office of the State Auditor

Lawrence F. Alwin, CPA

This audit was conducted in accordance with Government Code, § 321.0133, and Code of Criminal Procedure, Article 60.02(j).

Executive Summary

Overall, the Criminal Justice Information System Is Not Fully Implemented, and Weaknesses in Controls Indicate the Risk That Information Is Not Complete, Accurate, and Timely

As a result of incomplete implementation and control weaknesses, a risk exists that information on 260,000 probationers, 71,500 parolees, 127,100 inmates, and 3,400,000 criminal histories may not be complete, accurate and timely. Incomplete implementation and lack of plans represent significant concerns involving the Texas Department of Criminal Justice (TDCJ). For the Department of Public Safety (DPS), corrective actions to improve and protect information are more readily attainable.

The process used to identify criminal backgrounds for prehiring purposes is ineffective because criminal histories in other states are not routinely searched. The quality of Criminal Justice Information System (CJIS) information affects public safety through decision making by CJIS users such as law enforcement agencies, employers, state leaders, and others.

The performance of CJIS-related responsibilities by individual local government entities is not publicly evaluated. Without adequate public accountability, poor compliance with statutory requirements for providing complete, accurate, and timely information is likely to go undetected and uncorrected. Local governmental entities, such as police departments, district attorneys, and court clerks, are the original source of most of the criminal history information.

The Texas Department of Criminal Justice Has Not Completed Implementation of its Corrections Tracking System and Lacks Completed Plans to Resolve a History of Automation Problems

Information systems on probationers are not complete and operating as part of the Corrections Tracking System (CTS). Statutes mandated a CTS completion date of January 1, 1993, an implementation delay of approximately three years. The Criminal Justice Policy Council commented on this problem in January 1995: "In other words, the state does not know the basic demographic and criminal characteristics of approximately 260,000 offenders on direct community supervision." CTS consists of eight major components (subsystems), seven of which are implemented, and provides the information for the TDCJ portion of CJIS involving an estimated 260,000 probationers, 71,500 parolees, and 127,100 inmates.

What is the Criminal Justice Information System?

CJIS is intended to provide state-of-the-art offender tracking information for operational use, policy analysis, and strategic planning. TDCJ is responsible for the Corrections Tracking System, which should maintain prisoner, parolee, and probationer information. DPS is responsible for the Computerized Criminal History system, which contains information on arrests, prosecutions, and court decisions. These two systems, and the link between them, define the Criminal Justice Information System.

TDCJ lacks comprehensive, documented plans to resolve a history of automation problems that affect CTS systems and data quality.

Reports by an outside consultant, prior State Auditor's Office reports, and other state agencies indicate a history of automation problems during the 1990s. A March 1995 consultant's report cited several weaknesses, concluding that "(t)his has caused the reliability of the automated data to become suspect."

The DPS Component of CJIS Is Operating and Improving with Time, but Weaknesses in Controls Increase the Risk That Criminal History Information May Not Be Complete, Accurate, and Timely

The DPS component of CJIS, the Computerized Criminal History (CCH) system, is operating and in place. DPS is improving its information gathering process and has effective controls that primarily address data accuracy.

Data completeness has improved over several years. In the first analysis of data completeness conducted in 1987 by the Criminal Justice Policy Council, only 32 percent of arrests had a disposition (outcome) recorded. In 1993, this improved to 43 percent as indicated by a U.S. Department of Justice survey. The Council will update their study in a 1996 report.

However, as a result of some weaknesses, existing strengths are diminished, and DPS cannot provide assurance that criminal history information is complete and timely. Confidence in data accuracy is compromised by risk of unauthorized changes.

Controls should be improved to minimize the risk of unauthorized modification of criminal history data. Inappropriate access to information systems compromises existing controls that otherwise protect criminal history information and creates the risk of unauthorized changes in criminal history data. For example, programming staff (application and system programmers) have unrestricted, and therefore inappropriate, access to live production programs and production data. This may result in unauthorized changes that may not be detected. This affects CJIS-related data and has an overall impact on all DPS information systems.

Controls related to completeness, accuracy, and timeliness of data quality are not fully in place. For example, deletions of records are not subject to independent review by others, and identification of individuals who create and modify criminal history records is not preserved in an audit trail for more than seven days within the CCH database.

Summary of Management's Responses

TDCJ management's summary response (complete responses at page 28):

The Auditors' observations relative to the incompleteness of the Corrections Tracking System are accurate. The CTS consists of three modules: prisoner information, parolee information, and probationer information. The probation module is not yet complete and on-line. Although this module, known as the Community Supervision and Tracking System, was begun at the same time as the other two, completion has been hindered by several, often repetitive factors. The system is scheduled for placement into production on May 15, 1996.

This integral part of the CJIS will provide statistical material for administrative and legislative review, as well as, much needed information to local criminal justice entities.

In order for the Agency to maintain an accurate, useful, integrated criminal justice information system, all employees of the Texas Department of Criminal Justice will be made aware of the importance of data integrity, and their role in ensuring data quality. Incorrect or erroneous data in the computer not only impacts their department, but the entire criminal justice system within the state of Texas, as more and more users begin to depend on that data to perform their duties. All decisions made utilizing the data available within CJIS are the shared responsibility of those individuals that create and maintain the records.

TDCJ will consider an educational program to make its employees aware of the seriousness of their positions. Staff in all divisions and at all levels of the organization, from executives to senior management to administrative and support staff, from line supervisors to field office staff should be informed that their input into the system carries such gravity. This information, as well as better documentation concerning data entry and integrity within each department, would spur all system users to be conscientious of the impact of their performance.

DPS management's summary response (complete responses at page 35):

Regarding lack of controls, your report contains a number of valid findings and some valuable recommendations, which our agency intends to implement. I believe the overall value of the report is diminished, however, by your overstatement of the negative implications of lack of controls.

Specifically, while the findings regarding potential unauthorized modification of data may be technically accurate, it is highly unlikely that anyone could have traversed the numerous boundaries to have actually changed any data in the criminal history file. Security enhancements will be made to address this issue, but your report does not accurately inform the reader as to the highly improbable nature of any such unauthorized access actually having occurred. The security of the computerized criminal history information is a great concern to the DPS.

We believe that we are on the right course with the management of the Computerized Criminal History file, especially in our combined efforts with the Criminal Justice Policy Council encouraging electronic reporting. However, we realize that it will require additional time and resources for the Computerized Criminal History file and the Criminal Justice Information System to achieve an optimal level of timeliness, completeness, and accuracy.

Auditor's follow-up comment to Department of Public Safety management summary response, above

It is difficult to quantify the risk of unauthorized access or unauthorized changes to criminal history information. Because of the impact of CJIS information on public safety, *reducing the opportunity* to make unauthorized changes to data or by otherwise protecting information integrity through better controls is important. (See examples in Appendix 4, Table 1.)

Summary of Audit Objective and Scope

The objective of this audit was to provide an assessment of CJIS by determining its status and by evaluating controls related to completeness, accuracy, and timeliness of data quality. The scope included CJIS-related activities at TDCJ and DPS. The scope at TDCJ was limited primarily to determining status. At DPS, evaluation of controls, as well as status, was possible due to the greater extent of implementation than at its counterpart at TDCJ. In a separate report in 1996, the Criminal Justice Policy Council will publish its evaluation of the data within CJIS.

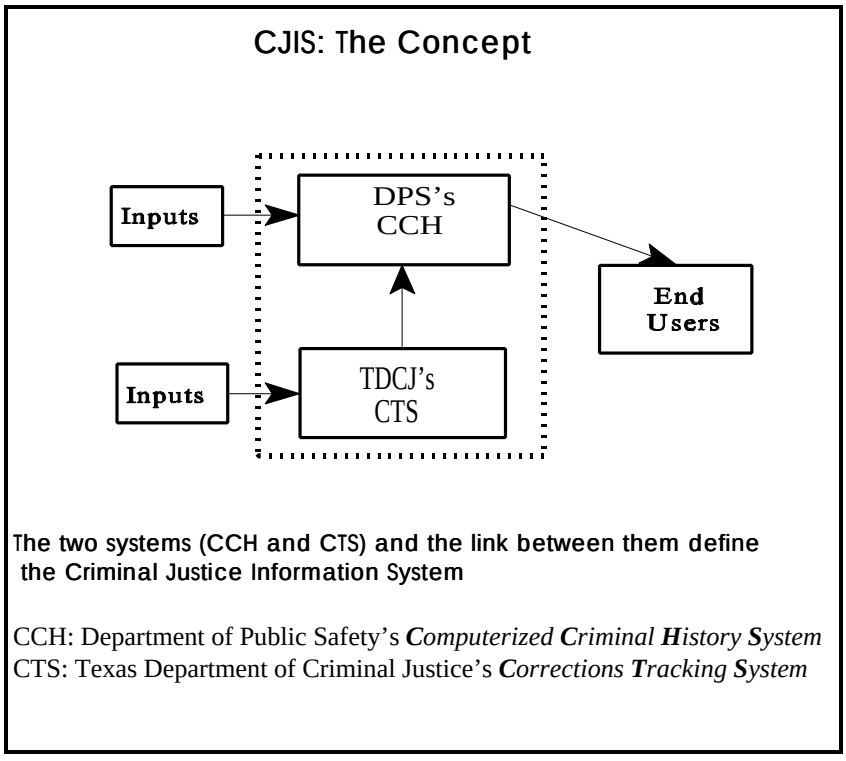
Overall, the Criminal Justice Information System Is Not Fully Implemented, and Weaknesses in Controls Indicate the Risk That Information Is Not Complete, Accurate, and Timely

As a result of control weaknesses and incomplete implementation, a risk exists that information on 260,000 probationers, 71,500 parolees, 127,100 inmates and 3,400,000 criminal histories may not be complete, accurate, and timely. The quality of this information affects decision making by CJIS users such as law enforcement agencies, employers, state leaders, and others.

- The Corrections Tracking System (CTS), the Texas Department of Criminal Justice's (TDCJ) portion of CJIS, is not fully implemented as required by statute. A history of automation problems, coupled with a lack of documented solutions, indicates a risk of continued statutory noncompliance in providing criminal offender information, particularly for probationers.

- The Computerized Criminal History (CCH) system, the Texas Department of Public Safety's (DPS) portion of CJIS, has been implemented for more than two years. CCH is improving and is in fundamental compliance with statutory requirements. However, weaknesses in controls at DPS indicate a risk that criminal history information on arrests, prosecutions, and court decisions may not be complete, accurate, and timely until controls are strengthened.

Figure 1



What is the Criminal Justice Information System?

CJIS is intended to provide state-of-the-art offender tracking information for

strategic planning (Figure 2, page 6). TDCJ and DPS have operational

administering respective parts of CJIS (Figure 3, page 7). TDCJ is responsible for

should maintain prisoner, parolee, and probationer information (Figure 4, page

Computerized Criminal History system, which contains information on arrests,

page 18). These two systems and the link between them define the Criminal Justice

The U.S. Department of Justice illustrates the importance of criminal history records by recognizing that data quality is emerging as one of the most important and timely issues confronting the criminal justice community. There is a direct relationship between high quality criminal history record information and the effectiveness of the criminal justice system in Texas and nationally.

Weaknesses in controls over CJIS can adversely impact the criminal justice system. The quality of criminal history records can affect the following types of criminal justice decisions:

- police officer requests to obtain search and arrest warrants
- prosecutor decisions to charge individuals based in part on prior criminal history
- judicial decisions to grant or deny bail or to sentence a convicted offender

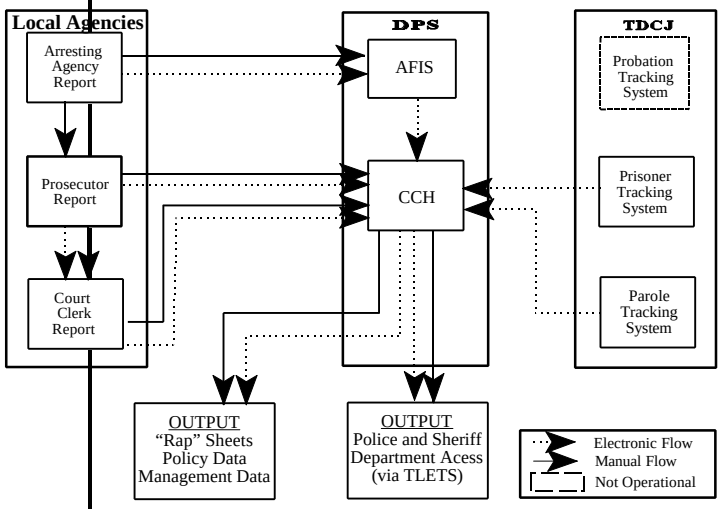
Figure 2

Potential Users of CJIS

CJIS is intended to provide state-of-the-art offender tracking information for operational use, policy analysis, and strategic planning

Figure 3

Texas' Criminal Justice Information System
Flow of Information



TDCJ and DPS have operational responsibility for developing and administering respective parts of CJIS

Section 1-A:

Quality of Information in CJIS Is Affected by Limited Accountability of Local Criminal Justice Agencies That Originate the Data

Without adequate public accountability, poor compliance with statutory requirements for providing complete, accurate, and timely information is likely to go undetected and uncorrected. DPS is dependent upon the cooperation of local governmental entities to provide timely, accurate, and complete data. Local governmental entities, such as police departments, district attorneys, and court clerks, are the original source of most of the criminal history information.

Enabling statutes place joint responsibility on both DPS as well as each local criminal justice agency for data quality for criminal history information:

- Each local criminal justice agency is responsible for compiling and maintaining records for reporting data required by DPS and for cooperating with DPS so that DPS can perform its duties.

- DPS has the overall responsibility for recording data and maintaining a database for a computerized criminal history system for the State.

- DPS has statutory responsibility to develop, by rule, reporting procedures to ensure that criminal history data is reported completely.

The following weaknesses contribute to limited public accountability of local criminal justice agencies:

- Information provided by local governmental entities is not measured for timeliness using statutory standards. State law generally requires arrests to be reported not later than the seventh day after an arrest, and dispositions of arrests shall be reported promptly but not later than after 30 days.

- DPS has not adopted operational benchmarks which could serve as measurable targets for data accuracy. Texas' statutes require accurate criminal history records, but do not define a specific accuracy requirement.

- DPS has not adopted policies which could emphasize and clarify the responsibility for data completeness between DPS and local reporting entities. In the absence of written understandings for data quality, the risk is greater that DPS and local agencies will defer responsibilities to the other, resulting in data quality problems. For instance, we noted that DPS does not review output (individual criminal histories called "rap" sheets) for completeness or accuracy. Ordinarily, rap sheets are mailed to the local agency for this review. However, several local agencies have requested that rap sheets should not be mailed, and DPS suppresses printing of this output. As a result, neither DPS nor the local agency is reviewing rap sheets for accuracy and completeness.

DPS has taken specific steps to improve overall data quality through training of and cooperation with local users. DPS also created a field service representative program to assist local users in improving completeness, accuracy, and timeliness of data.

Recommendation:

To improve accountability of local criminal justice agencies, we recommend that DPS:

- Track submitting agency compliance (local users) with statutory timeliness requirements and share performance information with local users on a monthly basis.

- Establish benchmarks for data accuracy, and periodically evaluate performance with benchmarks. Provide the Criminal Justice Policy Council with information on completeness, accuracy, and timeliness of CCH data in the aggregate and by local reporting entity for annual publication for the Legislature.

- Define DPS policy which clearly articulates the relative responsibilities and authority between DPS and local users in terms of timeliness, accuracy, and completeness.

TDCJ Management's Response:

In order to reduce redundancy in criminal justice reporting by local governments,

efforts are underway which will allow information submitted to DPS to update the Corrections Tracking System directly, instead of being re-submitted. Any steps taken by DPS to ensure the accuracy and dependability of the data prior to "sharing" it with TDCJ will only enhance the value of the data.

DPS Management's Response:

Regarding timeliness, accuracy, and completeness
While stating the need for greater public accountability for the timeliness, accuracy, and completeness of the data, your report does not adequately describe the history of the creation of CJIS as a state mandate, placed upon local reporting entities without state funding. By definition, the legislature created the DPS portion of CJIS, that is, the Computerized Criminal History file (CCH), as a statewide repository of data submitted by local agency contributors. The role of the DPS is to establish and manage the system in such a manner that enables and encourages submissions, while at the same time enforcing uniformity. Timeliness, accuracy, and completeness are measures of the performance of the reporting agencies. Given the statutory definition of CCH, and being mindful that the mandatory reporting of criminal history data adds to the long list of state requirements placed upon already overburdened local reporting entities, the DPS set upon a course of encouragement and assistance rather than enforcement and administrative sanctions--there are no statutory sanctions. We have expressed this same position to your agency in the past.

It is our firmest belief that the timeliness, accuracy, and completeness of criminal history data will best be achieved through the electronic submission of data from local contributors' computers to our own. As you are aware, the effort to provide local reporting entities resources to convert to electronic submission of data has been a major initiative of the DPS and the Criminal Justice Policy Council, through the use of federal funds. To respond directly to your recommendation, we will develop an improved monitoring process to keep local agencies informed of their data reporting. This effort will be implemented in concert with the efforts of our field service representatives. In addition, we will provide reporting data to the Criminal Justice Policy Council, upon their request, and we are preparing formalized rules.

Section 1-B:

Continuing, Long-Term Strategic Planning Would Benefit CJIS

No state agency has clearly defined responsibility for long-term, strategic planning for CJIS, although all involved agencies continue to contribute at some level to planning:

- The Criminal Justice Policy Council (Council) completed a one time, statutorily required strategic implementation plan for CJIS. The Council issued its report as of December 31, 1991.
- DPS and TDCJ are required by statute to develop biennial plans to improve the reporting and accuracy of CJIS with advice from the Council and the Department of Information Resources. This requirement focuses more on operational aspects, not including long-term planning, in order to comply with statutory requirements.

Lack of a vision in the form of a strategic plan can diminish the effectiveness of overall, long-term CJIS performance. Opportunities for long-term improvement of CJIS may go unrecognized and may not be achieved. In addition, changes to the system may be more expensive than necessary without appropriate long-term planning for CJIS needs. Opportunities to plan for compliance with changing federal mandates may be missed.

Recommendation:

TDCJ and DPS should contribute to a biennial strategic planning process led by the Criminal Justice Policy Council patterned after the 1991 effort.

TDCJ Management's Response:

TDCJ agrees with this recommendation. During the initial development of CJIS, staff from DPS and TDCJ met weekly in order to thoroughly plan and implement an integrated, analogous system. DPS participated in portions of the detail design phase of the Corrections Tracking System. Both agencies sent representatives to participate in legislatively mandated, quarterly "local meetings" to inform interested parties across the state of the progress of the CJIS and implementation schedules and requirements.

DPS Management's Response:

Regarding a statewide strategic planning effort
Your recommendations regarding the need for a more formalized statewide CJIS strategic planning function are valuable in that the system can benefit from a more formal process. Your report suggests, however, that upon our current path we might miss opportunities for improving CCH and we might not keep up with advancing federal mandates. In fact, the DPS, the Criminal Justice Policy Council, and the Criminal Justice Division of the Governor's Office have combined to stay well ahead of opportunities and mandates. Through cooperative planning, these state agencies have funneled more than $4 million in federal funds to the local agency contributors to enable their county data processing systems to electronically report court dispositions to DPS. In addition, the DPS and the Criminal Justice Policy Council, through a joint planning effort, have recently developed a plan to place "live scan" fingerprinting devices in approximately 30 arresting agencies throughout the state and to provide those agencies funds with which to upgrade their computer systems. This effort will allow these agencies to submit arrest data electronically to CCH. In October, the federal government approved $4.9 million for Texas for this purpose--the largest award in the nation.

While you are suggesting that we might miss opportunities and mandates, you fail to mention that, through cooperative planning, we have taken advantage of every opportunity available and are preparing for federal mandates. In the absence of state

money, the cooperating state agencies have tapped into federal resources to greatly enhance local agencies' reporting abilities, and to lay the groundwork for interfacing Texas with the FBI's planned nationwide Automated Fingerprint Identification System.

(Auditor's Note: The Council, along with DPS, the Governor's Office, and the Department of Information Resources, have been successful in obtaining more than $8.9 million in incremental federal funding in response to statutory requirements to develop and adopt a grant program.)

Section 2: CJIS ISSUES AT THE TEXAS DEPARTMENT OF CRIMINAL JUSTICE (TDCJ)

Texas Department of Criminal Justice Has Not Completed Implementation of its Corrections Tracking System and Lacks Completed Plans to Resolve a History of Automation Problems

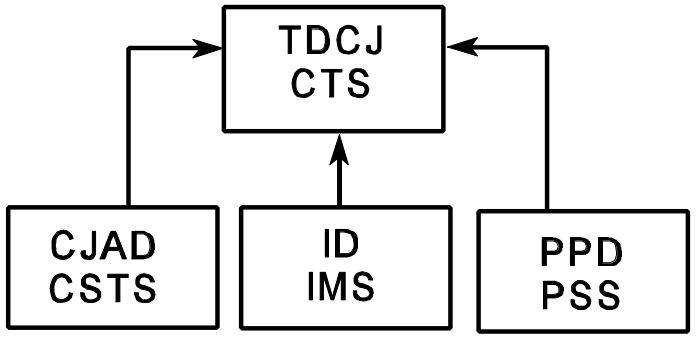
CJAD - Community Justice Assistance Division
Community Supervision Tracking System (CSTS for 260,000 probationers)

ID - Institutional Division
Inmate Management System (IMS for 127,100 inmates)

PPD - Pardon and Parole Division
Parole Supervision System (PSS for 71,500 parolees)

Figure 4

Texas Department of Criminal Justice's Corrections Tracking System (CTS)



TDCJ is responsible for the Corrections Tracking System, which should maintain prisoner, parolee, and probationer information

The scope at TDCJ was limited primarily to evaluating implementation status and corrective action plans. This limitation was due to known overall weaknesses in systems and data identified in previous studies. Controls related to completeness, accuracy, and timeliness of data quality were not evaluated as was done at DPS.

Section 2-A:

Statutorily Required Information Systems on Probationers Are Not Complete and Operating as Part of CTS

Information systems on probationers are not complete and operating as part of CTS. Statutes mandated a CTS completion date of January 1, 1993, an implementation delay of approximately three years. The Criminal Justice Policy Council commented on this problem in January 1995: "In other words, the state does not know the basic demographic and criminal characteristics of approximately 260,000 offenders on direct community supervision." CTS consists of eight major components (subsystems), seven of which are implemented, and provides the information for the TDCJ portion of CJIS, involving an estimated 260,000 probationers, 71,500 parolees, and 127,100 inmates.

Recommendation:

We recommend TDCJ complete CTS information systems related to probationers to fulfill statutory requirements for CJIS.

TDCJ Management's Response:

The probation portion of the Corrections Tracking System, the Community Supervision and Tracking System (CSTS) is not in production at this time. Implementation of the system in pilot form is planned for May 15, 1996 and will be completed in phases (see attached time line, page 34). Reasons for the extensive timeline are many, (i.e. changes in management, changes in project team members, and a lack of dedicated resources), and will be presented in TDCJ's report to the Legislature that was prescribed in House Bill 269.

Section 2-B:

TDCJ Lacks Documented Plans to Resolve a History of Automation Problems

Written plans to address identified automation problems are not complete. During the last three years, reports by an outside consultant, the State Auditor's Office, and other state agencies indicate a history of automation problems. Weaknesses include:

- Lack of written plans, as of October 31, 1995, to implement a consultant's March 1995 recommendations to improve fundamental business processes prior to improving automation capabilities. The consultant cited several weaknesses, concluding "(t)his has caused the reliability of the automated data to become suspect."

- Two State Auditor reports in 1993 indicated weaknesses in both data and automation planning at TDCJ.[1]

- Other agencies indicate automation problems at TDCJ:

  - The Criminal Justice Policy Council, a CJIS user, describes TDCJ's automation as "years behind . . . in its technology and data quality" in a comparison with DPS in comments made in the Council's June 1995 newsletter.

  - The Department of Information Resources (DIR) disapproved TDCJ plans related to CJIS on June 14, 1995, due to a lack of available information. Subsequently, DIR issued a letter dated October 16, 1995, citing TDCJ for noncompliance with statutory requirements related to automation projects.

Current inadequacies in the Corrections Tracking System at TDCJ are due to a variety of complex reasons, including:

- Lack of effective, long-term, automation planning involving agency-wide needs.

- Lack of Data Services personnel resources dedicated to the data processing function. Only 69 percent of authorized employee positions are filled which contributes to overall ineffectiveness of Data Services.

- Lack of an effective methodology involving the system design, development, and maintenance process for major systems development projects.

Shortcomings in TDCJ data adversely affect the ability of CJIS to meet statutory requirements that include:

- allowing criminal justice system modeling

- conducting analyses of proposal legislative changes in the criminal justice system

- analyzing overall the functioning of the criminal justice system

As a result, TDCJ cannot provide assurance that criminal offender information on prisoners, probationers, and parolees in CJIS is complete, accurate, and timely. Instead, TDCJ continues reliance on existing but inefficient and costly information systems, including manual systems. Thus, CJIS users, such as law enforcement personnel, district attorneys, and probation officers, may not have complete and

---

[1]The reports referred to are (1) *The Verdict on Probation: Its Effectiveness is Unknown* (SAO Report No. 3-037, February 1993) and (2) *Texas Lacks Effective Controls for Developing Automated Information Systems* (SAO Report No. 3-038, February 1993).

accurate information on suspects and criminal offenders through CJIS. This may lead policy and operational users to develop independent, alternative information systems at additional cost.

The Legislature is requiring TDCJ to report by December 1, 1996, with an evaluation of the Corrections Tracking System, including reporting requirements, accountable divisions, and a time line for implementing an automated Corrections Tracking System.

Recommendation:

We recommend that TDCJ:

- Expand its 1996 report to the Legislature to include the proximate causes for the delay so that corrective action can be taken, and include sources of and justification for resources required to complete CJIS automation. TDCJ should include a follow-up report one year from the date of its original report to the Legislature.

- Comply with statutory requirements involving the Department of Information Resources.

- Address human resources problems affecting Data Services' effectiveness.

- Improve long-term automation planning for the agency as a whole, including adoption of an appropriate system design, development, and maintenance methodology for major systems development projects. For development of major automation projects, Data Services should provide automation and project management skills to complement user departments that should take ownership responsibility for project management.

TDCJ Management's Response:

Regarding "TDCJ lacks documented plans to resolve a history of automation problems"

According to the auditor's report, "Written plans to address identified automation problems are not complete." One of the cited "weaknesses" refers to Andersen Consulting's March, 1995 recommendations that fundamental business processes be improved prior to improving automation capabilities. The consultant was addressing the lack of real time processing specifically referring to the in-processing of offenders, of the Diagnostic Intake Process. This observation was made, and documented, in 1991 in the Diagnostic Intake Processing Analysis. Due to staffing shortages, and budgetary restraints, most of the recommendations made in the analysis have never been implemented. However, TDCJ is currently working on restructuring the existing database to improve data integrity and response time.

Additionally, real-time inmate strength reporting is currently undergoing analysis. The Inmate Strength Reporting System is a batch system and updated on a daily basis. The resulting information is utilized to update almost every offender management system used by the department. This modification will end the existing problem of real-time data in every system currently utilized, except the Diagnostic Intake Process, where data entry relative to offenders occurs days after the data is collected. The change to the Strength System will provide this area with opportunities to make its functions real-time, and allow data entry at the point of collection.

Andersen Consulting's report stated:

> *"Computer automation of these tasks will only deliver "automated complexity" and the business and economic expectations would not be achieved. Our recommendations address the streamlining and simplification of business process around the introduced technology."*

Clearly, the consultants meant that the business processes used within TDCJ should be reviewed for modification and streamlining prior to the automation of those processes. TDCJ shares this position, and has formed a Re-engineering Steering Committee to perform a review of business operations throughout the Agency for efficacy and efficiency. The findings of the Steering Committee will be utilized to determine the appropriateness of developing automation to improve the execution methods of various functions.

The auditor's report quotes the Criminal Justice Policy Council as describing TDCJ's automation as "years behind...in its technology and data quality" in a comparison with DPS. It should be noted that Dr. Fabelo, Executive Director of CJPC, made this statement to support his suggestion that TDCJ would benefit from federal funding to enhance its automated system, in the same way that DPS did. The entire statement reads:

> *"A cohesive, long-term strategy funded by the federal government to improve CCH records in the state is already paying-off in terms of better information to track criminals in Texas. Clearly, a similar initiative will benefit the state's correctional tracking system at TDCJ. This system is years behind the CCH system in its technology and data quality."*

TDCJ supports Dr. Fabelo's intentions, as funding to design, implement, and maintain CTS has never been forthcoming.

Regarding the recommendation to expand TDCJ's report to the Legislature

TDCJ concurs with this recommendation, and the inclusion to the report will be made. Follow up reports will be prepared annually at the request of the Legislature or at the direction of TDCJ administration.

Regarding the recommendation to comply with statutory requirements for DIR

TDCJ concurs with this recommendation. The statutory requirement referred to is the Information Services Biennial Operating Plan which was prepared by TDCJ Data Services and submitted to the Department of Information Resources for approval on November 21, 1995.

Regarding the recommendation to address human resources problems affecting Data Services

For the past few years, Data Services has experienced numerous problems in hiring and maintaining adequate staff to fulfill its function. As the auditor's report stated, only 69% of authorized employee positions are filled at this time. Although the severity of the staffing shortage varies by department, this problem is systemic throughout the Agency. Two reasons for this problem are:

1. Limitations on Office Space - The Agency has grown to gargantuan proportions since its creation by legislation in 1989. The number of incarcerated offenders has grown five-fold within that time period, necessitating the construction of new confinement facilities. Construction and operating costs for those facilities are priority items within the TDCJ budget. Support staff throughout the Agency have suffered increased workloads and dwindling office space as additional positions have been created. The Agency is addressing this problem and procuring additional buildings and offices as quickly as possible. The addition of space will allow the recruitment and hiring of new staff.

2. Non-Competitive Salary Levels for Technical Expertise - The Agency's salary scale for senior level technical staff is not always competitive with the salary ranges offered by private industry. This phenomena is shared with every state operated agency, as the stock holders in these agencies are taxpayers rather than share holders. The inability to compensate experienced engineers, attorneys, medical staff and computer staff, as well as other technical staff, is a burden endured state-wide and necessitates the hiring of less experienced personnel who are then trained in-house. Once these staff members reach the level of expertise necessary to provide insightful, technological leadership within the Agency, they are often underpaid for their qualifications and may well seek employment elsewhere.

Regarding the recommendation to improve long term automation planning

TDCJ concurs with this recommendation. Data Services presently utilizes a Systems Development Life Cycle (SDLC) that was developed in-house utilizing industry standards. The existing SDLC is currently under revision within the Data Services Department to incorporate recommendations noted in this audit as well as the change in Agency philosophy regarding automation. The SDLC provides step-by-step guidelines for the design, development, and implementation of automated systems. Data Services staff receive training on utilization of the SDLC. However, the user departments have received little or no training regarding on utilization of the SDLC. TDCJ, via the Data Services Department, will create a training curriculum for all user

departments within the agency on the utilization of the SDLC for systems development projects. This course will be presented to each department's designated liaison for automation. A management overview will also be presented to ensure that all Agency staff understand and follow the appropriate development steps, providing the agency with the most thorough analyses of both processes and expenditures relative to automation.

Project management software has been evaluated and a product selected. Procurement of this software is currently underway. A position has been created and filled within the Data Services Department to oversee the implementation and proper utilization of this product.

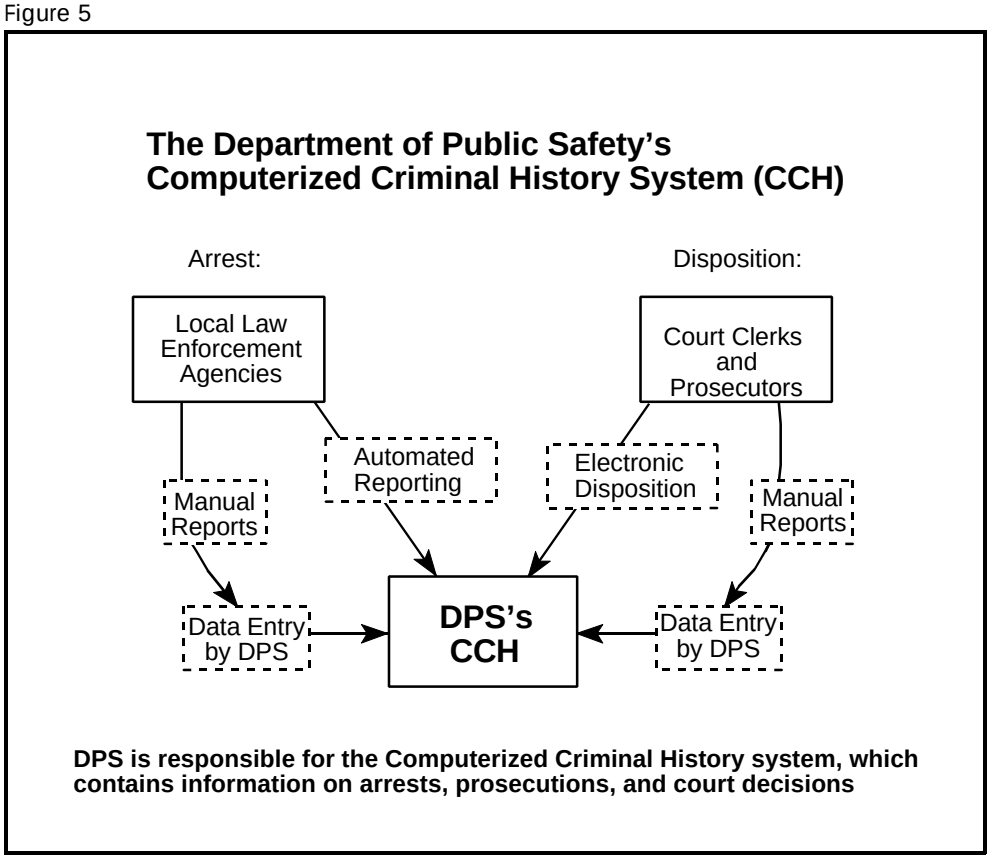
TDCJ concurs with the auditor's recommendations concerning project ownership responsibility and encourages and supports all user departments' vital participation, input, and leadership relative to automation projects.

Section 3: CJIS ISSUES AT THE TEXAS DEPARTMENT OF PUBLIC SAFETY (DPS)

The DPS Component of CJIS Is Operating and Improving with Time, but Weaknesses in Controls Increase the Risk That Criminal History Information May Not Be Complete, Accurate, and Timely

At DPS, evaluation of controls related to CJIS was possible due to the greater extent of implementation than at its counterpart at TDCJ. As with TDCJ, we evaluated the overall status of CJIS at DPS. (In a separate report in 1996, the Criminal Justice Policy Council will publish its evaluation of the data within CJIS.)

Figure 5



Section 3-A:

The DPS Component of CJIS Is Operating, and Data Quality Is Improving

The Computerized Criminal History (CCH) system, which is the DPS component of CJIS, is operating and in place. DPS is improving its information gathering process and has some effective controls for data accuracy. The following sampling of controls protect CJIS-related information systems:

- Fingerprints initiate the recording of arrest information which aids in subsequent identification of criminal histories and helps ensure that arrest information is authentic.
- Numerous automated edit checks help to validate critical data fields once information is included in the system.
- Automated search procedures are used to identify duplicate transactions for correction.
- All on-line inquiries by CJIS users requesting criminal history information are logged to allow follow-up.
- A team of CJIS field representatives serves as the DPS liaison with local

government users in order to improve the overall process.

Data completeness has improved over several years. In the first analysis of data completeness, conducted in 1987 by the Criminal Justice Policy Council, only 32 percent of arrests had a disposition (outcome) recorded. In 1993, this improved to 43 percent as indicated by a U.S. Department of Justice survey. The Council will update their study in a 1996 report.

The findings that follow involve recommendations to improve CJIS-related controls at DPS.

Section 3-B:

Controls Should Be Improved to Minimize the Risk of Unauthorized Modification of Criminal History Data, and to Further Improve Overall Data Quality

We identified control weaknesses related to access to criminal history information and overall data quality in terms of completeness, accuracy, and timeliness:

- Inappropriate access to information systems compromises the integrity of existing controls that otherwise protect criminal history information and creates the risk of unauthorized changes in criminal history data. This affects CJIS-related data and DPS information systems overall.

- Controls related to completeness, accuracy, and timeliness are not fully in place. For example, deletions of criminal history records are not subject to independent review by others, and identification of individuals who create and modify criminal history records is not preserved in an audit trail for more than seven days within the CCH database.

As a result of control weaknesses, existing control strengths are diminished, and DPS cannot provide assurance that criminal history information is complete and timely. Confidence in data accuracy is compromised by risk of unauthorized changes.

DPS is in the process of drafting written policies addressing the security for access to automated resources. Written policies will strengthen access controls overall. However, until sufficient preventive access controls are implemented, security weaknesses related to access will continue to affect DPS information systems overall.

Recommendations:

We recommend that DPS strengthen controls to minimize risk of unauthorized modification of data for all DPS systems and also strengthen those controls that

provide for completeness, accuracy, and timeliness of CCH data. Detailed weaknesses and recommendations related to access controls and data quality are included in

Appendix 4, Tables 1 and 2 (pages 55, 59).

DPS Management's Response:

Regarding lack of controls
Your report contains a number of valid findings and some valuable recommendations, which our agency intends to implement. I believe the overall value of the report is diminished, however, by your overstatement of the negative implications of lack of controls. Specifically, while the findings regarding potential unauthorized modification of data may be technically accurate, it is highly unlikely that anyone could have traversed the numerous boundaries to have actually changed any data in the criminal history file. Security enhancements will be made to address this issue, but your report does not accurately inform the reader as to the highly improbable nature of any such unauthorized access actually having occurred.

The security of the computerized criminal history information is a great concern to the DPS. We limit direct connections to our system almost exclusively to law enforcement agencies, who place a high value on the data we provide. In a related issue, the agency has not authorized access to the INTERNET through any device that is connected to the DPS host computer. In addition, our programmers go through an extensive background investigation prior to employment. These are steps we take beyond the electronic access checks that protect the systems and data.

Auditor's Follow-up Comment:

We share DPS' concern with the security of the computerized criminal history information and agree that security enhancements can be made to address this issue. It is difficult to quantify the risk of unauthorized access or unauthorized changes to criminal history information. Improvements in controls by DPS (examples are in Appendix 4, Table 1) can lessen the risk of unauthorized access from both internal and external means.

Section 3-C:

DPS Should Improve its Disaster Recovery Plan

The disaster recovery plan for DPS has a potentially slow recovery time, a significant omission, and other weaknesses. The importance of disaster recovery is expressed in rules adopted in the Texas Administrative Code by the Department of Information Resources for all Texas state agencies:

> "Automated information and information resources residing in the various agencies of state government are strategic and vital assets belonging to the people of Texas. These assets require a degree of protection commensurate with their value. The expense of security safeguards must be appropriate to the value of the assets being protected. In the event a disaster or catastrophe disables information processing and related telecommunications functions, the ability to

continue critical governmental services must be assured. Information resources must be available when needed."

The ability of DPS to recover its automation capabilities overall has a direct impact on its ability to continue providing information through its CCH system. The weaknesses noted include:

- DPS has selected a potentially slow disaster recovery time of up to 14 days. Faster restoration of automation capabilities would help avoid life-threatening situations to DPS officers and protect against degradation in DPS services.

- The Automated Fingerprint Identification System (AFIS) is not included within a disaster recovery plan. AFIS is the backbone of CCH, using fingerprints to provide effective automated identification of individuals.

- The disaster recovery plan focused on involvement by the data processing department, but minimized user involvement.

Recommendations:

We recommend that DPS improve its disaster recovery plan. Detailed weaknesses and recommendations related to disaster recovery are included in Appendix 4, Table 3, page 61.

DPS Management's Response:

Regarding disaster recovery
The agency has worked diligently to prepare a disaster recovery plan that covers a worst case scenario in a straightforward manner. Enumeration of all known possibilities in a worst-case scenario would probably not be accurate and would be impossible to fund. Accordingly, the agency has selected a practical approach that meets the needs of the state, in a fiscally responsible manner.

Section 3-D:

System Design, Development, and Maintenance Procedures Lack Consistency

Control weaknesses exist in DPS' overall system development, design, and maintenance procedures. These weaknesses include:

- DPS does not follow consistent system development procedures to ensure that systems are developed in a cost-effective manner for all user areas. Instead, each area determines how a system will be developed and managed. Some user areas determine how systems will be developed and managed in conjunction with Data Processing Services, while other user areas make these

determinations independently without input from Data Processing Services. Overall system development is also complicated by the large variety of systems, hardware, and software in use by DPS.

- DPS has minimal project management tools to manage and monitor the time and cost of project development.

  A comprehensive, overall system development methodology for DPS involving participation of users and internal audit would help ensure the cost-effective development of automated systems which also meets users' needs. A formalized system development process, if enforced, could ensure that effective controls, realistic requirements, timely completion, proper system documentation, and cost-effective maintenance and enhancement are attained.

  A steering committee with agency-wide authority could be established to guide the direction of and ensure the effective use of data processing resources. This committee should ensure that plans and priorities established for the data processing function are consistent with the agency's overall mission, plans, and objectives.

Without a formal methodology and steering committee that has an agency perspective, management cannot be assured of uniform acceptable quality in the development of new systems and the modification of existing systems. The opportunity to provide strengths through controls in a centralized fashion is likely to be missed. Best practices of some user departments may not be identified for sharing with other departments. Deficiencies in system development by departments may not be identified in a timely manner for correction. DPS is at greater risk of delays in implementation, cost overruns, and developed systems that do not fully meet needs and expectations.

Controls over system development, design, and maintenance should include the establishment of agency priorities, standards, and documentation requirements for the following aspects of system development:

- analysis of cost alternatives
- planning
- project managing and monitoring
- user and internal audit involvement
- quality assurance
- maintenance and enhancements of existing systems
- post-implementation reviews

Recommendation:

We recommend that DPS establish an agency-wide steering committee and methodology to ensure user areas adhere to important system design, development, and maintenance controls for data processing.

DPS Management's Response:

Regarding system design and development
We recognize that design and development procedures can always be improved; however, we do not believe that this issue is relevant to the DPS portion of CJIS. The CCH file is developed and is now in maintenance. We continue to make ongoing improvements in our design and development methodology, but lack of resources limits our solution possibilities in this regard.

Auditor's Follow-up Comment:

System design and development controls directly impact all of DPS systems, whether in development or maintenance. Improvements made now in controls in this area can benefit future developments involving CJIS enhancements as they occur.

Section 4:
Other Issues

Section 4-A:
Criminal Background Check Process Is Ineffective Because it Does Not Identify Complete Criminal Histories

Two types of searches use DPS' CCH database: prehiring background checks and periodic searches involving persons with professional licenses. DPS refers to this process as criminal history inquiries for non-criminal justice agencies. Texas school districts, child care facilities, nursing homes, and state agencies rely on this process to identify individuals having criminal histories. The process is ineffective because:

- Only criminal histories in Texas (not including the 49 other states) are searched.

- Most prehiring background checks use identification methods (i.e., names, date of birth, sex, and race) that are considered unreliable by the U.S. Department of Justice due to risk of counterfeiting. While more effective searches using fingerprints may be available, they involve a significantly higher cost. (DPS usually charges $1 per name to conduct searches based on names, date of birth, sex, and race. Costs would increase to almost $40: $15

  for a Texas' records only fingerprint search, plus the FBI charges an additional $24 for a nationwide fingerprint search.)

- Searches that compare professional licensees with DPS' criminal history records are considered effective because fingerprints are used to identify criminal records. However, this process also identifies *only* Texas criminal histories, not those of other states.

Some requesting agencies and other users may not understand or be aware of the limitations of the search process if fingerprints are not used, or if only criminal histories in Texas are searched. DPS attempts to disclose shortcomings in a disclaimer provided to those entities requesting criminal searches, but the disclaimer does not indicate that only Texas records are searched.

As a result, school districts, child care centers, nursing homes, and others are at risk of hiring individuals with undisclosed criminal histories. Also, licensees are held accountable only for criminal behavior occurring in Texas. In fiscal year 1995, DPS records indicate 970,476 criminal history name inquiries were made for non-criminal justice agencies. Most searches are for prehiring background checks. The primary users (70 percent of all name inquiries) were school districts, Department of Human Services (nursing homes), and Department of Protective and Regulatory Services (child-care related).

Improving this process is complex and requires additional study considering many factors, including:

- Increased transaction costs to use fingerprints to identify individuals.
- Use and cost of constantly improving technology such as paperless, "live scanning" fingerprint devices to improve the process.
- Federal considerations, such as approval to access federal fingerprint files, and completion (now underway) of a national database for this purpose.
- Data processing capacity of DPS and the FBI to handle increased searches by fingerprint.

Recommendation:

We recommend DPS present alternative solutions, including costs and benefits, for the Legislature to consider in improving the effectiveness of criminal history searches for non-criminal justice agencies.

We also recommend that DPS amend its disclaimer notice to agencies that request criminal information to mention that criminal histories in other states, if any, may not be included in this search process.

DPS Management's Response:

Regarding access to federal records for non-criminal justice purposes
This is an important issue that becomes rather complicated, and can cause confusion. The following comments are submitted only for the purpose of clarification.

Access to federal criminal records for non-criminal justice purposes is allowed only

under the following federal conditions:

- *A state law exists authorizing the access to the FBI's records;*
- *The FBI has approved the state law for such access;*
- *The records are disseminated only to governmental agencies;*
- *The requests are made by fingerprint card submission to FBI through DPS;*
- *The requester pays a $24 federal fee.*

Unless we meet those conditions, the FBI will not allow access to the nationwide criminal history records for non-criminal justice purposes. Of course, access to Texas criminal records is totally under the authority of the Texas Legislature. Currently, for noncriminal justice purposes this includes:

- *State law authority must exist (almost exclusively Chapter 411 , Government Code, Subchapter F, for third-party entities, and the Texas Open Records Act, for access by the record subject himself or herself);*
- *The records are disseminated to the entities identified in the law, including private entities;*
- *The requests may be made by fingerprint card, letterhead request (including name, sex, race, and date of birth) or electronically, including the same identifiers;*
- *Most requesters pay a fee, as follows:*
  - *$ 15 statutory fee per name for inquiries by fingerprint card*
  - *$ 10 statutory fee per name for inquiries on letterhead*
  - *$ 1 statutory fee per name for inquiries by magnetic means*
  - *$ 17.25 fee for inquiries by personal review (under Open Records Act)*

The interrelationship between the means of access to the Texas records and the means of access to the FBI records must be kept in mind when discussing use of the federal records. Although many private entities would like access to the federal records, and many governmental entities would like to access the federal records by name/sex/race/DOB rather than by fingerprint card, the FBI has been steadfast in its resistance to such changes. Such changes are subject to the future will of the U. S. Congress; however, recent sessions have reaffirmed the current policies. For example, the Oprah Winfrey Bill, while encouraging broad access to the records, did not relax the current requirements.

In addition, once a governmental agency has been granted access to the FBI records, they must elect to take advantage of that access. Funding and time constraints prompt licensing agencies to submit magnetic tapes to DPS at $1 per name--and not search the FBI records--rather than to cause their applicants to be fingerprinted and submit those fingerprint cards to DPS for forwarding to FBI with a federal fee of $24 each. If they were to process fingerprint cards through DPS, as well, that would be an additional statutory charge of $15 each.

The search by fingerprint card greatly increases the chances of finding a criminal record on a person who used a fictitious name at the time of arrest, or is using a fictitious identity to apply for a job or a license. A great increase in the number of applicant fingerprint cards processed by DPS would require an enhancement to the

Automated Fingerprint Identification System.

Auditor's Follow-up Comment:

DPS now also processes concealed hand gun applications. This application process uses fingerprints, with criminal background checks made using both state and federal databases.

Section 4-B:

Texas Should Consider the Benefits of Selling Conviction Data to the Public

Selling data on Texas convictions could raise funds to improve CJIS at both state and local levels. The future effectiveness of CJIS will in part be dependent on adequate funding for improved automation capabilities at the local level.

For example, for every one percent of the Texas workforce that could generate a such a background check, $1.1 million additional revenues could be raised at $15 per search.[2] This information would include only conviction information, not arrest and prosecution information already available to noncriminal justice agencies for background search purposes.

At present, most local agencies do not have efficient, electronic reporting capabilities, instead relying on manual processes. Current plans will fund electronic reporting capability for only 75 percent of arrests, prosecutions, and court dispositions from local criminal justice agencies.

To date, funding for the criminal justice information system has largely been provided by either local funds or federal funds. The Criminal Justice Policy Council, in conjunction with the Governor's Office, has been instrumental in obtaining more than $8.9 million in incremental federal funding in the 1990s. Federal funding has allowed local agencies to improve automation capabilities that otherwise would not have occurred.

Four of the ten most populated states (Florida, Illinois, Pennsylvania, and Michigan) sell conviction data to the public. However, in Texas there are some statutory prohibitions against making public any data on criminal histories maintained by DPS. Ironically, conviction data is already a matter of public record for each individual case at the local level.

Other states charge fees for summary conviction information based on the type of search conducted. Searches using names, race, sex, and date of birth for identification range in cost from $5.00 to $15.00 dollars per search request. A more effective search

[2] Estimated on 1994 Texas employment of 7,711,000 x one percent x $15 = $1,156,650.

using fingerprints ranges in cost from $14.00 to $50.00 per search.

Additional study is required to address policy considerations of selling conviction information as well as whether anticipated revenues would off set increased DPS automation costs to handle these requests.

Recommendation:

We recommend that DPS, in cooperation with the Criminal Justice Policy Council, develop a proposal addressing anticipated revenues and expenses related to selling conviction data to the public, including statutory provisions that need amendment, to fund CJIS improvements at the state and local level.

Appendix 1:

Objectives, Scope, and Methodology

Objectives

The audit objectives were to:

- Evaluate and report on controls relevant to the timeliness, accuracy, and completeness of the Criminal Justice Information System involving the Texas Department of Criminal Justice (TDCJ) and the Texas Department of Public Safety (DPS).

- In a separate report, provide assistance to the Criminal Justice Policy Council in completing its mandated data quality examination of the Criminal Justice Information System.

Scope

At the Texas Department of Criminal Justice, the audit involved limited fieldwork consisting of reviewing plans to complete and improve the Corrections Tracking System (CTS). TDCJ is required to present a CTS status report to the Legislature on or before December 1, 1996. We determined the status of TDCJ's CTS by examination of existing reports, review of existing TDCJ's plans, and interviews to confirm our understanding.

At the Texas Department of Public Safety, the audit focused on controls surrounding the Computerized Criminal History (CCH) system. The scope at DPS included information management controls and considered policy and performance management controls as they apply to this system.

The consideration of DPS' information management controls, as they relate to CCH, included a review of:

- agency-wide data processing general controls, involving access, computer operations, physical security, and system design development and maintenance

- application controls specifically related to input, processing, and output of CCH data

The consideration of DPS policy and performance management controls, as they relate to CCH, included a review of:

- strategic planning, organizational structure, and significant policies and procedures

- performance measures, program evaluation of CCH, and quality control/assurance procedures

Methodology

The methodology for the first objective of this audit consisted of collecting information, performing audit tests and procedures, analyzing the information, and evaluating the information against established criteria. We will complete the second objective by conducting and reporting separately the results of a survey of CJIS users.

Information collected to accomplish our objective included the following:

- Interviews with management and staff of TDCJ and DPS
- Enabling legislation (Chapter 60, Code of Criminal Procedure)
- Agency documents and memoranda

Tests and procedures conducted:

- Completion of standardized EDP internal control questionnaires
- Physical inspection and observation of facilities
- Observation of procedures performed
- Tests of selected controls to determine existence and effectiveness

Analytical techniques:

- Evaluation of adequacy of TDCJ plans to complete automation of CTS
- Identification of existing controls in each applicable area
- Evaluation of the adequacy of controls that provide reasonable assurance that DPS is fulfilling its role in CJIS

Criteria used:

- State Auditor's Office Management Control Methodology
- State Auditor's Office Accountability Project Methodology (general and specific)
- Other standards and criteria developed through research (see Reference List - Appendix 3)

Other Information

Fieldwork was conducted from July 27 through October 13, 1995. The audit was performed in accordance with applicable professional standards, including generally accepted government auditing standards. There were no significant instances of a noncompliance with these standards.

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

- Carleton S. Wilkes, CPA (Project Manager)
- Teresa Menchaca, CDP
- Matthew Osburn
- Beverly Wood, CPA
- Carol Noble, CISA (Quality Control)
- Charlie Hrncir, CPA (Audit Manager)
- Deborah L. Kerr, Ph.D. (Audit Director)

Appendix 2:

Background Information

Texas' Criminal Justice Information System (CJIS) is a criminal records database that serves the needs of law enforcement, prosecutors, courts, and corrections personnel throughout Texas. It also provides a source of information for policymakers to evaluate the functioning of the criminal justice system, as well as a means to conduct non-criminal background checks for licensing or employment purposes. The Computerized Criminal History (CCH) system, the Corrections Tracking System (CTS), and the electronic link between them define CJIS.

Without complete, accurate, and timely information, there is a substantial risk that a decisionmaker will make an incorrect or misguided decision. As a result, criminal history records often directly determine the effectiveness of a criminal justice system in serving and protecting the public.

The 71st Legislature made sweeping changes in Texas' criminal justice records system. These changes were codified as Chapter 60 of the Code of Criminal Procedure in 1989. Chapter 60 outlines and defines CJIS and assigns responsibility for the system:

- The Texas Department of Public Safety is responsible for recording data and maintaining the CCH system.
- The Texas Department of Criminal Justice is responsible for recording data and maintaining the CTS database.
- The Criminal Justice Policy Council is responsible for looking at the "big picture" in Texas criminal justice and providing decisionmakers with credible, accurate, practical, and nonpartisan information. The Council works with DPS, TDCJ, and counties to design and implement CJIS.

According to the U.S. Department of Justice, criminal history records are critical to every phase of the administration of criminal justice. For example, records may:

- Determine if a police officer can obtain an arrest or search warrant.
- Influence a prosecutor's decision to formally charge an individual.
- Be a critical element in a judge's decisions on bail and sentencing.

Appendix 3:

Reference List

Andersen Consulting. *TDCJ Offender Information Management Reengineering Project.* Houston, Texas, May 1995.

State of Illinois. Illinois Criminal Justice Information Authority. *A Comprehensive Examination of the Illinois Criminal History Records Information (CHRI) System.* Chicago, Illinois, August 1995.

State of Texas. Criminal Justice Policy Council. *Texas Criminal Justice Information System: Recommendations for System Improvements for the 1994-1995 Biennium.* Austin, Texas, September 1992.

_____. Criminal Justice Policy Council. *National Criminal History Improvement Program: Grant Application for the State of Texas.* Austin, Texas, June 1995.

_____. Criminal Justice Policy Council. *Criminal Justice Records Improvement Plan for the State of Texas*. Austin, Texas, July 1992.

_____. Criminal Justice Policy Council. *Strategic Implementation Plan for the Texas Criminal Justice Information System (CJIS)*. Austin, Texas, December 1993.

_____. Criminal Justice Policy Council. *Biennial Report to the Governor and the 74th Texas Legislature, The Big Picture Issues in Criminal Justice*. Austin, Texas, January 1995.

_____. Criminal Justice Policy Council. *Agency Plan for Information Resources.* Austin, Texas, March 1995.

_____. Criminal Justice Policy Council. *Review of Federal-State-Local Partnerships to Improve the Information to Track Criminals in Texas.* Bulletin from the Executive Director, Number 15. Austin, Texas, June 1995.

_____. General Services Commission. *Report on Charges for Public Records by State Agencies.* Austin, Texas, November 1993.

_____. Legislative Budget Board. *Staff Performance Report to the 74th Legislature, Planning and Utilization of Scheduled Prison Capacity*. Austin, Texas, January 1995.

_____. State Auditor's Office. *An Audit Report on the Implementation of State Auditor's Office Recommendations*. Austin, Texas, SAO Report No. 95-016, October 1994.

_____. State Auditor's Office. *Texas Lacks Effective Controls for Developing*

Automated Information Systems. Austin, Texas, SAO Report No. 93-038, February 1993.

_____. State Auditor's Office. *Tough Choices: Finding Ways to Balance Criminal Justice Policy and Criminal Justice Dollars - A Review*. Austin, Texas, SAO Report No. 93-124, May 1993.

United States. U.S. Department of Justice. Bureau of Justice Statistics. *Use and Management of Criminal History Record Information: A Comprehensive Report.* Washington, D.C., November 1993.

_____. U.S. Department of Justice. Bureau of Justice Statistics. *Survey of Criminal History Information Systems, 1993.* Washington, D.C., 1993.

_____. U.S. Department of Justice. Bureau of Justice Statistics. *Assessing Completeness and Accuracy of Criminal History Records Systems: An Audit Guide*. Washington, D.C., January 1992.

_____. Office of the Federal Register. *Code of Federal Regulations 28, Parts 0 to 42*. Washington, D.C., July 1, 1995.

Appendix 4:

Detail Recommendations to Improve Controls at DPS

Figure 6

Table 1 - Controls should be improved to minimize the risk of unauthorized modification of criminal history data (page 19)		
Weakness	Recommendation	*DPS Management Response* ***Overall*** *- Unless otherwise noted, all changes will be implemented as resources permit.*
1. Programming staff (application and system programmers) has unrestricted, and therefore inappropriate, access to live production programs and production data.	1. Change programming staff responsibilities to avoid access to live production programs and production data.	*1. Programming staff must have access to data and programs to do their jobs. Problems arise, even in the production environment, that require very quick resolution because law enforcement personnel rely on our information 24 hours-a-day, 7 days-a-week. We are in the process of implementing Top Secret, which provides an additional layer of security and monitoring. We have invested resources in background checks on our personnel, and we believe that, at some point, we must trust the individual programmers.* Auditor's Follow-Up Comment: Programmers with update access to live production data create the risk of unauthorized data changes. This is a fundamental weakness in segregation of duty control.
2. Data entry supervisors have inappropriate access to criminal history data which includes the combined ability to set up user ID's and also add, change, and delete criminal history records.	2. Eliminate data entry supervisors' ability to modify and delete criminal history data, or to set up users' access capabilities.	*2. The nature of data entry supervisor's duties requires their having the ability to modify and delete data. We will institute a third-party check of deleted records rather than removing this ability from the supervisors. In addition, we will investigate user authorization being assigned by a disinterested party. These changes will be made within 90 days.*

Table 1 - Controls should be improved to minimize the risk of unauthorized modification of criminal history data (page 19)		
Weakness	Recommendation	*DPS Management Response* ***Overall*** *- Unless otherwise noted, all changes will be implemented as resources permit.*
3. AFIS (Automated Fingerprint Identification System) Coordinators and AFIS vendor engineers can set up user ID's and know all passwords. Also, they can add, delete, and change AFIS records of fingerprint data. Access by AFIS engineers is required, but their access is not monitored.	3. Eliminate AFIS Coordinator access to all user passwords. Monitor, and limit where possible, AFIS vendor engineer access to AFIS fingerprint data.	*3. AFIS Operator ID's and Passwords are maintained within the User Authorization File (UAF) which resides within the proprietary NEC host computer. Due to the design of this proprietary system, access to the UAF for additions, modifications and deletions is only via the on-line terminal. By design, users at AFIS workstations cannot access this file to maintain their own passwords. The AFIS Coordinator is responsible for maintenance of the UAF and can change an operator's password upon request when he/she feels his/her password has been compromised. The DPS has discussed this issue with the vendor, and it is clear that the whole password management system would have to be rewritten to accomplish the requested change. The DPS accepts the risk of the AFIS Coordinator managing the passwords.* *The nature of the NEC engineers' work requires the level of access they now enjoy. We will consider other controls to monitor that access.*
4. A large number of individuals with physical access to both the main computer room (160 employees) and AFIS computer room (297 employees) is not justified by daily job responsibilities. Physical access reports are not reviewed by management.	4. Limit physical access to computer rooms to those individuals justified by relevant daily job responsibilities.	*4. The list of individuals with access to the main computer room has been reviewed, and the number will be reduced. The number with access to the AFIS computer room has been reduced to approximately 100. In addition, the AFIS computer room will be physically reconfigured to further limit access to just those computer operators and engineers who need to be in the room. This will be completed by January 1997.*
5. A current, detailed plan to achieve implementation of TOP SECRET (software that provides security controls) by the September 1, 1996, deadline established by the Department of Information Resources does not exist.	5. Develop short-term, detailed plans with time lines to fully implement TOP SECRET.	*5. The implementations of Top Secret is a complicated process. For instance, all file names must be changed to conform to a standard. Various regions must be brought under Top Secret control. The process must be deliberate and careful or dire consequences can occur. We are implementing Top Secret as quickly as we can. The existing timeline will be modified, as appropriate.*

Table 1 - Controls should be improved to minimize the risk of unauthorized modification of criminal history data (page 19)		
Weakness	Recommendation	*DPS Management Response* ***Overall*** *- Unless otherwise noted, all changes will be implemented as resources permit.*
6. Terminated or transferred employees do not have their access capabilities deleted or modified on a timely basis to reflect an updated access status. We identified eight individuals still having access authority with termination dates extending back to April 20, 1995.	6. Eliminate or modify access capabilities of terminated and transferred employees immediately.	*6. Communications have taken place with the Personnel Bureau to speed up the transmission of this information to the persons who can update the files. In addition, local administrators are being established, who will have the ability to delete access for terminated or transferred employees.*
7. Access to all system software is not controlled. Some DPS system software that allows modification of programs and data without an audit trail is not protected from unauthorized access.	7. Monitor access to system software, and restrict access to only appropriate employees after implementation of TOP SECRET.	*7. System programmers must have access to system software to accomplish their responsibilities. Audit trails do exist. These trails will be more complete following the implementation of Top Secret.* Auditor's Follow-Up Comment: Some DPS software does not create an audit trail (such as the DPS version of the utility program generally known as "SUPERZAP"). We do agree that DPS has some audit trails but they are not regularly reviewed. Existing audit trails are not readily available for review, rendering them inaccessible for practical purposes.
8. Access to database information is not adequately protected. Approximately 69 databases are not password protected. This includes 23 databases of the CCH system.	8. Review and increase the extent of password protection for all DPS databases, including those related to CCH.	*8. Access will become more restrictive with the full implementation of Top Secret.*

Table 1 - Controls should be improved to minimize the risk of unauthorized modification of criminal history data (page 19)		
Weakness	Recommendation	*DPS Management Response* ***Overall*** *- Unless otherwise noted, all changes will be implemented as resources permit.*
9. Access by Tower system users to DPS' Model 204 database has a low level of security protection. This could allow unauthorized access to database system commands. As a result, a user with technical knowledge of the system and application-specific knowledge could make undetected changes to CCH data files. This risk is present with over 1,500 accounts (individual and group users, including local authorities such as sheriff's offices).	9. Strengthen access controls over Tower system users to minimize risk of unauthorized data changes.	*9. No evidence was provided that showed that any tower user can make it through a very complicated system to alter data. A person on a tower would have to alter security on the tower by writing a program, have access privileges to Model 204, and be authorized to access the CCH file. The likelihood of this happening is very remote. Local P.D.s and sheriffs access CCH through the TLETS network. There is not direct connection between TLETS and Model 204. The TLETS user cannot use Model 204. The risk in this "weakness" is very close to zero.* Auditor's Follow-up Comment: We identified a former DPS data processing employee with Tower system knowledge and access capability through his consulting work. However, strengthening controls in this area could make this risk in this weaknesses very close to zero.

Figure 7

Table 2 - Controls related to completeness, accuracy and timeliness are not fully in place (page 19)		
Weakness	Recommendation	*DPS Management Response* ***Overall*** *- Unless otherwise noted, all changes will be implemented as resources permit.*
1. Deletions of records are not subject to independent review by others. Supervisors who delete criminal history records also receive the only summary report of deleted records.	1. Have persons independent of the deletion process review reports that summarize deleted criminal history records.	*1. We will institute a third-party check of deleted records. This change will be implemented within 90 days.*
2. A single criminal may have more than one State Identification Number (SID). The consequence of an offender having more than one SID is that criminal history inquiries may not report complete information. DPS recognizes the major causes for multiple SID's and is taking steps to address this concern.	2. Continue current efforts to address causes of, and to correct, multiple SID's in criminal history records.	*2. We are continuing our efforts to limit duplicate SID assignment.*
3. Identification of individuals who create and modify criminal history records is not preserved in an audit trail for more than seven days within the CCH database.	3. Enhance the CCH database to capture the user ID of the person making an original entry or a subsequent record modification.	*3. This change will require major modifications to the CCH system, but we recognize its value, and will include it in the next major system enhancement, if it is feasible.*
4. A control does not exist to ensure that all documents received from local criminal justice agencies are processed. Criminal history records received by mail are not counted for comparison with processed document counts.	4. Compare counts of received and processed documents to help ensure completeness of processing.	*4. Documents processed through AFIS are counted and audited to insure that all are processed. We do not have any evidence that processing of all incoming documents is a problem, and we believe this control would create more work than it would provide benefit. As we move more and more to electronic reporting, this decreases as an issue.*

Table 2 - Controls related to completeness, accuracy and timeliness are not fully in place (page 19)		
Weakness	Recommendation	*DPS Management Response* ***Overall*** *- Unless otherwise noted, all changes will be implemented as resources permit.*
5. Electronic prosecution and court information, which may arrive before arrest data, is not used to identify and request missing arrest information that should normally precede it. Instead, prosecution and court information is not processed but returned as a rejected error. Until arrest information is included for an offender, prosecution or court information cannot be entered into the system.	5. Use prosecution and court information that arrives before arrest information as an indicator of the need to request missing arrest information.	*5. This is an issue brought to our attention by Harris County officials just prior to the audit. We concur that such cross-checking should be done, and we will institute that process.*
6. Criminal history records are not aged individually or in the aggregate to help identify records which have missing information. Identification of "stale records" which are also incomplete is an opportunity to locate potentially missing records.	6. Create reports which identify aged or stale records and conduct appropriate follow-up procedures to identify potentially missing information.	*6. The uncertainty of timeliness in the criminal justice process complicate any straightforward attempts to "age" criminal history records; however, we agree that a broad approach to aging records could find missing data. We will investigate such a program. Of course, the completion of those records will be a function of the local agencies ability to submit the missing data.*
7. Key data entry fields are not verified for accuracy. Data entry errors in fields such as name, race, sex, and date of birth can reduce the effectiveness of searches for criminal history records that rely on these fields to be accurate.	7. Verify data entry of key fields such as name, race, sex, and date of birth.	*7. We have not been able to institute key-verification due to our extraordinary work loads. When the resources permit, we will consider verification of key fields.*

Figure 8

Table 3 - DPS should improve its disaster recovery plan (page 21)		
Weakness	Recommendation	*DPS Management Response* ***Overall*** *- Unless otherwise noted, all changes will be implemented as resources permit.*
1. DPS has selected a potentially slow disaster recovery time of up to 14 days. Faster restoration of automation capabilities would help avoid life-threatening situations to DPS officers and protect against degradation in DPS services.	1. Reconsider the length of acceptable downtime for critical and essential information systems.	*1. The agency has worked diligently to prepare a disaster recovery plan that covers a worst-case scenario in a straightforward manner. Enumeration of all known possibilities in a worst-case scenario would probably not be accurate and would be impossible to fund. Accordingly, the agency has selected a practical approach that meets the needs of the state, in a fiscally responsible manner.*
2. The Automated Fingerprint Identification System (AFIS) is not included within a disaster recovery plan. AFIS is the backbone of CCH, using fingerprints to provide effective automated identification of individuals. In the event of a major disaster (e.g., fires, tornadoes, terrorism, etc.), AFIS would be inoperable for a longer period than if adequate contingency plans were already in place.	2. Include AFIS within the DPS disaster recovery plan.	*2. AFIS will be included within the DPS disaster recovery plan.*
3. AFIS data is backed up every two hours, but data is moved off site only every two weeks. This creates the risk of losing up to two weeks of data before saving data off site. In a two- week period, more than 25,000 records are entered into AFIS.	3. Move AFIS data off site more frequently than every two weeks.	*3. While approximately 25,000 transactions are processed by AFIS within a two week period, only about 40 percent or approximately 10,000 records are registered in the AFIS databases during that two week period. However, DPS agrees with the Auditor's recommendation. The AFIS daily backups will be moved off-site each weekday to reduce the amount of risk, beginning January 16, 1996.*

Table 3 - DPS should improve its disaster recovery plan (page 21)		
Weakness	Recommendation	*DPS Management Response* ***Overall** - Unless otherwise noted, all changes will be implemented as resources permit.*
4. The disaster recovery plan focused on involvement by the data processing department, but minimized user involvement. DPS has established a user liaison group between data processing and users during a recovery, but documentation of user procedures (plans to direct and guide users during disaster recovery) was not included. Users will not know where they will be housed or tasks to perform and, as a result, information needed by the public and law enforcement community may not be available.	4. Involve data processing users to a greater extent in documentation of disaster recovery planning.	*4. Creating detailed procedures and acquiring rented facilities to house 2,000 headquarters personnel in anticipation of a disaster is not considered feasible, and has not been included in our disaster recovery plan. The current industry doctrine is to develop a simple disaster recovery plan with workable action plans. The user liaison team was established with defined responsibilities to assist and guide users during the recovery process. The DPS headquarters complex consists of multiple buildings and "off-site" lease space. In the event of a disaster to one of these buildings, non-office space such as cafeterias, training facilities, and auditoriums, could be converted to office space, if necessary. Based on specific circumstances, the executive management team and the DPS user liaison team will decide where personnel will be housed.*
5. All computer operations employees have not been trained in the use of fire control equipment or in procedures for emergency shut down of data processing equipment for both the AFIS and main computer rooms.	5. Train all computer operations employees in disaster recovery procedures.	*5. Computer operations management in both the main computer room and AFIS computer room will ensure that employees are trained in the use of fire control equipment and emergency shut down procedures for data processing equipment.*

Appendix 4:

Recommendations to Improve Controls

Table 1 - Controls should be improved to minimize the risk of unauthorized modification of criminal history data (page 24)		
Weakness	Recommendation	DPS Management Response **Overall** - Unless otherwise noted, all changes will be implemented as resources permit.
1 Programming staff (application and system programmers) has unrestricted, and therefore inappropriate, access to live production programs and production data.	1 Disallow programming staff to have update access to production programs and production data. Auditor's follow up comment: Programmers with update access to live production data creates the risk of unauthorized data changes. This is a fundamental weakness in segregation of duty control.	1 Programming staff must have access to data and programs to do their jobs. Problems arise, even in the production environment, that require very quick resolution because law enforcement personnel rely on our information 24 hours-a-day, 7 days-a-week. We are in the process of implementing Top Secret, which provides an additional layer of security and monitoring. We have invested resources in background checks on our personnel, and we believe that, at some point, we must trust the individual programmers.
2 Data entry supervisors have inappropriate access to criminal history data which includes the combined ability to set up user ID's and also add, change, and delete criminal history records.	2 Eliminate data entry supervisors' ability to modify and delete criminal history data, or to set up users' access capabilities.	2 The nature of data entry supervisor's duties requires their having the ability to modify and delete data. We will institute a third-party check of deleted records rather than removing this ability from the supervisors. In addition, we will investigate user authorization being assigned by a disinterested party. These changes will be made within 90 days.
3 AFIS (Automated Fingerprint Identification System) Coordinators and AFIS vendor engineers can set up user ID's and know all passwords, and can add, delete, and change AFIS records of fingerprint data. Access by AFIS engineers is required, but their access is not monitored.	3 Eliminate AFIS Coordinator access to all user passwords. Monitor, and limit where possible, AFIS vendor engineer access to AFIS fingerprint data.	3 AFIS Operator ID's and Passwords are maintained within the User Authorization File (UAF) which resides within the proprietary NEC host computer. Due to the design of this proprietary system, access to the UAF for additions, modifications and deletions is only via the on-line terminal. By design, users at AFIS workstations cannot access this file to maintain their own passwords. The AFIS Coordinator is responsible for maintenance of the UAF and can change an operator's password upon request when he/she feels his/her password has been compromised. The DPS has discussed this issue with the vendor, and it is clear that the whole password management system would have to be rewritten to accomplish the requested change. The DPS accepts the risk of the AFIS Coordinator managing the passwords. The nature of the NEC engineers' work requires the level of access they now enjoy. We will consider other controls to monitor that access.

4 A large number of individuals with physical access to both the main computer room (160 employees) and AFIS computer room (297 employees) is not justified by daily job responsibilities. Physical access reports are not reviewed by management.	4 Limit physical access to computer rooms to those individuals justified by relevant daily job responsibilities.	4 The list of individuals with access to the main computer room has been reviewed, and the number will be reduced. The number with access to the AFIS computer room has been reduced to approximately 100. In addition, the AFIS computer room will be physically reconfigured to further limit access to just those computer operators and engineers who need to be in the room. This will be completed by January 1997.
5 A current, detailed plan to achieve implementation of TOP SECRET (software that provides security controls) by the September 1, 1996 deadline established by the Department of Information Resources does not exist.	5 Develop a short term, detailed plans with time lines to fully implement TOP SECRET.	5 The implications of Top Secret is a complicated process. For instance, all file names must be changed to conform to a standard. Various regions must be brought under Top Secret control. The process must be deliberate and careful or dire consequences can occur. We are implementing Top Secret as quickly as we can. The existing timeline will be modified, as appropriate.
6 Terminated or transferred employees do not have their access capabilities deleted or modified on a timely basis to reflect an updated access status. We identified eight individuals still having access authority with termination dates extending back to April 20, 1995.	6 Eliminate or modify access capabilities of terminated and transferred employees immediately.	6 Communications have take place with the Personnel Bureau to speed up the transmission of this information to the persons who can update the files. In addition, local administrators are being established, who will have the ability to delete access for terminated or transferred employees.
7 Access to all system software is not controlled. Some DPS system software that allows modification of programs and data without an audit trail are not protected from unauthorized access.	7 Monitor access to system software, and restrict access to only appropriate employees after implementation of TOP SECRET. Auditor's follow up comment: Some DPS software does not create an audit trail (such as the DPS version of the utility program generally known as "SUPERZAP"). We do agree that DPS has some audit trails but they are not regularly reviewed. Existing audit trails are not readily available for review, rendering them inaccessible for practical purposes.	7 System programmers must have access to system software to accomplish their responsibilities. Audit trails do exist. These trails will be more complete following the implementation of Top Secret.
8 Access to database information is not adequately protected. Approximately 69 databases are not password protected. This includes 23 databases of the CCH system.	8 Review and increase the extent of password protection for all DPS databases, including those related to CCH.	8 Access will become more restrictive with the full implementation of Top Secret.

9 Access by Tower system users to DPS' Model 204 database has a low level of security protection. This could allow unauthorized access to database system commands. As a result, a user with technical knowledge of the system, and application specific knowledge, could make undetected changes to CCH data files. This risk is present with over 1500 accounts (individual and group users including local authorities such as sheriff's offices).	9 Strengthen access controls over Tower system users to minimize risk of unauthorized data changes. <u>Auditor's follow up comment:</u> We identified a former DPS data processing employee, with Tower system knowledge and access capability through his consulting work. However, strengthening controls in this area could make this risk in this weaknesses very close to zero.	9 No evidence was provided that showed that any tower user can make it through a very complicated system to alter data. A person on a tower would have to alter security on the tower by writing a program, have access privileges to Model 204, and be authorized to access the CCH file. The likelihood of this happening is very remote. Local P.D.s and sheriffs access CCH through the TLETS network. There is not direct connection between TLETS and Model 204. The TLETS user cannot use Model 204. The risk in this "weakness" is very close to zero.

Table 2 - Controls related to completeness, accuracy and timeliness are not fully in place (page 24)		
Weakness	Recommendation	DPS Management Response **Overall** - Unless otherwise noted, all changes will be implemented as resources permit.
1 Deletions of records are not subject to independent review by others. Supervisors who delete criminal history records also receive the only summary report of deleted records.	1 Have persons independent of the deletion process review reports that summarize deleted criminal history records.	1 We will institute a third-party check of deleted records. This change will be implemented within 90 days.
2 A single criminal may have more than one State Identification Number (SID). The consequence of an offender having more than one SID is that criminal history inquiries may not report complete information. DPS recognizes the major causes for multiple SID's, and is taking steps to address this concern.	2 Continue current efforts to address causes of, and to correct, multiple SID's in criminal history records.	2 We are continuing our efforts to limit duplicate SID assignment.
3 Identification of individuals who create and modify criminal history records is not preserved in an audit trail for more than seven days within the CCH database.	3 Enhance the CCH database to capture the user ID of the person making an original entry or a subsequent record modification.	3 This change will require major modifications to the CCH system, but we recognize its value, and will include it in the next major system enhancement, if it is feasible.
4 A control does not exist to ensure that all documents received from local criminal justice agencies are processed. Criminal history records received by mail are not counted for comparison with processed document counts.	4 Compare counts of received and processed documents to help ensure completeness of processing.	Documents processed through AFIS are counted and audited to insure that all are processed.We do not have any evidence that processing of all incoming documents is a problem, and we believe this control would create more work than it would provide benefit. As we move more and more to electronic reporting, this decreases as an issue.

5 Electronic prosecution and court information, which may arrive before arrest data, is not used to identify and request missing arrest information that should normally precede it. Instead, prosecution and court information is not processed but returned as a rejected error. Until arrest information is included for an offender, prosecution or court information cannot be entered within the system.	5 Use prosecution and court information that arrives before arrest information as an indicator of the need to request missing arrest information.	5 This is an issue brought to our attention by Harris County officials just prior to the audit. We concur that such cross-checking should be done, and we will institute that process.
6 Criminal history records are not aged individually, or in the aggregate, to help identify records which have missing information. Identification of "stale records" which are also incomplete is an opportunity to locate potentially missing records.	6 Create reports which identify aged or stale records and conduct appropriate follow up procedures to identify potentially missing information.	6 The uncertainty of timeliness in the criminal justice process complicate any straightforward attempts to "age" criminal history records; however, we agree that a broad approach to aging records could find missing data. We will investigate such a program. Of course, the completion of those records will be a function of the local agencies ability to submit the missing data.
7 Key data entry fields are not verified for accuracy. Data entry errors in fields such as name, race, sex, and date of birth can reduce the effectiveness of searches for criminal history records that rely on these fields to be accurate.	7 Verify data entry of key fields such as name, race, sex, and date of birth.	7 We have not been able to institute key-verification due to our extraordinary work loads. When the resources permit, we will consider verification of key fields.

Table 3 - DPS should improve its disaster recovery plan (page 27)		
Weakness	Recommendation	DPS Management Response **Overall** - Unless otherwise noted, all changes will be implemented as resources permit.
1 DPS has selected a potentially slow disaster recovery time of up to 14 days. Faster restoration of automation capabilities would help avoid life threatening situations to DPS officers and protect against degradation in DPS services.	1 Reconsider the length of acceptable downtime for critical and essential information systems	1 The agency has worked diligently to prepare a disaster recovery plan that covers a worst-case scenario in a straightforward manner. Enumeration of all known possibilities in a worst-case scenario would probably not be accurate and would be impossible to fund. Accordingly, the agency has selected a practical approach that meets the needs of the state, in a fiscally responsible manner.
2 The Automated Fingerprint Identification System (AFIS) is not included within a disaster recovery plan. AFIS is the backbone of CCH, using fingerprints to provide effective automated identification of individuals. In the event of a major disaster (e.g. fires, tornadoes, terrorism, etc.), AFIS would be inoperable for a longer period than if adequate contingency plans were already in place.	2 Include AFIS within the DPS disaster recovery plan.	2 AFIS will be included within the DPS disaster recovery plan.
3 AFIS data is backed up every two hours, but data is moved off site only every two weeks. This creates the risk of losing up to two weeks of data before saving data offsite. In a two week period, more than 25,000 records are entered into AFIS.	3 Move AFIS data offsite more frequently than every two weeks.	3 While approximately 25,000 transactions are processed by AFIS within a two week period, only about 40% or approximately 10,000 records are registered in the AFIS data bases during that two week period. However, DPS agrees with the Auditor's recommendation. The AFIS daily backups will be moved off-site each weekday to reduce the amount of risk, beginning January 16, 1996.
4 The disaster recovery plan focused on involvement by the data processing department, but minimized user involvement. DPS has established a user liaison group between data processing and users during a recovery, but documentation of user procedures (plans to direct and guide users during disaster recovery) was not included. Users will not know where they will be housed or tasks to perform, and as a result information needed by the public and law enforcement community may not be available.	4 Involve data processing users to a greater extent in documentation of disaster recovery planning	4 Creating detailed procedures and acquiring rented facilities to house 2,000 headquarters personnel in anticipation of a disaster is not considered feasible, and has not been included in our disaster recovery plan. The current industry doctrine is to develop a simple disaster recovery plan with workable action plans. The user liaison team was established with defined responsibilities to assist and guide users during the recovery process. The DPS headquarters complex consists of multiple buildings and "off-site" lease space. In the event of a disaster to one of these buildings, non-office space such as cafeterias, training facilities, and auditoriums, could be converted to office space, if necessary. Based on specific circumstances, the executive management team and the DPS user liaison team will

5 All computer operations employees have not been trained in the use of fire control equipment or in procedures for emergency shut down of data processing equipment for both the AFIS and main computer rooms.	5 Train all computer operations employees in disaster recovery procedures	5 Computer operations management in both the main computer room and AFIS computer room will ensure that employees are trained in the use of fire control equipment and emergency shut down procedures for data processing equipment.