

Department of Correction

October 2003

Arthur A. Hayes, Jr., CPA, JD, CFE
Director

Charles K. Bridges, CPA
Assistant Director

Elizabeth M. Birchett, CPA
Audit Manager

Dean Smithwick
In-Charge Auditor

Jennifer Cawthon
Bradley Moore, CFE
Iffath Sajid
Suzanne Smotherman, CPA
Staff Auditors

Amy Brack
Editor

Comptroller of the Treasury, Division of State Audit
1500 James K. Polk Building, Nashville, TN 37243-0264
(615) 401-7897

Financial/compliance audits of state departments and agencies are available on-line at
www.comptroller.state.tn.us/sa/reports/index.html.
For more information about the Comptroller of the Treasury, please visit our Web site at
www.comptroller.state.tn.us.



STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY
State Capitol
Nashville, Tennessee 37243-0260
(615) 741-2501

John G. Morgan
Comptroller

October 30, 2003

The Honorable Phil Bredesen, Governor

and

Members of the General Assembly

State Capitol

Nashville, Tennessee 37243

and

The Honorable Quenton I. White, Commissioner

Department of Correction

Fourth Floor, Rachel Jackson Building

320 Sixth Avenue North

Nashville, Tennessee 37243-0465

Ladies and Gentlemen:

Transmitted herewith is the financial and compliance audit of the Department of Correction for the period July 1, 2000, through March 31, 2003.

The review of management's controls and compliance with policies, procedures, laws, and regulations resulted in certain findings which are detailed in the Objectives, Methodologies, and Conclusions section of this report.

Sincerely,

John G. Morgan
Comptroller of the Treasury

JGM/eb
03/042



STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY
DEPARTMENT OF AUDIT
DIVISION OF STATE AUDIT
SUITE 1500
JAMES K. POLK STATE OFFICE BUILDING
NASHVILLE, TENNESSEE 37243-0264
PHONE (615) 401-7897
FAX (615) 532-2765

June 4, 2003

The Honorable John G. Morgan
Comptroller of the Treasury
State Capitol
Nashville, Tennessee 37243

Dear Mr. Morgan:

We have conducted a financial and compliance audit of selected programs and activities of the Department of Correction for the period July 1, 2000, through March 31, 2003.

We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. These standards require that we obtain an understanding of management controls relevant to the audit and that we design the audit to provide reasonable assurance of the Department of Correction's compliance with the provisions of policies, procedures, laws, and regulations significant to the audit. Management of the Department of Correction is responsible for establishing and maintaining internal control and for complying with applicable laws and regulations.

Our audit disclosed certain findings which are detailed in the Objectives, Methodologies, and Conclusions section of this report. The department's administration has responded to the audit findings; we have included the responses following each finding. We will follow up the audit to examine the application of the procedures instituted because of the audit findings.

We have reported other less significant matters involving the department's internal controls and/or instances of noncompliance to the Department of Correction's management in a separate letter.

Sincerely,

Arthur A. Hayes, Jr., CPA,
Director

AAH/eb
03/042

State of Tennessee

Audit Highlights

Comptroller of the Treasury

Division of State Audit

Financial and Compliance Audit
Department of Correction
For the Period July 1, 2000, Through March 31, 2003

AUDIT SCOPE

We have audited the Department of Correction for the period July 1, 2000, through March 31, 2003. Our audit scope included a review of management's controls and compliance with policies, procedures, laws, and regulations in the areas of Internal Audit, contracts, facility visits (petty cash, equipment, purchasing, warehouse and commissary inventory, and payroll), the Inmate Trust Fund Account, the Tennessee Offender Management Information System, and the Financial Integrity Act. The audit was conducted in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

AUDIT FINDINGS

Policies, Procedures, and Operating Controls for TOMIS Are Inadequate*

The department has not implemented adequate operating controls to protect the integrity of the Tennessee Offender Management Information System (TOMIS) data and limit the opportunities for fraud, sabotage, or inappropriate disclosures (page 8).

Ineffective Controls Over Inmate Trust Fund Account

Central office accounting duties for the Inmate Trust Fund are not segregated or adequately monitored (page 7).

Disaster Recovery Plan Insufficient

The disaster recovery plan lacks the specific instructions necessary to restore TOMIS in an emergency (page 12).

*This finding is repeated from the prior audit.

"Audit Highlights" is a summary of the audit report. To obtain the complete audit report, which contains all findings, recommendations, and management comments, please contact

Comptroller of the Treasury, Division of State Audit
1500 James K. Polk Building, Nashville, TN 37243-0264
(615) 401-7897

Financial/compliance audits of state departments and agencies are available on-line at
www.comptroller.state.tn.us/sa/reports/index.html.

For more information about the Comptroller of the Treasury, please visit our Web site at
www.comptroller.state.tn.us.

Audit Report
Department of Correction
For the Period July 1, 2000, Through March 31, 2003

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
Post-Audit Authority	1
Background	1
AUDIT SCOPE	1
PRIOR AUDIT FINDING	3
Repeated Audit Finding	3
OBJECTIVES, METHODOLOGIES, AND CONCLUSIONS	3
Internal Audit	3
Contracts	4
Facility Visits	4
Inmate Trust Fund Account	6
Finding 1–The Department of Correction lacks effective internal controls Request over the Inmate Trust Fund account at the central office	7
Tennessee Offender Management Information System	7
Finding 2–Policies, procedures, and operating controls for the Tennessee Offender Management Information System are inadequate	8
Finding 3–TOMIS disaster recovery plan is insufficient	12
Financial Integrity Act	13
OBSERVATIONS AND COMMENTS	13
Title VI of the Civil Rights Act of 1964	13
APPENDIX	14
Allotment Codes	

Department of Correction
For the Period July 1, 2000, Through March 31, 2003

INTRODUCTION

POST-AUDIT AUTHORITY

This is the report on the financial and compliance audit of the Department of Correction. The audit was conducted pursuant to Section 4-3-304, *Tennessee Code Annotated*, which authorizes the Department of Audit to “perform currently a post-audit of all accounts and other financial records of the state government, and of any department, institution, office, or agency thereof in accordance with generally accepted auditing standards and in accordance with such procedures as may be established by the comptroller.”

Section 8-4-109, *Tennessee Code Annotated*, authorizes the Comptroller of the Treasury to audit any books and records of any governmental entity that handles public funds when the Comptroller considers an audit to be necessary or appropriate.

BACKGROUND

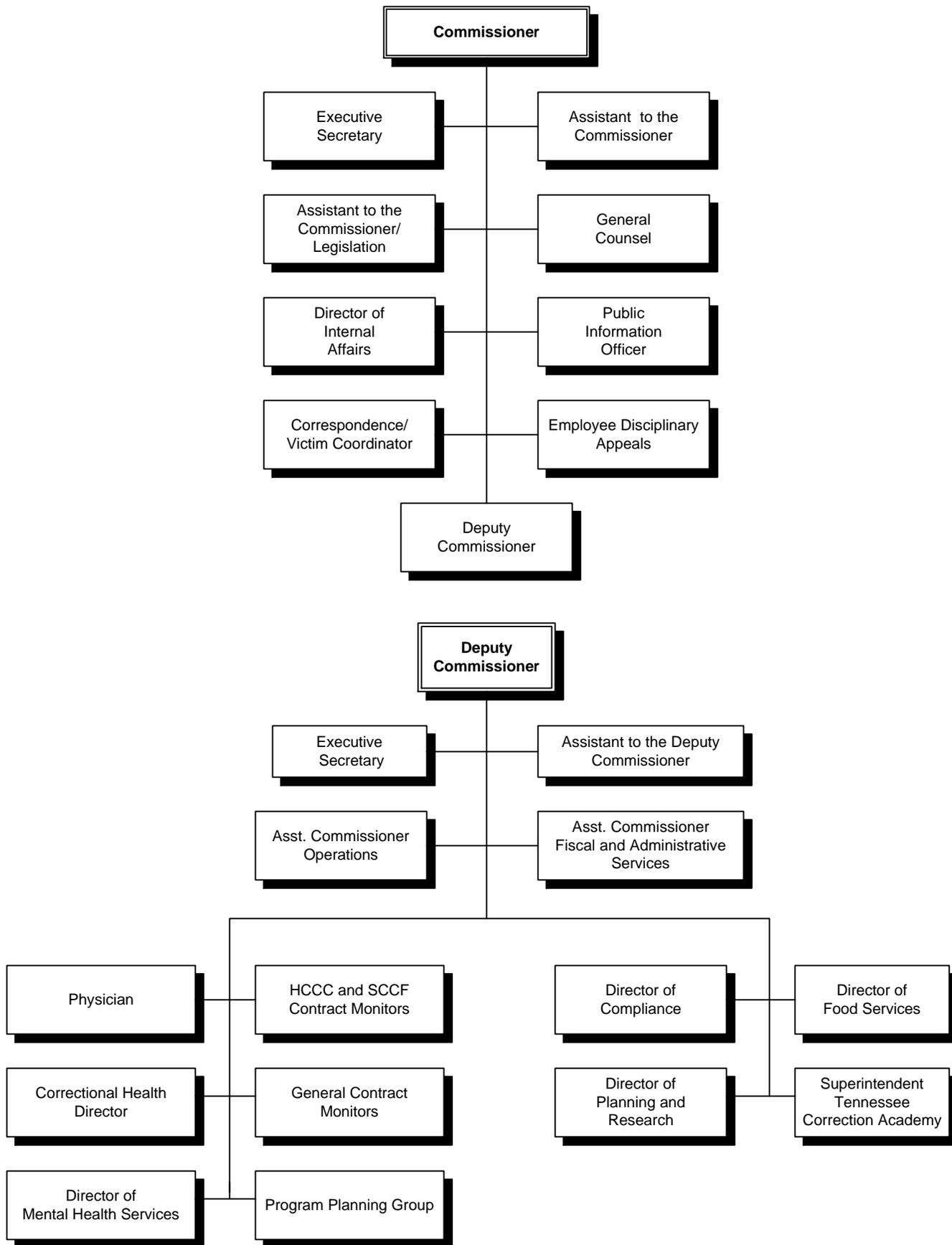
The mission of the Tennessee Department of Correction is to ensure public safety through incarceration of convicted felons; enhance inmate life skills through selected rehabilitative programming; and make implementation of cost-effective measures a clear priority. The department’s vision is to be an organization where employees are empowered in the decision making process; involved in the improvement of individual knowledge and skills, the workplace and society; and committed to providing a safe and humane environment and to assisting offenders by providing opportunities for positive behavioral changes.

An organization chart of the department is on the following page.

AUDIT SCOPE

We have audited the Department of Correction for the period July 1, 2000, through March 31, 2003. Our audit scope included a review of management’s controls and compliance with policies, procedures, laws, and regulations in the areas of Internal Audit, contracts, facility visits (petty cash, equipment, purchasing, warehouse and commissary inventory, and payroll), the Inmate Trust Fund Account, the Tennessee Offender Management Information System, and the Financial Integrity Act. The audit was conducted in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial

Department of Correction



audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

PRIOR AUDIT FINDING

Section 8-4-109, *Tennessee Code Annotated*, requires that each state department, agency, or institution report to the Comptroller of the Treasury the action taken to implement the recommendation in the prior audit report. The Department of Correction filed its report with the Department of Audit on January 14, 2003. A follow-up of the prior audit finding was conducted as part of the current audit.

REPEATED AUDIT FINDING

The prior audit report contained a finding concerning policies and procedures, operating controls, and training for the Tennessee Offender Management Information System. This finding has not been resolved and is repeated in the applicable section of this report.

OBJECTIVES, METHODOLOGIES, AND CONCLUSIONS

INTERNAL AUDIT

The objectives of our review of the controls and procedures for Internal Audit were to determine whether

- Internal Audit was independent of the program functions of the department;
- internal auditors had the education, experience, and supervision needed for their work to be relied on by other auditors;
- the internal auditors adequately documented their work;
- all correctional institutions in Tennessee, including the Tennessee Correction Academy, were audited in the past two years; and
- Internal Audit issued audit reports in compliance with established policies and procedures.

We interviewed key Department of Correction personnel to obtain an understanding of the department's controls and procedures for Internal Audit, and we reviewed supporting documentation for these controls and procedures. We reviewed the department's organization chart and interviewed the director of compliance to determine whether Internal Audit was independent of the program functions of the department. We reviewed personnel files including supporting documentation to determine whether the internal auditors had the education and experience needed for their work to be relied on by other auditors. We also reviewed Internal Audit's working papers for evidence of adequate supervision and to determine whether auditors adequately documented their work. We obtained and reviewed a listing of all audits completed during the audit period to determine if all the correctional institutions in Tennessee, as well as the Tennessee Correction Academy, had been audited during the past two years. We reviewed all the audit reports issued during the audit period to determine if Internal Audit issued audit reports in compliance with the established policies and procedures.

Based on our interviews, review of supporting documentation, and testwork, we determined that the internal auditors had the education, experience, and supervision needed for their work to be relied on by other auditors; the internal auditors adequately documented their work; that all correctional facilities were audited during the past two years; and that internal audit reports were issued in compliance with established policies and procedures. We also determined that Internal Audit was independent of the program functions of the department.

CONTRACTS

The objective of our review of the controls and procedures for contracts was to determine whether the department had properly executed contracts in place before contracted services were rendered. We interviewed key Department of Correction personnel to gain an understanding of the department's controls and procedures over contracts, and we reviewed supporting documentation for these controls and procedures. We tested all contracts over \$1,000,000 for proper authorization in a timely manner.

Based on our interviews, review of supporting documentation, and testwork, it appears that contracts over \$1,000,000 were properly executed before contracted services were rendered.

FACILITY VISITS

The objectives of our review of the controls and procedures over the petty cash fund, equipment, purchasing, warehouse and commissary inventory, and payroll at the 12 facilities and the Tennessee Correction Academy were to determine whether

- expenditures paid from the petty cash account were adequately documented and were allowable per the petty cash policies and procedures;
- the balance in the petty cash ledger reconciled with the balance in the bank account;

- equipment at the facilities was correctly listed on the Property of State of Tennessee equipment list;
- recorded procurements were for goods or services that were properly authorized;
- procurements during the audit period complied with applicable policies, procedures, and other regulations or requirements;
- inventory in the warehouse was properly reported on the perpetual inventory system;
- overages/shortages listed on the commissary inventory summary were adequately explained; and
- individuals receiving payroll checks were actual employees.

We interviewed key Department of Correction personnel at the facilities visited to gain an understanding of the department's controls and procedures over the petty cash fund, equipment, purchasing, warehouse and commissary inventory, and payroll. We also reviewed supporting documentation for these controls and procedures.

The following testwork was performed at each facility visited. Twenty-five petty cash expenditures were tested to determine if expenditures paid from the petty cash account were adequately documented and allowable per the petty cash policies and procedures. In addition, bank confirmations for the petty cash bank accounts were reconciled to the petty cash ledger. Twenty-five equipment items were located to determine whether equipment was correctly listed on the Property of State of Tennessee equipment list. A nonstatistical sample of 25 purchase requests were tested to determine whether the procurements were for goods or services that were properly authorized, and the purchase complied with applicable policies, procedures, and regulations. Twenty-five items from the warehouse inventory listing were counted and reconciled with listing to determine if inventory in the warehouse was properly reported on the perpetual inventory system. All the monthly commissary overage/shortage reports during the audit period were reviewed to determine if overages/shortages listed on the commissary inventory summary were adequately explained. Payroll payout testwork was performed for a nonstatistical sample of payroll checks to determine whether individuals receiving payroll checks were actual employees.

Based on the interviews and testwork performed, petty cash expenditures were allowable and adequately documented, the balance in the petty cash ledger reconciled with the balance in the bank account, equipment was correctly listed on the equipment list, purchases were properly authorized and in compliance with applicable policies and procedures, and only actual employees received payroll checks. Also, the inventory in the warehouse was properly reported on the perpetual inventory system, and overages/shortages listed on the commissary inventory summary were adequately explained.

INMATE TRUST FUND ACCOUNT

The Inmate Trust Fund Account was established by Department of Correction Policy 208.01 to create a cashless inmate economy. This policy became effective on December 15, 1998, and is in the process of being updated. The policy receives its authority through *Tennessee Code Annotated*, Public Chapter 992, and the Inmate Financial Responsibility Act of 1998.

At each of the department's facilities and the central office, the objectives of our review of the department's controls and procedures over the Inmate Trust Fund Account were to determine whether

- the transactions were properly supported, approved, and recorded;
- the procedures used to administer the account followed the applicable regulations;
- accounting duties were segregated; and
- reconciliations were reviewed, and reviews were documented.

We interviewed key Department of Correction personnel and reviewed supporting documentation at the visited facilities and the central office to gain an understanding of the department's controls and procedures over the Inmate Trust Fund Account. We tested a nonstatistical sample of 75 transactions. For each of those transactions, we examined the applicable expenditures, receipts, and holding accounts to determine whether the transactions were properly supported, approved, and recorded, and the procedures used to administer the account followed the applicable regulations.

Job duties required to perform the transactions of the Inmate Trust Fund Account were discussed with the appropriate personnel to determine if the duties were segregated. Reconciliations for checks payable, backup withholding, inmate IRS Form 1099 reporting, inmate telephone logs, and unclaimed funds were obtained and reviewed to determine whether the reconciliations were reviewed and the reviews were documented.

Based on the auditor's discussions with appropriate personnel, reviews, and testwork performed, the transactions appeared to be properly supported, approved, and recorded, and the procedures used to administer the account followed the applicable regulations. However, as noted in the following finding, there were inadequacies in the of segregation of duties and the review and documentation of reconciliations.

1. The Department of Correction lacks effective internal controls over the Inmate Trust Fund account at the central office

Finding

The Department of Correction lacks effective internal controls over the Inmate Trust Fund account at the central office. Accounting duties for the fund are not segregated, management does not adequately monitor these duties, and management does not document applicable reviews.

Duties related to Inmate Trust Fund functions in the central office are not adequately segregated. The Accounting Technician's responsibilities include processing and approving transactions through the Tennessee Offender Management Information System (TOMIS), correcting processing errors, monitoring the issuance of checks, and performing account reconciliations. Management has not adequately monitored most of these accounting functions, nor has management documented its reviews of applicable reconciliations.

Although the opportunity for fraud existed, based on the audit testwork, there was no indication that fraud occurred. While there were no exceptions noted due to the lack of effective accounting internal controls, an employee whose accounting job duties were not adequately segregated and monitored could have allowed fraudulent activities to occur in the Inmate Trust Fund account. In addition, reviews of applicable accounting reconciliations cannot be determined as having been performed if management does not document its reviews.

Recommendation

Management needs to monitor the duties of personnel performing Inmate Trust Fund accounting functions and make the appropriate changes to ensure proper segregation of duties. Management also needs to ensure that all applicable reconciliations are reviewed and that reviews are documented.

Management's Comment

We concur. Duties of the personnel performing Trust Fund accounting functions were not properly segregated, and reconciliations were not properly reviewed and documented. Actions are being taken to ensure that duties are properly segregated. Reconciliations will be reviewed in a timely manner and documentation of those reviews will be maintained.

TENNESSEE OFFENDER MANAGEMENT INFORMATION SYSTEM

The Tennessee Offender Management Information System (TOMIS) is an on-line, interactive, table-driven application used by the Department of Correction and various law-enforcement agencies within the State of Tennessee to track offenders from the point of conviction through release from all supervision. The system addresses many aspects of an offender's life including conviction, sentencing, incarceration, offender treatment, behavior,

health, finances, and services provided during parole or probation. The department's Management Information Systems division (MIS) supports the system. Resource Access Control Facility (RACF) is the statewide mainframe security software, used to provide access security at the initial level (or front-end) before the user can access department or agency systems such as TOMIS. The Department of Finance and Administration's Office of Information Resources is administratively responsible for RACF; however, the Department of Correction's MIS division is responsible for establishing, maintaining, and terminating departmental users.

The objectives of our review of the procedures and controls over TOMIS were to follow up on the status of the prior year audit finding by determining whether

- departmental and Management Information Systems policies and procedures regarding TOMIS were adequate and operating effectively;
- logical access controls were adequate to restrict unauthorized use of TOMIS;
- changes to user group attributes were properly controlled;
- system overrides (table changes) were properly documented and approved;
- override changes to data were properly documented and authorized; and
- the department had an adequate disaster recover plan.

We examined the MIS policies and procedures manual to determine whether management had developed proper operating controls over administrative access to all components of TOMIS and its data. We evaluated management's development and implementation of a plan to establish segregation of duties within MIS. We interviewed key personnel, observed operations, and reviewed supporting documentation to determine if user access to TOMIS is adequately controlled. Inquiries were made of management regarding changes to user groups and other TOMIS tables and offender data overrides. We also obtained and reviewed the department's disaster recover plan and requirements for a plan to determine if the plan was adequate.

As noted in the following findings, our testwork revealed inadequacies in the following areas: the department's written policies and procedures; controls over TOMIS user groups, table changes, and offender data overrides; and the disaster recover plan.

2. Policies, procedures, and operating controls for the Tennessee Offender Management Information System are inadequate

Finding

The Tennessee Offender Management Information System (TOMIS) is a computer application consisting of more than 1,300 programs. The Department of Correction is administratively responsible for the system that is used throughout the state to capture data

relating to offenders. Despite the size and complexity of TOMIS, the Department of Correction does not have adequate written operating policies and procedures for the system. After this was reported in the prior audit, the department's Management Information Systems division (MIS) expanded and updated the existing manual; however, many critical access-of-system operations are still not completely addressed. These operations include the review and supervision of MIS staff activities, alteration of database information, and changes to system tables.

Furthermore, as also noted in the prior audit, the department has not implemented adequate operating controls to protect the integrity of the system data and limit the opportunities for fraud, sabotage, or inappropriate disclosures. There is a critical lack of segregation of duties. Most MIS-Systems Development Section (SDS) employees have unlimited access to change information in the system. Additionally, the department has not enacted adequate compensating controls to counteract the lack of segregation of duties. Although some of the operating control weaknesses noted in the prior audit have been corrected, the following problems still exist.

- Eleven of 12 MIS-SDS employees can “add,” “modify,” and “delete” user group definitions. The user group definitions establish the level of access for every TOMIS user. Furthermore, changes to user group levels of access are not monitored, and an adequate history of changes is not maintained.
- All MIS-SDS employees can perform the functions of system security, data security, data administration, and system design. The department has partially addressed this lack of segregation by developing a plan to separate the system security from system design functions. However, this plan has not yet been enacted and fails to remove access to production data from employees with system design responsibilities.
- Changes to tables within the system are left to the discretion of each MIS-SDS employee, and no written approval of these changes is required. Changes to system tables are not addressed in the policies and procedures manual.
- MIS-SDS employees are allowed access to override the system (or circumvent the controls designed into the system) to correct data instead of using program changes to resolve existing design problems within the system. For example, MIS-SDS employees frequently change an offender's status from inactive to active to allow certain updates to the offender's data that cannot be processed if the offender's status is inactive. The policies and procedures manual does not address overriding the system to alter database information.
- MIS policy does not require standard security authorization forms for establishing new user security access. Additionally, the policy does not require authorization and documentation before changing an existing user's level of access.
- Requests for MIS to change data within TOMIS are often made via telephone and are not documented or approved.

- Although various system history logs are generated to document alterations to TOMIS data and system tables, MIS management does not review most of these logs and does not document the review of any logs.

Adequate written operating policies and procedures provide guidance to employees and help to ensure consistency in system operations. System operating controls are necessary to prevent the unauthorized access, deletion, or alteration of data. Without adequate controls, the integrity of the system data may be compromised, and opportunities for fraud, sabotage, and inappropriate disclosures may occur.

Recommendation

Management should continue to review and enhance their written operating policies and procedures for MIS and ensure that these operating policies and procedures are fully implemented. Management's review should address adequate operating controls over all components of TOMIS and its data. Additionally, management should evaluate current MIS functions to develop and implement a plan to establish complete segregation of duties within MIS. Authorized requests for current and new system access and changes to individual user groups should be obtained and retained to document approval. All requests for data changes should be documented and approved before implementation. Management should routinely review the history logs of changes to TOMIS and document the review.

Management's Comment

We concur. The SDS staff has historically served as system administrators for the TOMIS system and as such has 'X5' user group security access. This gives them add, modify and delete access to most conversations, including the master 'table of tables' (WTMM) that defines specific override security access parameters.

The master table provides the ability to specify individual RACF IDs who have Add, Modify and Delete access to certain tables where incorrect data changes could be particularly risky, such as the USER CLASS ENTRY TABLE where users are assigned to particular user classes. Technically anyone in the X5 user class (SDS staff) has rights to change this access information through the table of tables, but procedurally this function is restricted. Currently eight of the SDS staff have Add, Modify and Delete rights to the USER CLASS ENTRY TABLE as defined in the master table.

Under the staff reorganization plan, only the five persons on the MIS Help Desk will be in the X5 user class, as well as have individual RACF ID rights to the USER CLASS ENTRY TABLE. The plan is part of an overall MIS staff reorganization and reclassification proposal. MIS management has documented this proposed staff structure in an overview organization chart and is currently developing written justification and job descriptions for the reclassifications. Formal approval for the plan from executive management is being sought.

Changes to code table values are only made in conjunction with well-documented design changes (SIRs, RFS) [System Investigative Requests, Requests for Service] to support requested business logic changes. The MIS procedures manual describes how program changes may be submitted and approved for work. MIS management concurs the procedure does not include a final approval step. Since procedures have changed somewhat from what is documented, this section of the manual will be rewritten to reflect actual practice as well as address the missing steps of testing and sign off.

Such procedures are well instituted and SDS management monitors and trains staffs to ensure such procedures are followed. However, MIS management concurs that what is in practice is not fully documented, and will work to commit these to written format.

Since its inception in the early 1990s, TOMIS has been flawed with various design or logic shortcomings. SDS has worked to correct such design flaws in addition to incorporating new logic required by statutory or business process changes. Reported program flaws must be prioritized and worked as they can be based on severity of the problem, availability and skill of SDS staff and availability of OIR programmers. Currently there are over 100 SIRs in the queue, some in progress, most awaiting resources to work them. Until such program changes can be worked into the schedule, it is necessary to change the data that is erroneously entered.

MIS concurs it needs to add a section to the procedures manual describing how requested data changes should be managed and tracked, as well as set guidelines for developing SIRs when logic errors are the cause for PDCAs [Production Data Change Authorizations].

The MIS procedure manual, attached to policy 109.05, specifically includes a security administration form that new TOMIS users must complete to gain access. Users' level of access changes are only made upon request from the institution's contact person, usually by e-mail. MIS management will review these procedures to determine if there is a tighter way to document what is required.

MIS procedure manual specifically documents procedures to be followed to delete TOMIS data. Each SDS staff individually retains copies of written requests. However, procedural documentation is lacking regarding where and how long such information should be retained. This is being reviewed by SDS management and will be documented to ensure consistency.

TOMIS has a transaction log of deletions, each record of which includes user ID, time and date stamps. The log is accessible only through Platinum. The log records are not in a readable format and only a handful of SDS analysts are skilled in using the database tool.

MIS management has asked SDS management to investigate the possibility of generating a readable extract from this file for review purposes. To our knowledge, there have not been any inappropriate record deletions.

There are no transaction logs that capture data modifications only; such a log would be unmanageable.

MIS management concurs the greatest weakness in the management of TOMIS is a lack of centralized, consistent documentation of the procedures that are generally followed. The division has a FY 2004 project to review and update its policies and procedures, both to comply with good IT business practices as well as to address HIPAA specific security concerns.

3. TOMIS disaster recovery plan is insufficient

Finding

The disaster recovery plan in the *Management Information Systems Policy Manual* for the Department of Correction Tennessee Offender Management Information System (TOMIS) is insufficient. This plan lacks the specific instructions necessary to restore TOMIS in an emergency. The Information Systems Council, Information Resources Policy 9.00: Disaster Recovery states, “Disaster recovery planning and the capability for implementing a recovery are required encompassing all critical data processing applications and their peripheral support activities.” To assist agencies in their disaster recovery planning, the Office of Information Resources has developed *Guidelines for State of Tennessee Disaster Recovery Planning* “to provide information and present issues that should be considered when creating a disaster recovery plan.” The guidelines include a list of agency responsibilities and activities to use as a starting point in evaluating actions that need to be included in the agency’s plan. Specific instructions are vital to the execution of a sufficient plan.

The guidelines also state, “One of the most important considerations for all aspects of disaster recovery preparedness is the ability to keep information up-to-date. Procedures should be established for review of all aspects of disaster recovery on some recurring schedule. As production programs and procedures change, they should be reviewed immediately for impact on disaster recovery capabilities.”

TOMIS is a mission critical system that processes most of the department’s inmate information and tracking. Thorough documentation of its disaster recovery procedures and the results of testing those procedures can help ensure that critical data processing applications and their peripheral support activities are quickly restored in the event of a disaster.

Recommendation

The department should thoroughly document specific disaster recovery procedures. The procedures should be prioritized and should list the specific actions to be taken from the declaration of a disaster until the time that normal business operations are resumed. The plan should be reviewed, updated, and tested periodically.

Management’s Comment

We concur. Now that MIS management has been made aware of OIR’s recommended guidelines for what should be included in a complete Disaster Recovery plan, SDS staff has begun drafting the detail of such a plan. As part of its three-year information systems plan in

2002 and 2003, MIS has included an inventory of all systems with an indication of criticality of the system and a high-level description of the backup and restore procedures. Specific procedures for each system will build on this spreadsheet.

FINANCIAL INTEGRITY ACT

Section 9-18-104, *Tennessee Code Annotated*, requires the head of each executive agency to submit a letter acknowledging responsibility for maintaining the internal control system of the agency to the Commissioner of Finance and Administration and the Comptroller of the Treasury by June 30 each year.

Our objective was to determine whether the department's June 30, 2002, and June 30, 2001, responsibility letters were filed in compliance with Section 9-18-104, *Tennessee Code Annotated*.

We reviewed the June 30, 2002, and June 30, 2001, responsibility letters submitted to the Comptroller of the Treasury and to the Department of Finance and Administration to determine adherence to the submission deadline. We determined that the Financial Integrity Act responsibility letters were submitted on time.

OBSERVATIONS AND COMMENTS

TITLE VI OF THE CIVIL RIGHTS ACT OF 1964

Section 4-21-901, *Tennessee Code Annotated*, requires each state governmental entity subject to the requirements of Title VI of the Civil Rights Act of 1964 to submit an annual Title VI compliance report and implementation plan to the Department of Audit by June 30 each year. The Department of Correction filed its compliance reports and implementation plans on July 15, 2002, and June 29, 2001.

Title VI of the Civil Rights Act of 1964 is a federal law. The act requires all state agencies receiving federal money to develop and implement plans to ensure that no person shall, on the grounds of race, color, or origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal funds. The Human Rights Commission is the coordinating state agency for the monitoring and enforcement of Title VI. A summary of the dates state agencies filed their annual Title VI compliance reports and implementation plans is presented in the special report *Submission of Title VI Implementation Plans*, issued annually by the Comptroller of the Treasury.

APPENDIX

DIVISIONS AND ALLOTMENT CODES

Department of Correction divisions and allotment codes:

329.01	Administration
329.04	State Prosecutions
329.06	Tennessee Correction Academy
329.08	Wayne County Boot Camp
329.11	Brushy Mountain Correctional Complex
329.13	Tennessee Prison for Women
329.14	Turney Center Industrial Prison and Farm
329.16	Mark H. Luttrell Correctional Center
329.17	Middle Tennessee Correctional Complex
329.18	Southeastern Tennessee State Regional Correctional Facility
329.21	Hardeman County Correctional Facility
329.32	Major Maintenance
329.41	West Tennessee State Penitentiary
329.42	Riverbend Maximum Security Institution
329.43	Northeast Correctional Complex
329.44	South Central Correctional Facility
329.45	Northwest Correctional Complex
329.46	Lois M. DeBerry Special Needs Facility
329.50	Sex Offender Treatment Program
329.98	Federal Construction Grants
329.99	Sentencing Act of 1985