AUDIT REPORT

Department of Safety

December 2008

STATE OF TENNESSEE

COMPTROLLER OF THE TREASURY

Department of Audit

Division of State Audit

TENNESSEE COMPTROLLER OF THE TREASURY

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

Kandi B. Thomas, CPA, CFE
Assistant Director

Shirley A. Henry, CPA
Teresa L. Kennedy, CPA
Audit Managers

Charles K. Bridges
Assistant Audit Manager

Rebecca W. Troyani, CPA, CFE
In-Charge Auditor

Herb Kraycirik, CPA
Tanya Latham
James Ligon
Erica Pettway
Lindsey Stadterman
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 website at www.comptroller.state.tn.us.

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

December 9, 2008

The Honorable Phil Bredesen, Governor
and
Members of the General Assembly
State Capitol
Nashville, Tennessee 37243
and
The Honorable Dave Mitchell, Commissioner
Department of Safety
1150 Foster Avenue
Nashville, Tennessee 37249

Ladies and Gentlemen:

We have conducted a financial and compliance audit of selected programs and activities of the Department of Safety for the period July 1, 2005, through July 31, 2007.

We conducted our audit in accordance with generally accepted government auditing standards. These standards require that we obtain an understanding of internal control significant to the audit objectives and that we design the audit to provide reasonable assurance of the Department of Safety's compliance with laws, regulations, and provisions of contracts significant to the audit objectives. Management of the Department of Safety is responsible for establishing and maintaining effective internal control and for complying with applicable laws, regulations, and provisions of contracts and grant agreements.

Our audit disclosed certain findings which are detailed in the Objectives, Methodologies, and Conclusions section of this report. The department's management 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 control and instances of noncompliance to the Department of Safety's management in a separate letter.

Sincerely,

Arthur A. Hayes, Jr., CPA
Director

AAH/sah
07/036

State of Tennessee

Audit Highlights

Comptroller of the Treasury Division of State Audit

Financial and Compliance Audit
Department of Safety
December 2008

AUDIT SCOPE

We have audited the Department of Safety for the period July 1, 2005, through July 31, 2007. Our audit scope included a review of internal control and compliance with laws, regulations, and provisions of contracts in the areas of fines and fees, computer application access and disaster recovery, contracts, evidence rooms, equipment, the Financial Integrity Act, and Title IX of the Education Amendments Act of 1972. The audit was conducted in accordance with generally accepted government auditing standards.

AUDIT FINDINGS

Management Has Not Assessed and Mitigated Risks Associated With Inadequate Controls Over Reinstatement Receipts, Increasing the Risk That Employees Could Make Unauthorized Changes to System Information

The department's Driver License System, IMS2, is used to update the driver's history file when reinstatement payments are processed. However, department staff did not reconcile the IMS2 system with the department's cash register system (which is used to record the receipt of funds) to ensure that updates to the driver's history file corresponded with the related reinstatement fees collected. In addition, access controls were not adequate to prevent unauthorized changes to the Driver License System (page 5).

Management Introduced a Manual Override of Controls Without Adequately Assessing and Mitigating the Risks of Inadequate Controls Over the Issuance of Handgun Permits, Which Allowed Fraud to Occur and Fees to Be Misappropriated

During our audit the Director of Internal Audit informed us that an examiner at the Clarksville driver's license station had stolen an undetermined amount of handgun permit fees. The department's Handgun Permit Division had originally discovered the theft of the handgun permit fees and had called the department's Criminal Investigations Division and Internal Affairs to investigate the matter. In addition, the Internal Audit Division completed an audit of the transactions related to the examiner. Management had introduced a manual override of controls which was designed to allow department staff to process handgun

applications and collect handgun fees when the cashiering system is down; however this override also allowed the examiner who was processing the handgun permit application to override the cash register system, which allowed the fraud to occur and fees to be misappropriated. We also noted that the handgun permit applications did not work very well with the cash register system, applications were not prenumbered, and staff did not reconcile the handgun permits issued with the money received. In addition, numerous individuals had access to make changes to the transaction record through a particular screen with no documentation of what was changed, who made the change, and when the change was made (page 8).

Management Still Has Not Adequately Monitored Access to the Driver License System by Individuals From Other Agencies, Resulting in Instances of Unauthorized Access**

The Department of Safety allows certain employees of other state agencies and agencies outside the state to have inquiry access to its Driver License System. Acceptable Use Policy forms were not maintained for some users, and some users were not properly authorized (page 14).

** This finding is repeated from prior audits.

Management's Lack of Contract Oversight Allowed Staff to Make Payments Under an Improperly Executed Contract and to Record Transactions Incorrectly in the Accounting System, Increasing the Risk of Fraudulent Transactions

Due to a lack of contract oversight, a Fiscal Director was able to circumvent state contracting procedures and processed payments for an invalid contract. The five-year, $2.7 million contract, which was for services relating to the processing of commercial vehicle licensing and tax administration, contained signatures that had been forged by the Fiscal Director (page 20).

Financial and Compliance Audit
Department of Safety

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

Financial and Compliance Audit
Department of Safety

INTRODUCTION

POST-AUDIT AUTHORITY

This is the report on the financial and compliance audit of the Department of Safety. The audit was conducted pursuant to Section 4-3-304, *Tennessee Code Annotated,* which requires 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 Department of Safety is to ensure through education, regulation, and enforcement the overall safety and welfare of the public. This mission is accomplished through the following major functions:

- Capitol Police are responsible for patrolling and securing state buildings and grounds surrounding the capitol.

- Highway Patrol is responsible for enforcing motor vehicle and driver's license laws; investigating traffic accidents; providing motorists with assistance; and enforcing commercial vehicle laws on size, weight, and safety requirements. In addition, the highway patrol also provides instruction for all school bus drivers and conducts safety inspections on school and other buses.

- Executive Security provides security for the Governor and associated parties.

- Criminal Investigations Division (CID) investigates auto thefts, stolen vehicle parts, and odometer fraud.

- Special Operations, which consists of the Tactical Squad and the Aviation Unit, is responsible for special assignments such as bomb threats, VIP security, drug searches and seizures, and prisoner escapes.

- Driver's License Issuance administers oral, written, and road tests and issues and renews driver's licenses.

- Homeland Security is responsible for planning, coordinating, and implementing all of the state's homeland security activities.

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

AUDIT SCOPE

We have audited the Department of Safety for the period July 1, 2005, through July 31, 2007. Our audit scope included a review of internal control and compliance with laws, regulations, and provisions of contracts in the areas of fines and fees, computer application access and disaster recovery, contracts, evidence rooms, equipment, the Financial Integrity Act, and Title IX of the Education Amendments Act of 1972. The audit was conducted in accordance with generally accepted government auditing standards.

PRIOR AUDIT FINDINGS

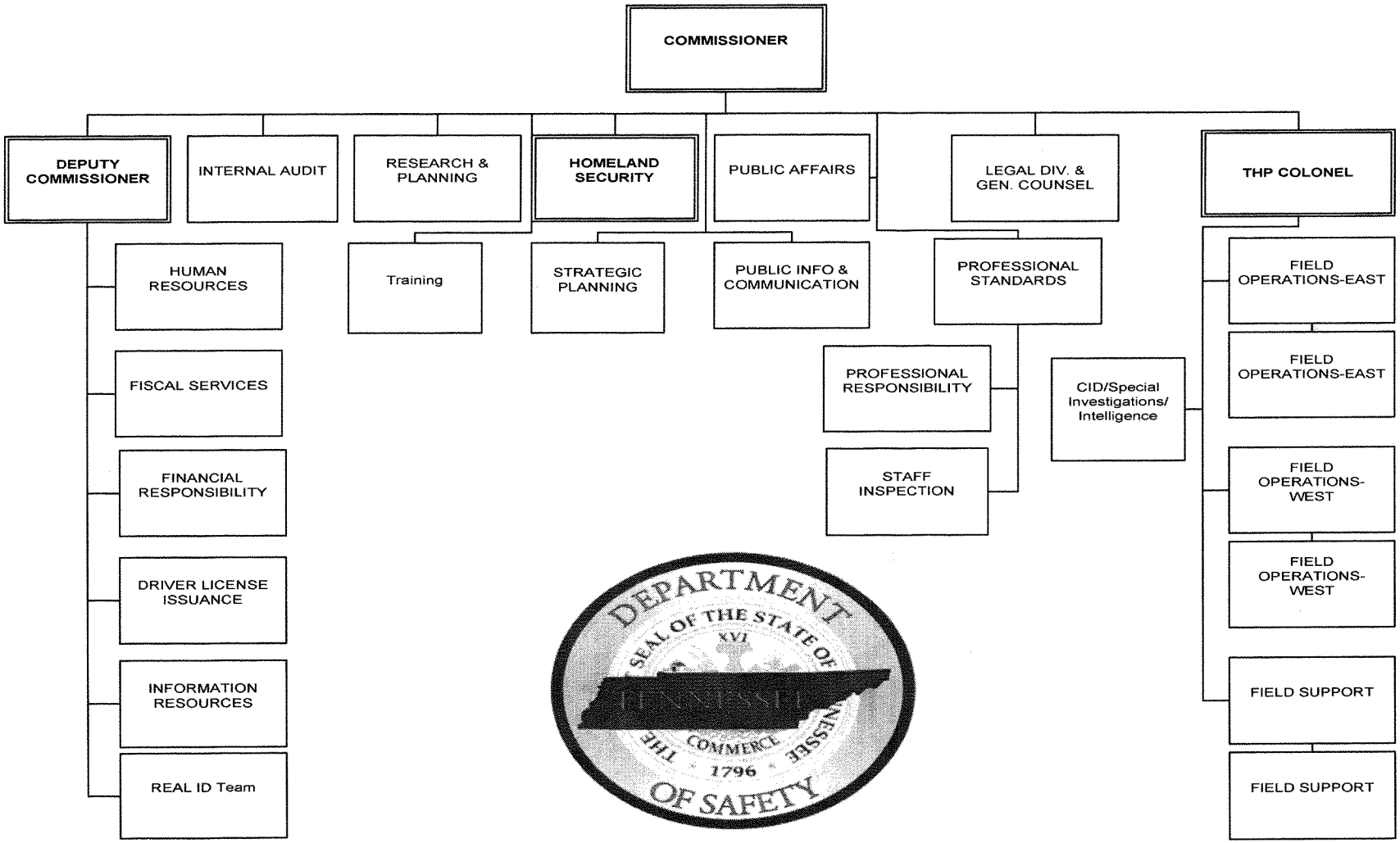
Section 8-4-109, *Tennessee Code Annotated*, requires that each state department, agency, or institution report to the Comptroller of the Treasury the action taken to implement the recommendations in the prior audit report. The Department of Safety filed its report with the Department of Audit on June 13, 2006. A follow-up of all but two of the prior audit findings was conducted as part of the current audit. The prior audit report contained two audit findings that were related to a division that was transferred to the Department of Revenue, and a follow-up on their implementation was conducted in the audit of the Department of Revenue.

RESOLVED AUDIT FINDINGS

The current audit disclosed that the Department of Safety has corrected previous audit findings concerning

- weaknesses in cash receipting procedures,
- the lack of written procedures for refunds of reinstatement fees,
- the lack of a disaster recovery plan for system applications which run independent from the state's data center,
- inadequate controls over equipment, and
- the department's failure to submit a Title IX implementation plan.

DEPARTMENT OF SAFETY
ORGANIZATION CHART



REPEATED AUDIT FINDING

The prior audit report also contained a finding concerning

- the department's failure to monitor access to the Driver License System and the Tag and Vehicle Inquiry System.

The Tag and Vehicle Inquiry System was transferred to the Department of Revenue on July 1, 2006, and the operation of that system will be considered as part of the Department of Revenue audit. The Department of Safety still maintains the Driver License System. The portion of the finding related to the Driver License System has not been resolved and is repeated in the applicable section of this report.

OBJECTIVES, METHODOLOGIES, AND CONCLUSIONS

FINES AND FEES

The objectives of our review of fines and fees were to follow up on prior audit findings and to determine whether

- fines and fees reconciliations were completed timely and in accordance with policy;
- system access was limited to employees who had jobs that required access;
- job duties were adequately segregated;
- driver's license reinstatement fees recorded in the IMS2 (Driver History File) agreed to the receipt and were properly calculated and reconciled to the daily deposit;
- driver's license reinstatement fees collected were reconciled to cash register activity and cash on hand;
- reinstatement refunds were properly calculated, approved, and mailed to the driver's address;
- an audit trail was created when changes were made to the IMS2 system; and
- incomplete handgun permit payment transactions were proper.

We interviewed key personnel and made observations to gain an understanding of controls and procedures over the receipt of fees and to determine whether job responsibilities were properly segregated. We performed testwork to determine if daily fines and fees reconciliations were completed timely and according to policy. We performed testwork to determine if system access was limited to employees who had jobs that required access and did not create an inadequate segregation of duties. We performed testwork on a sample of

reinstatement fees received from July 1, 2005, through May 5, 2007, to determine if the amount in IMS2 (Driver History File) was properly calculated and agreed to the receipt and reconciled to the daily deposit. We also reviewed the reconciliation procedures to determine if the reinstatement fees collected were reconciled to cash register activity and cash on hand. We tested a sample of reinstatement refunds with an effective date of July 1, 2005, through March 31, 2007, to determine if they were properly calculated and approved and to determine if they were mailed to the proper address. We discussed the use of the IMS2 system's Y16 screen with the Program Analyst Supervisor to determine if documentation was created when changes were made to the IMS2 system. We obtained a listing of incomplete payment entries for handgun permits in IMS2 which occurred between January 1 and March 31, 2007, and tested the transactions for propriety.

Based on our interviews, reviews, and testwork, we determined that

- daily fines and fees reconciliations were not properly completed (see findings 1 and 2);
- system access was not limited to employees who required such access (see finding 1);
- job duties were not properly segregated (see finding 1);
- the reinstatement fee recorded in the IMS2 (Driver History File) did not agree to the receipt for one sample item tested, but it was properly calculated and reconciled to the daily deposit;
- driver's license reinstatement fees collected were not reconciled with cash register activity and cash on hand (see finding 1);
- reinstatement refunds were properly calculated, approved, and mailed to the driver's address;
- there was no audit trail when changes were made to the IMS2 system using the Y16 screen (see finding 2); and
- there were some incomplete handgun permit payment transactions that could not be traced to a deposit of the permit fee (see finding 2).

1. Management has not assessed and mitigated risks associated with inadequate controls over reinstatement receipts, increasing the risk that employees could make unauthorized changes to system information

Finding

When a person loses his or her driving privileges and state-issued driver's license, the person must pay a fee in order to have his or her driver's license reinstated. Between July 1, 2005, and March 31, 2007, the department collected net reinstatement revenue of $14,147,660. The department's computer system, IMS2, is used to update the driver's history file when reinstatement payments are processed. The department also uses a cash register system, A2G, to

record the receipt of funds. We found that the department staff did not reconcile the two systems to ensure that updates to the driver's history file corresponded with the related reinstatement fees collected. We also found that access controls were not adequate to prevent unauthorized changes to the IMS2 system.

When a person makes a reinstatement payment, the examiner asks for the driver's license number, keys the number into the IMS2 system, and pulls up the driver's history file. The examiner prepares a prenumbered receipt form for the reinstatement fee, Memorandum to License Examiner/Receipt – TDS-SR-13A, which includes the name of the payer, the driver's license number of the record for which payment is being made, the amount of money received, and the reason for the receipt. The examiner signs the receipt and then enters the following information into the cash register: operator number, receipt number, department code, amount being paid, and amount of the reinstatement fee; then the examiner hits the reinstatement button. We found that no one in Financial Responsibility performed daily reconciliations of the activity within the IMS2 system used to update the status of driver's license reinstatements with receipts issued to drivers for reinstatement fees collected, the cash register activity, and the actual cash on hand. Management stated that to do this would require the development of new reports and would inevitably cause the daily reconciliation process to take longer. Department staff do perform daily reconciliations of cash register activity to receipts issued, money on hand, and the deposit slips. The lack of inclusion of the IMS2 system activity in the reconciliation process increases the risks that a driver could be given credit in IMS2 for paying a reinstatement fee when there was actually no payment received due to oversight, loss, or fraud.

The Assistant Director of Financial Responsibility stated that she receives a weekly report titled "Transaction Register," report ID DI07A008, which lists all driver records across the state on which department staff have entered a reinstatement code. The report shows each driver's first and last name, the license number, case number, event date (date of the ticket), action date (usually left blank), action code, operator ID and initials of the examiner who made the entry on the driver's record, and the operator user ID. She scans the listing looking for action codes that are not normally entered by a particular operator. She is familiar with the operator IDs and user IDs and knows the transaction codes that they normally work with. She then selects a certain number of transactions at random and reviews the supporting documentation, which would include the daily reconciliation and the deposit slip, to determine if the transaction appears proper and any related fees were deposited. Her review would include noticing if an examiner performed a transaction that was unusual for the assigned job duties of that person. However, her review is not documented, and considering the number of reinstatement transactions, this type of review would not be as effective in detecting discrepancies as would a daily reconciliation process, and such a review would not be as efficient or reliable as a routine, daily reconciliation that was a standard documented practice.

We obtained a listing of the ten employees at the Foster Avenue location in Nashville who were involved in the receipting, recording, and reconciling of reinstatement fees. Based on our review, we found the following:

- Four of the ten employees' job duties included collecting reinstatement fees, writing receipts, and posting receipts to the driver's license history file. Two of these four individuals, who were classified as working supervisors, had access to change addresses, change driver's license status, and remove or post information to the driver's license history file; two had access to remove or post information to the driver's license history file.

- Three of the ten employees' job duties included collecting receipts during the day and ensuring there were no missing receipts. Two of these three employees had access to change addresses and remove or post information to the driver's license history file; one had access to remove or post information to the driver's license history file.

- One of the ten employees' job duties included preparing the daily reconciliation of cash register activity to receipts to cash received and preparing the deposit slip. He had access to remove or post information to the driver's license history file.

With the ability that individuals have to make changes to the system and without adequate reconciliation procedures, inappropriate changes could be made and not be discovered.

Recommendation

The Director of Financial Responsibility should request that the Information Systems Director develop a daily report of driver's history updates related to reinstatement fees, which should be included in the daily reconciliation at each location that receives reinstatement fees. The Director of Financial Responsibility should revise the current reconciliation procedures to require that the reinstatement activity in the IMS2 system be made a part of the daily reconciliation process to ensure that updates to the driver's history file correspond with the related reinstatement fees collected. The Director of Financial Responsibility should request that the department's security administrator reduce the level of IMS2 system access to inquiry only for supervisors and employees who perform daily reconciliations.

As management continues their risk assessment activities, they should ensure that risks such as these noted in this finding are adequately identified and assessed in their documented risk assessment activities. Management should identify specific staff to be responsible for the design and implementation of internal controls to prevent and detect exceptions timely. Management should also identify staff to be responsible for ongoing monitoring for compliance with all requirements and taking prompt action should exceptions occur.

Management's Comment

We concur.

The Director of Financial Responsibility has requested that Information Technology (IT) modify the reinstatement "Transaction Register" to include the reinstatement fees collected from a driver with the reinstatement changes made to that driver's record. This report will be used to verify that the fee collected matches the reinstatement functions completed, will help identify any irregularities in the amount of money collected and help detect any reinstatements performed without the proper fees. This report will be available no later than the end of the first quarter 2009.

To ensure that the proper reinstatement fees are collected, the examiners must use the "Compliance Inquiry Screen" which lists the amount of reinstatement fees the computer system has calculated for that driver. Reinstatement fees collected at the driver license stations are then reconciled daily at each location. The reinstatement fees deposited are balanced with the fees shown on A2G and with the reinstatement receipts. Any differences are explained and documented. Once available, the modified Transaction Register discussed above will also be used to verify the fees collected with the reinstatement functions completed.

The Director of Financial Responsibility has reviewed and will modify the level of IMS2 system access. Out of 48 employees in Financial Responsibility, 24 have been identified to continue to have reinstatement access and 24 have been identified to have inquiry only. Staff assigned to perform any reconciliations in Financial Responsibility will have inquiry access only.

A documented risk assessment of the Financial Responsibility division has been completed. Risks that have been noted in this finding have been adequately assessed in the documented risk activities.

2. Management introduced a manual override of controls without adequately assessing and mitigating the risks of inadequate controls over the issuance of handgun permits, which allowed fraud to occur and fees to be misappropriated

Finding

In order to legally carry a handgun in the state of Tennessee, a person must complete handgun safety school training (as documented by a certificate of completion), pass a criminal history background check, complete an application for a handgun permit, and pay a fee to the Department of Safety when he or she submits the application. Between July 1, 2005, and March 31, 2007, the department collected $2,141,186 in fees for handgun permits. In our discussions with the Director of Internal Audit, she informed us that an examiner at the Clarksville driver's license station had stolen an undetermined amount of handgun permit fees, as discussed in detail below. When we reviewed the procedures and controls related to the issuance of handgun permits, we found inadequacies as discussed below.

All of the full-service driver's license stations accept handgun permit fees. The department's computer system, IMS2, is used to account for all transactions at a driver's license station, including the issuance of handgun permits. The department's cash register system, A2G, is also used at each driver's license station. These two systems were set up to interface. However, the cash registers sometimes do not function properly so at the Department of Safety's request, programmers in the Department of Finance and Administration's Office for Information Resources installed a manual override in 2003 to allow Department of Safety staff to process applications when the cashiering system is down. Management's decision to override the system and related controls enabled staff receiving the handgun permit fees to record the receipt in IMS2 but exclude the transaction from the cash register activity listing produced by the A2G system. This was accomplished by keying in "Paid" in the process code. When a handgun permit transaction is properly completed, a transaction record is created, and the transaction is captured in the department's infopac report, which is used in performing the daily reconciliation. Since the handgun permit transaction does not result in the issuance of the permit at the station, the employee completing the transaction could avoid having to make an entry on the final screen and creating the transaction record, which would keep the transaction off of the infopac report and therefore out of the daily reconciliation process. Thus, an employee could misappropriate money, and the theft could go undetected in the daily reconciliation of receipts issued to the cash register activity and money on hand.

The Director of Internal Audit stated that the theft perpetrated by the examiner at the Clarksville Driver's License station was accomplished through the use of "incomplete" transactions, which were created when the examiner entered the applicant's required information into the system and then abandoned the transaction before completion. Therefore, the system did not show the letter "P" in the print status field. Because of the theft disclosed to us by the Director of Internal Audit, we requested a list of all IMS2 system handgun permit transactions for the period January through March 2007 from the Director of the Handgun Permit Division; the list contained over 14,000 transactions. We examined the list and identified 71 transactions in which a fee amount was shown, but the "P" code was not shown. We requested the supporting documentation for those transactions from the Director of Internal Audit. Based on our review of the documentation, out of the 71 transactions, 64 handgun permits were issued. For five of those 64 transactions (8%), we found that although the applicant was issued a permit, we were unable to trace the fee amount to a deposit. The fee amount in each case was $115 so the five transactions amounted to $575. These five transactions were included in the list of transactions of the alleged fraud in the Clarksville Driver's License station as discussed below.

When the theft of handgun permit fees noted above was discovered by the Handgun Permit Division, staff called the department's Criminal Investigations Division and Internal Affairs to investigate the matter. On May 1, 2007, the examiner signed a statement admitting to the theft of handgun permit fees. The Internal Audit Division completed an audit of the transactions related to the examiner. In a memorandum dated July 1, 2007, the Director of Internal Audit detailed the work that was done by the Internal Audit Division and the results. The memorandum disclosed that the handgun permit fees for 52 handgun permit applications found in the examiner's workstation could not be traced to the bank; the fees totaled $5,655. In

an e-mail to the Director of Internal Audit dated September 13, 2007, the Special Agent in the Criminal Investigations Division stated that the examiner had been indicted.

Based on our review of the controls over handgun permits, we also found the following:

- the handgun permit applications did not work very well with the A2G system, the applications were not prenumbered, and staff did not reconcile the handgun permits issued with the money received; and
- numerous individuals had access to make changes to the transaction record through a particular screen with no documentation of what was changed, who made the change, and when the change was made.

The handgun permit application, which is a multi-page form, was developed before the A2G system was installed. It can be completed without using the A2G system or the IMS2 system. Employees who process the applications are to place the form into the cash register after a payment is received and print the transaction information on the form. The handgun permit application was not designed to be used with the A2G system; therefore, the printing on the form is often illegible or difficult to read. Besides having the ability to print the transaction on the handgun application, an employee is also permitted to write "paid" in the lower right corner of the form. Either method of indicating payment is accepted. In addition, the application is not prenumbered. The application number consists of either the last seven digits of the applicant's driver's license or the first seven numbers of the applicant's social security number. Once the completed form is received at the main office in Nashville and the required check of criminal history has been completed, the applicant is eligible to receive a permit to carry a handgun; however, we noted that no reconciliation of handgun permits issued to money received is performed.

There is a screen in the IMS2 system (designated Y16) which permits authorized users to access the transaction record for the purpose of updating the record for changes in the money paid amount, the status of the driver's license, or the applicant's physical description. Based on our discussion with the Information System Analyst 4 and the Program Analyst Supervisor, normally, only the supervisors at the stations have this access. The supervisor must use a special password to access the data record and make changes. However, the system does not maintain documentation of changes, including who made the change or when the change was made, so no accountability is established. At the time of our audit, there were 83 employees across the state with access to the Y16 screen.

The lack of adequate controls over the issuance of handgun permits allowed fraud to occur and fees to be misappropriated.

Recommendation

- The Commissioner should ensure that the Driver's License Issuance Director begins a documented risk assessment of her division and includes monitoring procedures for each identified risk and related control.

- The Commissioner should consider alternatives to the manual override of the cash register system and ensure that the problem that led to the override is corrected.

- The Commissioner should ensure that the Driver's License Issuance Director immediately begins redesigning the application for a permit to carry a handgun including prenumbering the form and designing it to accommodate the transaction information from the A2G system. In consultation with the Director of Internal Audit, the Driver's License Issuance Director should also develop procedures to account for all of the forms and to reconcile the fees received with the handgun permits issued.

- The Commissioner should ensure that the Information Systems Director limits access to the Y16 screen until appropriate system modifications can be made.

- The Commissioner should also instruct the Information Systems Director to generate a report which shows incomplete handgun permit transactions. The Driver's License Issuance Director should use the report to determine those stations with the greatest risk of underreporting handgun permit fee revenue and perform monitoring of controls immediately in coordination with the Director of Internal Audit.

- The Driver's License Issuance Director should also instruct the district managers to begin a documented random monitoring of recently issued handgun permits including determining if the permit fee was deposited into a state account.

As management continues their risk assessment activities, they should ensure that risks such as these noted in this finding are adequately identified and assessed in their documented risk assessment activities. Management should identify specific staff to be responsible for the design and implementation of internal controls to prevent and detect exceptions timely. Management should also identify staff to be responsible for ongoing monitoring for compliance with all requirements and taking prompt action should exceptions occur.

Management's Comment

We concur.

Risk Assessment:

A documented risk assessment of the Handgun Permits division has been completed. Risks that have been noted in this finding have been adequately assessed in the documented risk activities.

Cashiering System:

The current cashiering system has manual override capability in case the cashiering system goes down and is not available at the station. If this override is not available during an outage, personnel at the station would not be able to process applicants and print driver licenses. The current cash register system will be replaced with the iNovah cashiering system (Edison) no later than March 1, 2009. Until the implementation of iNovah, the following controls are in place to monitor an examiner's use of the current cash register system:

1. Driver License Policy Directives sent to all Driver License personnel in 2007 state that examiners must stay on-line when using the cashiering system. Supervisors must approve any off-line issuance and only in extreme circumstances. This approval must be documented by the supervisor on the Examiner's Daily Workstation Report, Section D.

2. The end of the day cash register report shows when an examiner has processed a transaction through IMS2 but has disabled the cash register system. The examiner is identified and their workstation report is reviewed to determine if they had approval to be off-line.

Handgun Carry Permit Application:

As of October 2007, the handgun application has been redesigned. All applications are prenumbered and blank space is available for the validation through the cash register system.

Under the current business process, accountability for all handgun applications would be very difficult. Applicants are handed applications as soon as they enter the station to complete while waiting, yet some may leave, make mistakes, throw away the application or take extra copies. Handgun safety schools and instructors also have applications available for their students yet they may not present the applications at the station. To require an applicant to fill out the handgun application at the examiner's window would be the only way to currently account for every handgun application number. This would significantly slow down customer service time, as the handgun application requires several minutes to complete.

However, the department is working with TennesseeAnytime to make the handgun application an online process. This would eliminate the need for paper copies of the handgun application. It is anticipated that this online application process will be available to the public sometime within the next 18 months.

Management is currently working with the Information Systems staff to develop a report that will provide information to reconcile the fees received with the handgun permits issued.

Revocation of Access to Y16 Screen:

The access to the Y16 screen has already been severely limited. No Driver License field staff or Handgun Permit division staff has access to the Y16 screen.

Incomplete Handgun Permit Transactions:

An Incomplete Transaction Report is available. Information Systems will isolate the incomplete handgun permit transactions, and this report will be sent on a monthly basis to the Handgun Unit Director for review.

Fees for Handgun Permit applications and Issued Handgun Permits:

The handgun permit fees are reconciled on a daily basis at the driver service centers with the applications. The fees deposited in the state account are balanced with the fees shown on InfoPac and A2G. In addition, management is currently working with the Information Systems staff to develop a report that will provide information to reconcile the fees received with the handgun permits issued.

COMPUTER APPLICATION ACCESS AND DISASTER RECOVERY

The objectives of our review of access for the Driver License System and the Tag and Vehicle Inquiry System and of the department's disaster recovery plan were to follow up on prior audit findings and to determine whether

- users' access to the systems was proper;
- appropriate security forms (Memorandum of Understanding, Acceptable Use Policy form, and Drivers Privacy Protection Act form) were maintained for outside agencies that were granted access to the systems;
- Information Resources monitored the outside agencies to determine if they were in compliance with the access agreement; and
- the department had a disaster recovery plan for those applications that were not covered by the Office for Information Resources in the Department of Finance and Administration.

We interviewed the Information Systems Director and the Security Administrator to gain an understanding of the department's procedures for granting access to its systems and to determine if the department had a disaster recovery plan for those applications that were not processed by the Office for Information Resources (OIR) and covered under the OIR's disaster recovery plan. We found that the Tag and Vehicle Inquiry System was transferred to the Department of Revenue on July 1, 2006, and the operation of that system will be considered as part of the Department of Revenue audit. We obtained the most current listings of all users with access to the system applications and tested a nonstatistical sample of users to determine if the users had proper access and the appropriate security forms were on file. We also discussed with the Security Administrator what procedures were in place to monitor outside agencies' compliance with the access agreement.

Based on our discussions and testwork, we determined that

- staff did not always properly authorize system access by outside users;
- staff did not maintain appropriate security forms for all users;
- Information Resources staff had not monitored the outside agencies with access to its system to determine if those users were in compliance with the access agreement; and
- Information Resources staff had developed a disaster recovery plan for those applications that were not covered by the Office for Information Resources in the Department of Finance and Administration.

The discrepancies noted above are discussed in finding 3.

3. Management still has not adequately monitored access to the Driver License System by individuals from other agencies, resulting in instances of unauthorized access

Finding

The Department of Safety allows certain employees of other state agencies and agencies outside the state to have inquiry access to its Driver License System. As noted in the prior two audits, the department still has not adequately monitored outside agencies' access to the system. Management concurred with the prior findings and in response to the most recent finding stated,

> Concerning documentation of agreements between agencies and with personnel within the department, records will be maintained and reviewed in accordance with state policy. Management will ensure that information system staff are knowledgeable about the significant risks to the department's information technology operations and know how to design and implement internal controls. The Director of Information Systems will designate staff to be responsible for monitoring for compliance and for taking prompt actions if exceptions occur.

> We have entered into agreements (Memorandum of Understanding) with other agencies to provide them with information necessary to carry out their lawful purposes, and we define such lawful purposes in the MOU. The department will ensure that each outside agency with ability to grant access to the system signs a new agreement each July. It is the responsibility of each agency to maintain access security as defined in the MOU, and the various security officers and IS Directors of the outside agencies should be familiar with their responsibilities under the MOU. Should any agency be found noncompliant with the MOU, the penalties defined in the MOU will be invoked. The department will develop procedures to ensure that outside agencies are collecting the appropriate security access forms. These procedures will include random sampling of individuals from such agencies to ensure that such access is on file.
>
> Except for the MOU agreements which are due in July, this recommendation will be implemented by April 1, 2006.

Management's response to this finding from the earlier audit is exhibited in the appendix titled "Management's Comment From Prior Audit."

In response to the prior findings, the Information Systems Director appointed an Information Resource Specialist 4 as the Department of Safety's Security Administrator. In addition, the department developed a template for the Memorandum of Understanding, with one version for state agencies and one version for agencies outside the state. By the end of July 2006, the department had signed agreements with all agencies, and the agreements are supposed to be updated each July. However, based on our testwork in the current audit, the department did not adequately monitor the outside agencies' compliance with the access requirements as stated in the agreements, as discussed below.

Once an outside agency has completed an *Agreement Authorizing Access to Data in Systems Managed by State of Tennessee Department of Safety*, the Security Administrator assigns each user to one or more user groups. User groups are the primary method used to control access to the department's systems since each member of a user group can access a pre-defined set of screens. Section 3.3.2 of the agreement states,

> Accessing Agency shall maintain security of information and insure proper usage of information by any user and shall support and enforce TDOS [Tennessee Department of Safety] security policies and procedures as promulgated by TDOS.

Therefore, along with the agreement, each user was supposed to sign an Acceptable Use Policy and sign the Drivers Privacy Protection Act form if he or she had access to the Driver License System.

We tested a sample of system users, which included seven users from outside agencies, and found that the Department of Safety did not have a signed Acceptable Use Policy for any of those seven users. Five of the users were with the Department of Human Services (DHS), one

was with the Board of Probation and Parole, and one was with the Tennessee Wildlife Resources Agency.

In its six-month follow-up response to the prior finding, dated June 8, 2006, management stated,

> The department will develop procedures to ensure that outside agencies are collecting the appropriate security access forms. These procedures will include random sampling of individuals from such agencies to ensure that such access is on file. These random samplings will be dated, documented and kept on file by the Safety RACF Administrator.

However, the Safety RACF Administrator stated that procedures had not been developed and she had not completed a random sampling of any of the agencies as of April 25, 2007. She had noted that DHS, with 1800 users, was the outside agency with the most users of the Driver License System. She requested the signed Acceptable Use Policy forms for DHS users on March 12, 2007; however, in early May, DHS had not sent the requested forms, and she had not contacted DHS again concerning the forms. When questioned about the lack of follow-through on the actions proposed in the follow-up report, the Information Systems Director stated that he was new to his position and was still learning his position and dealing with other projects that had priority. The RACF Administrator stated that she had been on leave for several months and was trying to catch up on her job responsibilities because there was no replacement for her while she was on leave.

In the sample testwork, we also found five users who were not properly authorized to access the systems. According to the *Agreement Authorizing Access to Data in Systems Managed by State of Tennessee Department of Safety*, Section 4.1.1, ". . . Accessing Agency shall not allow . . . 2) access to information or physical resources to any third party, except in the routine lawful conduct of terms of this Agreement." In violation of the agreement, the Department of Human Services granted access to two employees in county court clerks' offices and two employees of the Social Security Administration. One employee of the Internal Revenue Service was given access by the Department of Revenue. By giving this unauthorized access, these two departments violated their agreements with the Department of Safety.

Also, according to the *Agreement Authorizing Access to Data in Systems Managed by State of Tennessee Department of Safety*, Section 4.1., "Violation of the . . . provisions shall result in immediate termination of access, revocation of all privileges under this Agreement and such additional penalties as may apply." However, the non-compliant agencies noted above were not assessed any penalties by the Department of Safety for their actions. The Information Systems Director stated that he pointed out the issue to the other state agencies and asked them to resolve it; on a case-by-case basis they may revoke an errant user, but he made the decision not to take any action against another department.

The Information Systems Director's and Security Administrator's failure to collect the required forms or ensure the collection of forms by other agencies makes it more difficult for the

department to monitor and control access to their system. By not enforcing the requirement that access be limited to agencies which have completed the required agreement, the department has allowed unauthorized access to the Driver License System, increasing the risk of improper disclosure of confidential information.

Recommendation

The Commissioner should ensure that procedures are developed by the Information Systems Director for the monitoring of outside agencies by the Safety RACF Administrator to determine that they are in compliance with the agreements which they have signed including maintenance of the required forms and limitation of access to authorized employees of the agency. The Information Systems Director should revoke access to the Driver License System or take other effective and appropriate actions to ensure accountability by agencies that violate the provisions of their agreement.

As management continues their risk assessment activities, they should ensure that risks such as these noted in this finding are adequately identified and assessed in their documented risk assessment activities. Management should identify specific staff to be responsible for the design and implementation of internal controls to prevent and detect exceptions timely. Management should also identify staff to be responsible for ongoing monitoring for compliance with all requirements and taking prompt action should exceptions occur.

Management's Comment

We concur.

The department realizes that other state agencies have a legitimate need for driver license data. At the same time adequate safeguards should be in place to protect the data from unauthorized access. Historically the department has allowed outside agencies to have "inquiry only" access to the driver license system to meet their needs. This was done without any financial compensation for managing these additional users, or the additional cost of processing their requests within the system.

Over time the number of outside agency users increased to a point that existing departmental resources could no longer handle the administration of these users. To continue to allow access, the department opted to turn user administration for outside agencies users over to their own security administration with a Memorandum of Understanding (MOU). This MOU stated that they would be responsible for properly granting and revoking access of their users in accordance with state policy and the Driver Privacy Protection Act (DPPA).

After conducting reviews of agency user lists and requesting their supporting paperwork, it became apparent that several agencies were also struggling with the management of their uses

in the driver license system. This is the dilemma the department found itself in during the field observations of the Financial and Compliance audit.

The department has subsequently determined that user level access to the driver license system by outside agencies can no longer be supported due to the administrative overhead required to administrate the large number of access requests and the inability for outside agencies to self administrate their own users. In addition, the department is working towards Real ID compliance which would eliminate this level of access without additional safeguards, making this practice cost prohibitive for the department.

Realizing the need for outside agencies to use driver license data, the department has selected the following means for these agencies to obtain the data without direct access to the driver license system:

- For law enforcement agencies, the Criminal Justice Portal can provide a complete overview of a driver's record including driver data, history, signature, and photos.

- For agencies who need to check on the status of a driver license or to verify the address of a driver or identification card holder, the TennesseeAnytime portal has an application that will display the driver license information and its current status.

- For agencies who must determine the driver's ability to safely operate a motor vehicle, the TennesseeAnytime portal has an application that will display the driver's data and their Tennessee driving record.

Each of these systems provides logging functions to track all inquires by user and an interface for managing user access.

The department will be sending out notices to these agencies allowing them 90 days to transition from user level access in the driver license system to the appropriate portal server that meets their business objectives. This transition period will be completed by March 2, 2009.

A documented risk assessment of the Information Technology division has been completed. Risks that have been noted in this finding have been adequately assessed in the documented risk activities.

CONTRACTS

The Department of Safety contracted with a company to obtain processing services for the commercial vehicle licensing and tax administration, including the International Registration Plan, the International Fuel Tax Agreement, and the Single State Registration System. The five-year, $2.7 million contract covered the period July 1, 2005, through June 30, 2010. The Governor, by Executive Order No. 36, transferred the contract, associated staff, and functional

responsibilities from the Department of Safety to the Department of Revenue effective July 1, 2006. After the contract was transferred, Department of Revenue staff through the normal course of processing payments under this contract disclosed significant questions with the way the contract had been handled at the Department of Safety. In pursuing these questions, the Department of Revenue, Department of Finance and Administration, Department of Safety, and our office conducted inquiries and performed testwork to look into the problems that were disclosed.

The specific objectives of our review were to follow up on the work done by Internal Audit and to determine if

- department staff followed the required procedures in obtaining and executing the contract;
- contract expenditures were properly reviewed; and
- fiscal staff properly charged expenditures in the State of Tennessee Accounting and Reporting System (STARS) to the contract rather than charging expenditures as direct expenditures through transaction code 126 (TC 126).

We interviewed key personnel to gain an understanding of the internal control procedures over contracts and to determine the process that was used for this particular contract. We reviewed the procedures for ensuring that contract expenditures were properly recorded in STARS. We reviewed the testwork performed by Internal Audit, and we participated in investigative interviews with fiscal staff at the Department of Safety. We met with the Department of Finance and Administration's Director of Statewide Accounting to discuss proper TC 126 usage, post- and pre-audit reviews, and STARS vendor tables. We obtained a listing of contracts from the Director of the Office for Contract Review in the Department of Finance and Administration to use in our review of TC 126 transactions. We reviewed all transactions charged to TC 126 and compared the vendors to the contract listing to look for any contract expenditures that may have been incorrectly charged as direct expenditures.

Based on our interviews, reviews, and testwork, we determined that

- the required procedures were not followed in obtaining and executing the contract;
- contract expenditures were not properly reviewed; and
- expenditures were charged to transaction code 126 that should have been charged to the contract.

The discrepancies noted above are discussed in finding 4.

4. Management's lack of contract oversight allowed staff to make payments under an improperly executed contract and to record transactions incorrectly in the accounting system, increasing the risk of fraudulent transactions

Finding

Top management at the Department of Safety, other state officials, and the vendor believed that the Department of Safety had properly executed a contract with a vendor to obtain services for the processing of commercial vehicle licensing and tax administration, including the International Registration Plan, the International Fuel Tax Agreement, and the Single State Registration System when, in fact, no contract had been officially executed. The supposed contract was a five-year, $2.7 million contract for the period July 1, 2005, through June 30, 2010. The contractor had provided these services under a properly executed sole source contract for the prior five-year period covering July 1, 2000, through June 30, 2005.

To begin the contracting process, a Fiscal Director at the Department of Safety prepared a Request for Proposal (RFP) and submitted it to the Office of Contract Review (OCR) in the Department of Finance and Administration for approval; the RFP was approved, which meant that the Department of Safety was authorized to solicit proposals from vendors. However, based on our review, no one at the Department of Safety or OCR tracked the progress of the RFP to determine that the Fiscal Director properly completed the RFP process, that proposals were appropriately evaluated, and that a valid contract was executed. Apparently, the Fiscal Director was the one person in charge of all aspects of the RFP and contract execution process at the Department of Safety. As was subsequently determined, the Fiscal Director did not properly complete the RFP process, as discussed below, but instead misrepresented to other Safety officials and contractor representatives that the RFP process had been completed and that a valid contract had been awarded. In fact, the contract had not been properly awarded pursuant to the state's authorized procurement process and was therefore legally invalid because it had not been properly executed. In order for the services to continue, the Fiscal Director contacted the contractor and falsely informed them they had indeed been awarded the new contract through proper processes.

In addition, because a contract had not been correctly processed through the state's financial system, the state officials who would have to approve payments under the contract did not have any current information related to the purported contract needed to process the payments. Therefore, to effectuate payment to the contractor, the Fiscal Director also circumvented the authorized process to record contract transactions in the state's financial system by miscoding the contract payments as direct payments (using transaction code 126) rather than as contract payments. These direct pay expenditures were charged to object code 087 as "dues and subscriptions." As a result, contract expenditures totaling $528,699.84 that should have been charged to the contract were not. In an interview, the Fiscal Director stated that the RFP had never been completed, and the contract had never been approved by Finance and Administration or the Comptroller's office as required. Based on our testwork, we determined that in the initial RFP process, the Fiscal Director properly sent potential bidders the RFP package; however, only the one company that already had the contract responded. The Fiscal Director stated that when

she only received one bid, she was advised by the Director of OCR that the RFP process should begin again. However, when the Fiscal Director realized that the department was running out of time to get a contract in place, she decided to circumvent the proper process by creating a bogus contract document, forging required signatures, and sending the contract, which would otherwise appear to be appropriately approved, to the company.

To better coordinate functions of state government, the Governor, by Executive Order No. 36, transferred the contract, associated staff, and functional responsibilities from the Department of Safety to the Department of Revenue effective July 1, 2006. When an Assistant Fiscal Director at the Department of Revenue was unable to find the contract in the system in order to process a payment for a contractor invoice, he began asking questions and the lack of a properly executed contract came to light.

We expanded our review to search for other inappropriate transactions charged to transaction code 126. In our review of transactions, we found other instances where items appeared to have been charged incorrectly including payments to a local government data processing company under a sole source contract and payments to a university. Even though payments were processed incorrectly using the 126 transaction code, it appeared that the vendors were legitimate and did provide services to the state at what appeared to be a reasonable price. We found no evidence that the Fiscal Director personally profited from her conduct. Given no alternative, she subsequently retired from the Department of Safety in January 2007 in lieu of termination, and pursuant to Section 8-50-807(d), *Tennessee Code Annotated*, she forfeited 345 hours of annual leave valued at $10,908.90. She was also coded as not eligible for rehire in the state's system.

The Department of Finance and Administration's Office of Contract Review has established rules governing the state's contracts. These rules are designed to allow upper management to control the purchases of goods and services and to ensure that the state's purchases are made at the best price. Through the use of the prescribed procedures, the obligations of both parties are documented so there will be no misunderstanding about the goods or services to be provided and their cost. The state's established procedures also provide for the correct recording of payments made under contracts. However, upper management's lack of oversight of the contracting process at the Department of Safety allowed the Fiscal Director to circumvent the established state procedures, and the department's fiscal office had no written procedures for the approval and monitoring of expenditures charged to contracts. In addition, the Fiscal Director's level of access to the State of Tennessee Accounting and Reporting System (STARS) allowed her the ability to enter transactions for all of the department's allotment codes and to change cost centers and vendor files in the system. The Director of Fiscal Services' failure to monitor contract activities also increases the risk of fraudulent transactions.

Recommendation

The Commissioner in coordination with the Deputy Commissioner should appoint an employee with fiscal expertise to monitor all contracts. This person should report directly to the

Deputy Commissioner at least until such time as the Deputy Commissioner is assured that contract risks such as those identified have been mitigated. The person would be responsible for ensuring that all goods and services for the department are purchased through a valid contract. This person should have access to STARS to monitor the amount of expenditures charged as one-time purchases and determine if any should have been charged against an existing contract. He or she should also evaluate the goods or services being purchased and determine if other contracts may be needed. This person would be responsible for approving all contracts and expenditures charged to contracts. This employee should maintain a log of contracts in the approval process in order to ensure that the RFP process is properly followed.

The Director of Internal Audit should periodically monitor the contract process to ensure that the design and implementation of internal controls in this area are adequate.

As management continues their risk assessment activities, they should ensure that risks such as these noted in this finding are adequately identified and assessed in their documented risk assessment activities. Management should identify specific staff to be responsible for the design and implementation of internal controls to prevent and detect exceptions timely. Management should also identify staff to be responsible for ongoing monitoring for compliance with all requirements and taking prompt action should exceptions occur.

Management's Comment

We concur.

In March 2007 the Commissioner, in coordination with the Deputy Commissioner, appointed an employee with fiscal expertise to monitor all professional services contracts. This person serves as the Contract Services Coordinator (CSC) for those contracts processed through the Office of Contract Review. This individual reports directly to the Director of Fiscal Services to assure the Deputy Commissioner that contract risks as identified by the Comptroller have been mitigated.

The Contract Services Coordinator, in coordination with the Director of Fiscal Services, is responsible for ensuring that all goods and services for the department are purchased through a valid contract. The CSC has inquiry only access to STARS to monitor the amount of expenditures charged as one-time purchases and determine if any should have been charged against an existing contract. The CSC does not have access to record or enter contract transactions in the state's financial system, nor does the CSC have signature authority for the Director of Fiscal Services or the Commissioner.

The CSC, in conjunction with the Director of Fiscal Services, evaluates the goods or services being purchased and determines if other professional service contracts may be needed. The CSC and the applicable Section Head are responsible for approving all invoices and expenditures charged to professional services contracts. The CSC maintains a log of

RFPs/contracts in the approval process in order to ensure that the RFP/contract process is properly followed.

Management will ensure that risks such as these noted in this finding are adequately identified and assessed in their documented risk assessment activities. The Director of Fiscal Services is responsible for the design and implementation of internal controls to prevent and detect exceptions timely and to monitor contract activities. The Contract Services Coordinator is responsible for ongoing monitoring for compliance with all requirements and in conjunction with the Director of Fiscal Services taking prompt action should exceptions occur.

The Director of Internal Audit will periodically monitor the contract process to ensure that the design and implementation of internal controls in this area are adequate.

EVIDENCE ROOMS

The objectives of our review of evidence rooms were to determine whether

- evidence was properly recorded and properly controlled;
- confiscated money was deposited timely;
- an inventory of the evidence rooms was periodically performed; and
- the disposition of evidence was proper.

We obtained the audit reports and working papers from Internal Audit for their reviews of the evidence rooms at the Cookeville and Jackson Tennessee Highway Patrol (THP) district offices and reviewed them to see what types of problems they found. During May and June 2007, we interviewed key personnel and made observations at the other six Tennessee Highway Patrol (THP) district offices and the scale houses in Manchester and Greene County to gain an understanding of the controls and procedures over evidence. We obtained the evidence log books from the Evidence Custodian at each location. We tested a nonstatistical sample of items from the log books to determine if evidence was handled properly according to the department's General Orders and evidence standards, including whether evidence was properly recorded and properly controlled; the deposit of confiscated money was timely; and the disposition of evidence was proper. We made inquiries of staff to determine whether the evidence rooms had been inventoried. We performed a walk-through of each evidence room and examined all property in the evidence room to determine if the property was sealed and labeled and was actual evidence and to determine that no money had been left in the evidence room.

Based on our reviews, interviews, observations, and testwork, we determined that

- evidence was not always properly recorded and properly controlled;
- confiscated money was not always deposited timely;

- periodic inventories had not been performed for some evidence rooms; and
- the disposition of evidence was not always proper.

However, similar problems were identified in the audits performed by Internal Audit at the Cookeville and Jackson THP District Offices, and department personnel had already begun a major overhaul of the evidence room operations statewide.

EQUIPMENT

The objectives of our review of equipment were to follow up on a prior audit finding and to determine whether

- access to the Property of the State of Tennessee (POST) system was limited to employees whose job duties required access and the access did not create an inadequate segregation of duties;
- the information in POST for equipment assigned to the department was accurate;
- equipment assigned to the department could be located and was properly tagged;
- an annual physical inventory of all capitalized equipment was performed;
- total POST acquisitions during the period reconciled to total State of Tennessee Accounting and Reporting System (STARS) expenditures charged to object code 16 (equipment that is capitalized and $5,000 or more) for the period; and
- lost or stolen equipment was promptly reported to the Comptroller's office and was removed from POST timely.

We interviewed key personnel to gain an understanding of the procedures used to ensure that all equipment assigned to the department was properly accounted for and safeguarded. We obtained a listing of all persons with access to POST at April 26, 2007, from the Department of General Services and compared the list to the Payroll Register for April 2007 to determine if only active employees had access to POST. We tested a nonstatistical sample of active employees with POST access to determine if the employees' job duties required the level of access given and the access did not create an inadequate segregation of duties. We obtained an equipment list from the Department of General Services of items costing $5,000 or more assigned to the Department of Safety at May 1, 2007. We selected a nonstatistical sample of equipment items from this list to locate and determine if the information in POST was accurate and the equipment had a state tag attached. We also reviewed the list to determine if all equipment with an acquisition date prior to April 2007 had an inventory date after December 31, 2005. We compared the total cost of all equipment listed with an acquisition date between July 1, 2005, and February 28, 2007, with the total STARS expenditures for equipment for the same period to determine if the totals reconciled. We reviewed a sample of lost or stolen equipment from the reports sent to

the Comptroller's office from July 1, 2005, through April 26, 2007, to determine the timeliness of the reports and the timeliness of the related adjustments to POST.

Based on our interviews, reviews, and testwork, we determined that

- with minor exceptions, access to POST was limited to employees whose job duties required access and the access did not create an inadequate segregation of duties;
- with minor exceptions, the information in POST for the equipment assigned to the department was accurate;
- the sample equipment items were located in the department and were properly tagged;
- the department performed an annual physical inventory of all capitalized equipment;
- total POST acquisitions during the period reconciled to total STARS expenditures charged to object code 16 for the period based on a reconciliation from the Department of Finance and Administration; and
- although all equipment reported as lost or stolen was removed from POST timely, lost and stolen property was not always reported to the Comptroller's office timely (the items noted were part of a large write-off which resulted from work undertaken by the department's Internal Audit staff to properly inventory equipment).

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. In addition, the head of each executive agency is required to conduct an evaluation of the agency's internal accounting and administrative control and submit a report by December 31, 1999, and December 31 of every fourth year thereafter.

Our objective was to determine whether the department's June 30, 2007, and June 30, 2006, responsibility letters were filed in compliance with Section 9-18-104, *Tennessee Code Annotated.*

We reviewed the June 30, 2007, and June 30, 2006, responsibility letters submitted to the Comptroller of the Treasury and the Department of Finance and Administration to determine adherence to the submission deadline, and we determined that the Financial Integrity Act responsibility letters were submitted on time.

TITLE IX OF THE EDUCATION AMENDMENTS ACT OF 1972

Title IX of the Education Amendments Act of 1972 is a federal law. The act requires all state agencies receiving federal money to develop and implement plans to ensure that no one receiving benefits under a federally funded education program and activity is discriminated against on the basis of gender.

Section 4-4-123, Tennessee Code Annotated, requires each state governmental entity subject to the requirements of Title IX of the Education Amendments Act of 1972 (20 United States Code, Section 1681 et seq.) to develop a Title IX implementation plan and submit annual Title IX compliance reports and implementation plan updates to the Department of Audit by June 30, 1999, and each June 30 thereafter.

Our objective was to determine whether the department filed its compliance reports and implementation plans under Title IX. We discussed Title IX compliance with the Title IX Coordinator and reviewed the documentation that he provided. Based on our inquiries and review, we determined that the Department of Safety had not developed and submitted a Title IX implementation plan for fiscal year 2006 and fiscal year 2007; however, as of July 1, 2007, the department is no longer receiving federal funding for the applicable program.

OBSERVATIONS AND COMMENTS

MANAGEMENT'S RESPONSIBILITY FOR RISK ASSESSMENT

Auditors and management are required to assess the risk of fraud in the operations of the entity. The risk assessment is based on a critical review of operations considering what frauds could be perpetrated in the absence of adequate controls. The auditors' risk assessment is limited to the period during which the audit is conducted and is limited to the transactions that the auditors are able to test during that period. The risk assessment by management is the primary method by which the entity is protected from fraud, waste, and abuse. Since new programs may be established at any time by management or older programs may be discontinued, that assessment is ongoing as part of the daily operations of the entity.

Risks of fraud, waste, and abuse are mitigated by effective internal controls. It is management's responsibility to design, implement, and monitor effective controls in the entity. Although internal and external auditors may include testing of controls as part of their audit procedures, these procedures are not a substitute for the ongoing monitoring required of management. After all, the auditor testing is limited and is usually targeted to test the effectiveness of particular controls. Even if controls appear to be operating effectively during the time of the auditor testing, they may be rendered ineffective the next day by management override or by other circumventions that, if left up to the auditor to detect, will not be noted until

the next audit engagement and then only if the auditor tests the same transactions and controls. Furthermore, since staff may be seeking to avoid auditor criticisms, they may comply with the controls during the period that the auditors are on site and revert to ignoring or disregarding the control after the auditors have left the field.

The risk assessments and the actions of management in designing, implementing, and monitoring the controls should be adequately documented to provide an audit trail both for auditors and for management, in the event that there is a change in management or staff, and to maintain a record of areas that are particularly problematic. The assessment and the controls should be reviewed and approved by the head of the entity.

FRAUD CONSIDERATIONS

Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit*, promulgated by the American Institute of Certified Public Accountants requires auditors to specifically assess the risk of material misstatement of an audited entity's financial statements due to fraud. The standard also restates the obvious premise that management, not the auditors, is primarily responsible for preventing and detecting fraud in its own entity. Management's responsibility is fulfilled in part when it takes appropriate steps to assess the risk of fraud within the entity and to implement adequate internal controls to address the results of those risk assessments.

During our audit, we discussed these responsibilities with management and how management might approach meeting them. We also increased the breadth and depth of our inquiries of management and others in the entity as we deemed appropriate. We obtained formal assurances from top management that management had reviewed the entity's policies and procedures to ensure that they are properly designed to prevent and detect fraud and that management had made changes to the policies and procedures where appropriate. Top management further assured us that all staff had been advised to promptly alert management of all allegations of fraud, suspected fraud, or detected fraud and to be totally candid in all communications with the auditors. All levels of management assured us there were no known instances or allegations of fraud that were not disclosed to us.

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 Safety filed its compliance reports and implementation plans for the years ended June 30, 2006, and June 30, 2007, on July 5, 2005, and June 30, 2006, respectively.

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 Tennessee Title VI Compliance Commission is responsible for monitoring and enforcement of Title VI.

APPENDICES

MANAGEMENT'S COMMENT FROM PRIOR AUDIT

Current Finding

Management still has not adequately monitored access to the Driver License System by individuals from outside agencies, resulting in instances of unauthorized access

Management's Comment

For the Period July 1, 2000, Through June 16, 2003

We concur. The department has initiated a review of access to all of the state's computer applications. The Commissioner has requested reports of all persons who have access to departmental applications and departmental networks. The Director of each division will be required to review his or her employees' access on each computer system and network. The directors will also be required to review and submit to the Information System Director minimum levels of access required to perform their job duties. The Information Systems Director will develop policy and procedures requiring annual review of access to departmental information systems and networks. These procedures will incorporate a policy to ensure all employees are reviewed either annually or upon position termination/change. We have initiated changes in procurement practices to preclude any person having the authority to initiate, approve, and receive purchases.

The Director of the Driver License Division or a designee will periodically review a report from our Information Systems Division on all driver license employees' access levels. This report will be reviewed and appropriate action will be taken to ensure that access levels for all driver license employees are authorized at the minimum levels for employees to efficiently perform their assigned job responsibilities.

ALLOTMENT CODES

Department of Safety divisions and allotment codes:

349.01 Administration
349.02 Driver's License Issuance
349.03 Highway Patrol
349.04 Motorcycle Rider Education
349.06 Auto Theft Investigations
349.07 Motor Vehicle Operations
349.08 Driver Education

349.09 Tennessee Law Enforcement Training Academy
349.10 POST Commission
349.11 Title and Registration
349.12 Major Maintenance
349.13 Technical Services
349.14 CID Anti-theft