STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY

Office of the Comptroller of the Treasury

Performance Audit Report

January 2013

Justin P. Wilson
Comptroller of the Treasury

Department of Audit
Division of State Audit
Risk-Based Performance Audit Group

ARTHUR A. HAYES, JR., CPA, JD, CFE, CGFM
Director

KANDI B. THOMAS, CPA, CFE, CGFM
Assistant Director

SHIRLEY A. HENRY, CPA, CGFM
Audit Manager

Laura Isbell, CPA, CFE
In-Charge Auditor

Sarina Oster, CPA, CFE
Staff Auditor

Amy Brack
Editor

Comptroller of the Treasury, Division of State Audit
1500 James K. Polk Building
Nashville, TN 37243-1402
(615) 401-7897

Reports are available at
www.comptroller.tn.gov/sa/AuditReportCategories.asp.

Mission Statement
The mission of the Comptroller's Office is to improve the quality of life for all Tennesseans by making government work better.

Comptroller Website
www.comptroller.tn.gov

STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY
DEPARTMENT OF AUDIT
DIVISION OF STATE AUDIT
SUITE 1500
JAMES K. POLK STATE OFFICE BUILDING
NASHVILLE, TENNESSEE 37243-1402
PHONE (615) 401-7897
FAX (615) 532-2765

January 3, 2013

The Honorable Ron Ramsey
Speaker of the Senate
and
The Honorable Beth Harwell
Speaker of the House of Representatives
and
Members of the General Assembly
State Capitol
Nashville, Tennessee 37243
and
The Honorable Justin P. Wilson
Comptroller of the Treasury
State Capitol
Nashville, Tennessee 37243

Ladies and Gentlemen:

We have conducted a performance audit of selected programs and activities of the Office of the Comptroller of the Treasury for the period July 1, 2011, through June 30, 2012, and other periods for which management requested additional review.

Since we are not independent with respect to the Office of the Comptroller of the Treasury, we do not express any assurance on internal control and on compliance.

Our audit disclosed certain findings which are detailed in the Objectives, Methodologies, and Conclusions section of this report. Management of the Office of the Comptroller of the Treasury 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 office's internal control to the Office of the Comptroller of the Treasury's management in a separate letter.

Sincerely,

Arthur A. Hayes, Jr., CPA
Director

AAH/sah
13/016

State of Tennessee

Audit Highlights

Comptroller of the Treasury | Division of State Audit

Performance Audit
Office of the Comptroller of the Treasury
January 2013

AUDIT SCOPE

We have audited the Office of the Comptroller of the Treasury for the period July 1, 2011, through June 30, 2012, and other periods for which management requested additional review. Our audit scope included a review of internal control and compliance with laws, regulations, and provisions of contracts or grant agreements in the areas of fiscal operations, human resources, and information systems.

The auditors are not considered independent of the audited entity because they are employees of the Office of the Comptroller of the Treasury.

AUDIT FINDINGS

Since 1990, the Office of the Comptroller of the Treasury Has Operated a Non-state Bank Account for the Purpose of Sponsoring Its Annual Educational and Networking Event for the State's Property Assessors and Division Staff

The Division of Property Assessments established a non-state bank account to deposit registration fees for the annual Assessor Retreat and to make payments for retreat-related expenses. Based on our review of the related documentation and discussions with management, the decision to establish a non-state bank account was inconsistent with the Department of Finance and Administration's policies (page 12).

The Office Did Not Follow Information Systems' Industry Best Practices Regarding Computer Access, Resulting in the Increased Risk of Fraudulent Activity or Loss of Data

Based on our computer access testwork, the office did not follow information systems' industry best practices regarding user access (page 18).

Performance Audit
Office of the Comptroller of the Treasury

TABLE OF CONTENTS

	Page
INTRODUCTION	1
Post-Audit Authority	1
Background	1
AUDIT SCOPE	3
PRIOR AUDIT FINDINGS	3
OBJECTIVES, METHODOLOGIES, AND CONCLUSIONS	5
Fiscal Operations	5
Finding 1 – Since 1990, the Office of the Comptroller of the Treasury has operated a non-state bank account for the purpose of sponsoring its annual educational and networking event for the state's property assessors and division staff	12
Human Resources	14
Information Systems	15
Finding 2 – The office did not follow information systems' industry best practices regarding computer access, resulting in the increased risk of fraudulent activity or loss of data	18
APPENDICES	20
Business Unit Codes	20
Boards and Commissions	21

Performance Audit
Office of the Comptroller of the Treasury

INTRODUCTION

POST-AUDIT AUTHORITY

This is the report on the audit of the Office of the Comptroller of the Treasury. 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 Comptroller of the Treasury is a constitutional officer elected by the General Assembly for a two-year term. The functions and duties of the office are assigned through various legislative enactments. The Office of the Comptroller of the Treasury is organized into several divisions and offices to discharge its statutory duties. The basic functions of the divisions and offices are described below.

The Division of Administration provides direction, coordination, and supervision to the divisions and offices within the Comptroller's Office and represents the Comptroller on various boards and commissions.

The Office of Management Services provides administrative and support services to the divisions and offices of the Comptroller's Office in the areas of accounting, budgeting, human resources, and information systems. The office also assists the Comptroller in policy and contract matters and provides staff support for several boards and commissions.

The Division of State Audit conducts financial and compliance and performance audits and performs special studies to provide the General Assembly, the Governor, and citizens of Tennessee with objective information about the state's financial condition and the performance of the state's many agencies and programs. Under an agreement with the Department of Finance and Administration, the TennCare section of the division performs certain audit and rate-setting functions for the state's TennCare program.

The Division of Local Government Audit, created in fiscal year 2012 from the merger of the Division of County Audit and the Division of Municipal Audit, is responsible for annual audits of all 95 counties in the state and ensures that municipalities, designated school system funds, utility districts, and government-funded nonprofit agencies are audited as required by state statute. The division also establishes standards for county audits conducted by public accounting firms and assists local governments with financial administration questions.

The Division of Investigations was established during fiscal year 2012 by consolidating the investigative functions of State Audit, County Audit, and Municipal Audit. The division investigates and issues reports on allegations of misconduct, fraud, or waste in state and local government, often referring findings to other agencies for appropriate action.

The Office of State and Local Finance manages the state debt, including issuance of all bonds and notes and payment of such debt, and serves as staff for the State Funding Board, Tennessee State School Bond Authority, Tennessee Local Development Authority, and the Bond Finance Committee of the Tennessee Housing Development Agency. The office also approves certain debt obligations of local governments, approves budgets of local governments which have certain debt obligations outstanding, and assists local governments with other debt and financial management issues.

The Division of Property Assessments assists local governments in assessment of property for tax purposes and administers the property tax relief program, which provides reimbursements to low-income elderly or disabled persons and certain disabled veterans or their surviving spouses.

The Office of State Assessed Properties annually appraises and assesses all public utility and transportation properties as prescribed in Section 67-5-1301, *Tennessee Code Annotated.* These assessments are certified to counties, cities, and other taxing jurisdictions for the billing and collection of property taxes.

The Office of Local Government provides technical assistance to local governments in redistricting efforts and in establishing precincts, maintains county precinct information, and provides mapping services using geographic information systems (GIS) technology.

The Offices of Research and Education Accountability prepare reports at the request of the Comptroller and the General Assembly on various state and local government issues. The Office of Education Accountability monitors the performance of Tennessee's elementary and secondary school systems and provides the General Assembly with reports on selected education topics.

The Office of Open Records Counsel provides information and advice to citizens and local government officials regarding the Tennessee Public Records Act, collects data regarding Open Meetings Law inquiries and problems, and provides educational programs on Public Records and Open Meetings.

The State Board of Equalization is responsible for assuring constitutional and statutory compliance in assessments of property for ad valorem taxes. The board establishes rules and hears county and public utility assessment appeals. The board also reviews applications for religious, charitable, and related property tax exemptions; reviews certified tax rate calculations from jurisdictions undergoing revaluation; and regulates property tax appeals agents and agent practices. The board consists of the Governor, the State Treasurer, the Secretary of State, the Comptroller of the Treasury, the Commissioner of Revenue, one person named by the Governor at the city level, and one person named by the Governor at the county level.

The Office of Small Business Advocate provides information and answers questions for owners of businesses with 50 or fewer employees. The office may act as a mediator to help resolve issues involving small businesses and state departments and agencies.

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

AUDIT SCOPE

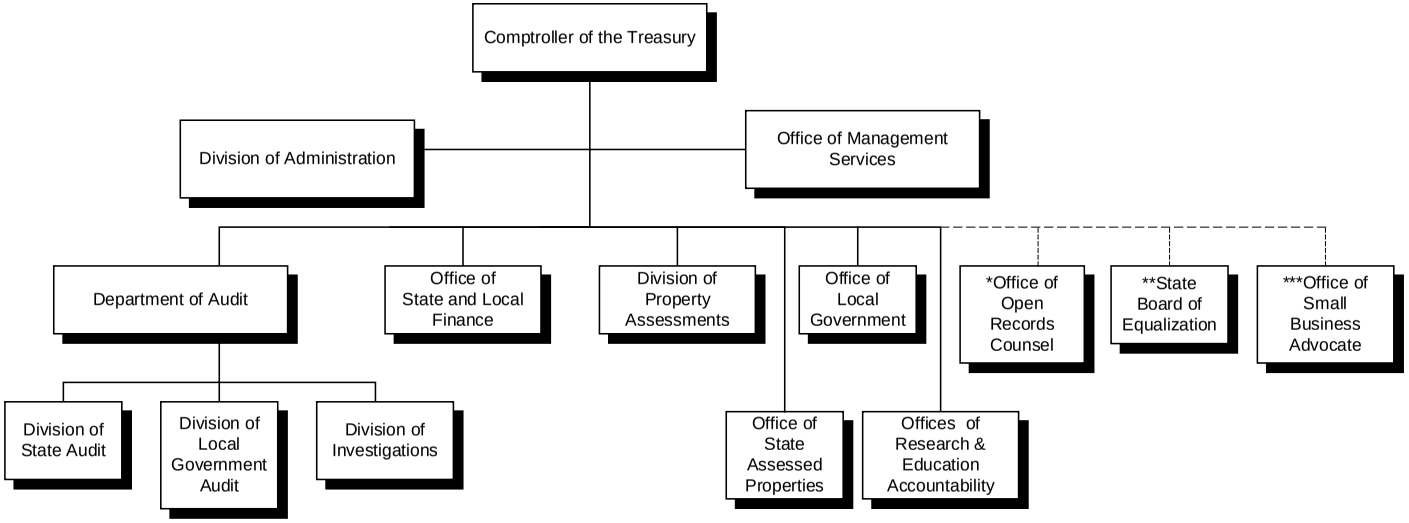
We have audited the Office of the Comptroller of the Treasury for the period July 1, 2011, through June 30, 2012, and other periods for which management requested additional review. Our audit scope included a review of internal control and compliance with laws, regulations, and provisions of contracts or grant agreements in the areas of fiscal operations, human resources, and information systems.

The auditors are not considered independent of the audited entity because they are employees of the Office of the Comptroller of the Treasury.

PRIOR AUDIT FINDINGS

There were no audit findings in the prior audit report.

Comptroller of the Treasury Organization Chart



*** The Office of Open Records Counsel is housed within the Comptroller's Office for administrative purposes.**
**** The Comptroller is a member of the State Board of Equalization, and the Board staff is housed within the Comptroller's Office for administrative purposes.**
*****The Office of Small Business Advocate is housed within the Comptroller's Office for administrative purposes.**

OBJECTIVES, METHODOLOGIES, AND CONCLUSIONS

FISCAL OPERATIONS

The Comptroller's Office receives approximately $10 million in annual revenues from Division of Property Assessments tax billings and course registration fees, audit and investigation billings, teaching contracts, State Board of Equalization surety billings, and State and Local Finance commercial paper and contract reimbursements, among other sources. The Comptroller's Office annually expends approximately $87 million on Tax Relief payments, Telecommunications Ad Valorem Tax Equity payments, payroll, computer system development, travel reimbursement, training, and other administrative items. The Fiscal Services section of the Office of Management Services coordinates and oversees the financial aspects of the Comptroller's Office, including accounting for all receipts and disbursements. As part of our review of fiscal operations for the Comptroller's Office, we focused on cash receipts, accounts receivable, and revenues; equipment; expenditures; and some miscellaneous issues. In some areas, management had requested that we review transactions going back to January 1, 2007. In areas where we performed a more extensive review, we refer to the period January 1, 2007, through June 30, 2012, as the "extended period."

Cash Receipts, Accounts Receivable, and Revenues

Our objectives in reviewing cash receipts, accounts receivable, and revenues were to determine whether

- the office had any unusual or suspicious cash receipts during the extended period and if so, based on further investigation, the receipts were reasonable considering the office's operations;

- for fiscal year 2012 cash receipts, the lag time between receipt and entry into the cashiering system was reasonable, deposits were made in compliance with applicable policies, and deposited amounts matched the form of the initial payment received;

- the office had any unusual or suspicious receivable transactions during the extended period and if so, based on further investigation, the transactions were reasonable considering the office's operations;

- for those receivables outstanding for six months or longer as of June 30, 2012, the office had a reasonable basis for establishing the receivable and made reasonable efforts to collect the amounts owed;

- the office followed relevant write-off policies for any receivable amounts written off during fiscal year 2012;

- the office had any unusual or suspicious revenues during the extended period and if so, based on further investigation, the revenues were reasonable considering the office's operations;

- the office experienced significant or unusual fluctuations in percentages of revenues received by division that required management explanations; and

- for fiscal year 2012, revenue transactions were adequately supported, revenue amounts agreed with supporting documentation, revenues were recorded properly, revenues received through the mail appeared on the revenue log, and the revenue transactions in the accounting system matched the revenue log entries.

To determine whether the office had any unusual or suspicious cash receipts during the extended period, we obtained and reviewed cash receipts listings for that time frame. To assess whether the cash receipts identified as unusual or suspicious were reasonable considering the office's operations, we analyzed the transaction details and the functions of the related divisions. For fiscal year 2012 cash receipts, to determine whether the lag time between receipt and entry into the cashiering system was reasonable, deposits were made in compliance with applicable policies, and deposited amounts matched the form of the initial payment received, we selected a random sample of 25 revenue transactions. For items received through the mail, we reviewed the deposit entry in the accounting system, revenue logs, deposit slips, and other documentation supporting the cash receipt. We also reviewed the Department of Finance and Administration's (F&A) Policy 25, "Deposit Practices Policy."

To evaluate whether the office had any unusual or suspicious receivable transactions during the extended period, we obtained and inspected listings of receivable transactions for that time frame. To identify those receivables outstanding for six months or longer as of June 30, 2012, we obtained a listing of outstanding receivables as of October 29, 2012, and the Receivables Aging Report as of June 30, 2012, and calculated the number of days the receivables had been outstanding as of June 30, 2012. To determine whether the office had a reasonable basis for establishing the receivable, we studied the documentation supporting the receivable. To assess whether the office made reasonable efforts to collect the amounts owed, we reviewed monthly dunning letters, which were sent out to remind each debtor of the amount owed, and F&A's Policy 23, "Accounts Receivable—Recording, Collection, and Write-offs." To discern whether the office wrote off any receivable amounts during fiscal year 2012, we inspected the office's analysis of accounts receivable collectability, which the office submitted to F&A.

To determine whether the office had any unusual or suspicious revenues during the extended period, we obtained and scanned revenue listings for that period. To evaluate whether the revenues identified as unusual or suspicious were reasonable considering the office's operations, we scrutinized the transaction details and the functions of the associated divisions. To determine whether the office experienced significant or unusual fluctuations in revenues, we obtained a summary of all revenues by division for the Comptroller's Office. We analyzed the changes in revenues from 2009 through 2011 and estimated the expected revenues for fiscal year

2012. To test fiscal year 2012 revenue transactions, in conjunction with the cash receipts sample testwork described above, we consulted with applicable personnel, reviewed supporting documentation for each transaction, compared the amounts on the supporting documentation with the amounts for the revenue entry in the accounting system, and inspected revenue logs.

Based on the procedures performed, we determined that

- based on further investigation, cash receipts during the extended period that initially appeared unusual or suspicious were reasonable considering the office's operations;

- for fiscal year 2012 cash receipts, the lag time between receipt and entry into the cashiering system was reasonable, deposits were made in compliance with applicable policies, and deposited amounts matched the form of the initial payment received;

- the office had no unusual or suspicious receivable transactions during the extended period;

- for those receivables outstanding for six months or longer as of June 30, 2012, the office had a reasonable basis for establishing the receivable and made reasonable efforts to collect the amounts owed;

- the office did not write off any receivable amounts during fiscal year 2012;

- based on further investigation, the revenues for the extended period identified as unusual or suspicious were reasonable considering the office's operations;

- the office experienced no significant or unusual fluctuations in revenues; and

- for fiscal year 2012, revenue transactions were adequately supported, revenue amounts agreed with supporting documentation, revenues were recorded properly, revenues received through the mail appeared on the revenue log, and the revenue transactions in the accounting system matched the revenue log entries.

Equipment

Our objectives in reviewing equipment were to determine whether

- the Comptroller's Office had located the seven equipment items that had not been found during prior inventory counts and if those items could not be located, the office took appropriate subsequent actions and

- perpetual inventory records matched fiscal year 2012 inventory counts.

We obtained a listing of the seven equipment items that had not been found during prior inventory counts. To determine whether the seven pieces of equipment had been located and if

the office took appropriate subsequent actions for any items that could not be located, we obtained and analyzed the results of the office's fiscal year 2012 inventory count and reviewed correspondence showing that the office had reported certain items as lost. To assess whether perpetual inventory records matched fiscal year 2012 inventory counts, we interviewed key personnel, inspected the fiscal year 2012 inventory results and the related lost items list, and reviewed inventory instructions developed by both F&A and internally by office management.

Based on the procedures performed, we determined that

- the Comptroller's Office located two of the seven equipment items and the other five items that could not be located were properly reported as lost and

- perpetual inventory records matched fiscal year 2012 inventory counts, except for minor differences.

Expenditures

Our objectives in reviewing expenditures were to determine whether

- the office had any unusual or suspicious expenditures during the extended period and if so, based on further investigation, the expenditures were reasonable considering the office's operations;

- the office experienced significant or unusual fluctuations in percentages of expenditures by division which required management explanations;

- travel expenditures incurred by key Management Services and fiscal staff complied with applicable travel regulations and were reasonable and necessary;

- travel expenditures incurred by other office personnel complied with applicable travel regulations and were reasonable and necessary;

- the office had appropriate procedures in place to mitigate risks resulting from unused airline tickets;

- fiscal year 2012 Integrated Multi Processing of Administrative and CAMA Technology (IMPACT) system expenditures were in compliance with applicable contract provisions, necessary and reasonable, and not a duplicate of other payments made and whether the source document submitted was formatted consistently with other such documents submitted by the vendor and management's signatures on the source document were consistent with the signatures on other documents;

- the office had procurement card controls in place;

- procurement cards were used during fiscal year 2012 to make any unusual or suspicious purchases and if so, based on further investigation, the expenditures were reasonable considering the office's operations;

- other expenditures were necessary and reasonable and not a duplicate of other payments made and whether the source document submitted was formatted consistently with other such documents submitted by the vendor and management's signatures on the source document were consistent with the signatures on other documents;

- the office had appropriate policies and procedures in place to prevent unauthorized WeCar Program expenditures; and

- the office appropriately included the risks related to the WeCar Program in its risk assessment.

To determine whether the office had any unusual or suspicious expenditures during the extended period, we obtained and reviewed expenditure listings for that period. For unusual or suspicious expenditures identified, we conferred with key personnel, performed Internet searches, and evaluated related supporting documentation. To evaluate whether the office experienced significant or unusual fluctuations in expenditures, we obtained a summary of all expenditures by division for the Comptroller's Office. We analyzed the changes in expenditures from 2009 through 2011 and estimated the expected expenditures for fiscal year 2012. We discussed with management any significant or unusual fluctuations identified and inspected documentation corroborating management's explanations.

We identified eight key Management Services and fiscal staff by reviewing the office's organizational charts and obtained a listing of all travel claims submitted by those personnel and approved for payment during fiscal year 2012. To determine whether those travel expenditures complied with applicable travel regulations and were reasonable and necessary, we performed inquiries with applicable personnel, inspected documentation supporting the travel claim, and reviewed travel regulations promulgated by both F&A and the Comptroller's Office. To determine whether travel expenditures incurred by other office personnel complied with applicable travel regulations and were reasonable and necessary, we selected a random sample of 25 travel claims from fiscal year 2012, documented the position title of the employee submitting the travel claim, scrutinized supporting documentation, and read F&A and Comptroller's office travel regulations. To determine whether the office had appropriate procedures in place to mitigate risks resulting from unused airline tickets, we asked various personnel to obtain the number, dollar amount, and status of the unused airline tickets. We also reviewed airline policies and procedures.

We extracted a listing of all fiscal year 2012 IMPACT expenditures and obtained copies of the IMPACT contract and related amendments. We inspected the source documents for the expenditures and evaluated the expenditures against contract provisions, reviewed other payments made to the vendor to identify any duplicates, compared the formatting of the source

documents with other such documents submitted by the vendor, and compared management's signatures on the source documents with the signatures on other documents for consistency.

To assess whether the office had procurement card controls in place, we interviewed key personnel and reviewed F&A's *State of Tennessee State Payment Card Cardholder/Approver Manual*; F&A's Policy 29, "State Contracts for Credit and Debit Cards"; state procurement card documentation templates; and the Department of General Services' *Purchasing Policy Manual*. We also reviewed a listing of the office's procurement card holders and reviewers, obtained a listing of all of the office's procurement card purchases during the extended period, and reviewed examples of procurement card receipts and transaction logs. To determine whether procurement cards were used during fiscal year 2012 to make any unusual or suspicious purchases, we scanned a listing of the fiscal year procurement card purchases. For unusual or suspicious procurement card purchases identified, we obtained explanations from applicable personnel, performed Internet searches, reviewed supporting documentation, and assessed the purchases against the normal duties performed by the division involved.

We selected and tested a random sample of 25 non-payroll expenditure transactions from fiscal year 2012. We analyzed source documents for those transactions, reviewed other payments made to that vendor and associated source documents, and juxtaposed management's signatures on the source document with the signatures on other documents. To determine whether the office had appropriate policies and procedures in place to prevent unauthorized WeCar Program expenditures, we conducted inquiries with key personnel and reviewed documentation describing the office's procedures for processing and reviewing WeCar expenditures. To evaluate whether the office appropriately included the risks related to the WeCar Program in its risk assessment, we interviewed management and scrutinized the office's December 2011 risk assessment.

Based on the procedures performed, we determined that

- based on further investigation, the unusual or suspicious expenditures identified for the extended period were reasonable considering the office's operations;

- the significant variances we noted between our estimated expenditures and the current year amounts were adequately explained by management;

- travel expenditures incurred by key Management Services and fiscal staff complied with applicable travel regulations and were reasonable and necessary;

- travel expenditures incurred by other office personnel complied with applicable travel regulations and were reasonable and necessary;

- the office was aware of the unused airline tickets and was in the process of developing procedures to mitigate the resulting risks;

- fiscal year 2012 Integrated Multi Processing of Administrative and CAMA Technology (IMPACT) system expenditures were in compliance with applicable

contract provisions, necessary and reasonable, and not a duplicate of other payments made and the source document submitted was formatted consistently with other such documents submitted by the vendor and management's signatures on the source document were consistent with the signatures on other documents;

- the office had procurement card controls in place;

- based on further investigation, unusual or suspicious procurement card purchases during fiscal year 2012 were reasonable considering the office's operations;

- other expenditures were necessary and reasonable and not a duplicate of other payments made and the source document submitted was formatted consistently with other such documents submitted by the vendor and management's signatures on the source document were consistent with the signatures on other documents;

- the office had appropriate policies and procedures in place to prevent unauthorized WeCar Program expenditures; and

- office personnel did not include WeCar Program risks in the December 2011 risk assessments because they were not alerted to the implementation of the new program until January 2012, but the office does plan to address WeCar risks in the risk assessments due in December 2012.

Miscellaneous

Our objectives in reviewing the miscellaneous issues were to determine whether

- transactions indicative of fictitious vendors, ghost employees, or other improprieties existed and if any such transactions were identified, the transactions were appropriate based on further review and

- businesses owned by key Comptroller's Office employees received any payments from the office for the extended period and if so, any payments identified were proper and transparent.

To identify transactions indicative of fictitious vendors, ghost employees, or other improprieties, we performed a series of computer-assisted audit techniques (CAATs) for the extended period. To assess the existence of fictitious vendors, we performed CAATs to identify single payment vendors; payments to vendors with Post Office (P.O.) box addresses; payments to vendors with mail drop addresses; vendors paid within seven days or less of invoice date; duplicate payments by vendor name and absolute value amount; duplicate payments by invoice number, vendor name, and absolute value amount; and duplicate payments by vendor name, and we created summaries by vendor and payment reference ID. We also performed CAATs to identify rounded invoice amounts; payments to vendors with no address information; payments made on weekends; vendors matching employee names or with employee Social Security

Numbers (SSNs); and vendor addresses matching employee addresses. To determine whether ghost employees existed, we performed CAATs to detect duplicate home addresses, duplicate phone numbers, duplicate bank accounts, and payments to P.O. boxes. To identify other improprieties, we further evaluated the results of the fictitious vendor and ghost employee CAATs and performed additional CAATs to look for payments with the same SSN and the same check date; paychecks with the same SSN, check date, and absolute value gross amount; paychecks with the same SSN, pay period date, and absolute value gross amount; and payments with terms related to cash, financial institutions, or other higher-risk items. We analyzed and evaluated the CAATs results by inspecting supporting documentation for transactions, comparing vendor information for consistency, performing Internet searches, conferring with key personnel, and reviewing purchasing regulations.

To determine whether 19 key Comptroller's Office employees owned businesses, we executed searches on the Secretary of State website and on general Internet search engines. We reviewed listings of all expenditures for the extended period to see if the office made payments to the names of companies owned by the employees.

Based on the procedures performed, we determined that

- although no transactions indicative of fictitious vendors or ghost employees were identified, the Comptroller's Office had a non-state bank account, as described in finding 1; and

- some key employees did own companies operating in the State of Tennessee although the office did not make any payments to those company names during the extended period.

1. Since 1990, the Office of the Comptroller of the Treasury has operated a non-state bank account for the purpose of sponsoring its annual educational and networking event for the state's property assessors and division staff

Finding

In 1990 the Office of the Comptroller of the Treasury established the Assessor Retreat to provide educational and networking opportunities for both county property assessors and state personnel associated with the Comptroller Office's Division of Property Assessments (DPA). In the first year of the Assessor Retreat, DPA's Assistant to the Comptroller for Assessments set up the retreat as a separate vendor at the recommendation of a former Office of Management Services (OMS) Assistant Director of Fiscal Services because DPA did not intake revenues and also to expedite the processing of transactions and ensure that the costs for the retreat remained as low as possible. To account for the fiscal operations of the Assessor Retreat, the Assistant to the Comptroller for Assessments established a non-state bank account that DPA personnel could use to collect and deposit retreat registration fees and to make payments for retreat-related

expenses. Since 2010, based on the annually estimated budgets for the Assessor Retreat, deposits and withdrawals for each annual retreat have totaled approximately $20,000.

As a routine audit procedure, on August 30, 2012, we asked the OMS Fiscal Officer to complete and sign a Bank Disclosure Form, certifying that he had disclosed all bank accounts, both official and unofficial, that the Comptroller's Office uses. He stated that he did not disclose the Assessor Retreat bank account because he was not aware of its existence since the retreat was coordinated outside of OMS operations.

We discovered this non-state bank account while performing computer-assisted audit techniques on Comptroller's Office expenditures for the period January 1, 2007, through June 30, 2012. Once we became aware of the bank account, we reviewed the receipts, checks, deposit slips, and other documentation for the 2010 through 2012 Assessor Retreats, and we reviewed the retreat account bank statements dating back to August 1998. Based on our review, the receipts, deposits, bank statements, and other retreat documentation appeared to be complete and well organized. Specifically, we did not identify any suspicious activity or inappropriate purchases. In addition, during our review, the Assistant to the Comptroller for Assessments was very forthcoming about the Assessor Retreat, and based on our inquiries, the Assessor Retreat bank account appears to have been created with good intentions.

Since state officials plan and organize this annual retreat and do so at least partially on state time and using state resources, we believe the original decision to open a non-state bank account is inconsistent with the state's Department of Finance and Administration Policy 7, "Petty Cash and Departmental Bank Accounts." Section 07-02-101 of F&A Policy 7 states that when "funds obtained by state employees or agents in the course of their state employment" are placed in a bank account, "the bank accounts are state funds and are subject to this policy statement and all applicable laws, rules and regulations pertaining to state funds."

Without proper transparency and accountability for the Assessor Retreat and the related fiscal operations and without documentation of the Comptroller Office's compliance with the state's procurement policies and procedures, the office and DPA increase the potential risks of noncompliance, fraud, waste, and abuse.

We also reviewed the risk assessment prepared by management of the Comptroller's Office. We determined that management had not identified and assessed the risks associated with unauthorized bank accounts in its risk assessment.

Recommendation

In order to increase transparency and accountability, the Director of Management Services, the Assistant to the Comptroller for Assessments, and the Management Services Assistant Director of Fiscal Services should work together to completely integrate the Assessor Retreat with regular Comptroller's Office operations. Specifically, registration fees and expenses should be processed through the office, and funds should be deposited into an official, state-

owned bank account authorized by the Department of Finance and Administration. This bank account should be appropriately listed on the office's Bank Account Disclosure Form.

The Comptroller of the Treasury should ensure that risks such as those noted in this finding are adequately identified and assessed in management's documented risk assessment.

Management's Comment

We concur with the recommendation to deposit the Assessor Retreat registration fees into an official, state-owned bank account. The accountability has always been present with this account, but we agree that the recommended scenario will provide more transparency. When the account was established 22 years ago, staff may have relied on their interpretation of Policy 7. We agree with the auditor's observation that the account was created with good intentions. Transparency is of the utmost importance to our office, and we are eager to provide such transparency across all our operations and to ensure that complete documentation and effective controls continue with regard to this account.

We have added consideration of this account to our current risk assessment.

HUMAN RESOURCES

The Human Resources section in the Office of Management Services (OMS) provides centralized services for all divisions and offices in the Comptroller's Office through the following functions: Affirmative Action Plan and Occupational Safety and Health Administration compliance reporting, policy administration, recruitment activities, employee/management time and attendance services, employee/management assistance programs, employee/management training and development, employee benefits, transit and notary services, and statewide sponsored employee programs.

The objectives of our review of Human Resources were to determine whether

- the Comptroller's Office had procedures to monitor leave without pay;
- the office properly monitored those employees whose number of hours worked fell below the threshold for leave accrual and/or insurance benefits;
- the office appropriately included the risk of leave without pay in its risk assessment; and
- the Human Resources section properly handled requests for personnel action.

To gain an understanding of the policies and procedures related to monitoring and managing leave without pay, we interviewed key personnel and reviewed the following documentation: the office's Family Medical Leave Act policy, the State Group Insurance Program "2012 Eligibility and Enrollment Guide," the Department of Human Resources' "New Employee Orientation" document, and the *Rules of Tennessee Department of Human Resources*, Chapter 1120-06.09, "Attendance and Leave." We analyzed the Human Resources section's fiscal year 2012 leave without pay report, employee hours worked report, and the leave without pay listing for the June 16 through June 30, 2012, payroll period to determine if there were any employees with substantial leave without pay to ensure that those employees were properly classified. In conjunction with that analysis, we reviewed documentation relating to employees' leave without pay status from their personnel files as necessary. To determine whether the office appropriately included the risk of leave without pay in its risk assessment, we examined the OMS Human Resources risk assessment.

To evaluate whether the Human Resources section properly handled requests for personnel action, we surveyed representatives from various Comptroller's Office divisions and reviewed the security request forms and other documentation related to personnel action requests that the divisional representatives provided. We also obtained and reviewed the Human Resources section's Employee and Job Data Changes form, Position Data Changes form, and New Hire form and consulted Edison manuals describing how dynamic groups and other time and labor processes work. We met with management to discuss any problems noted.

Based on the procedures performed, we determined that

- the Comptroller's Office had procedures to monitor leave without pay;
- the office properly monitored those employees whose number of hours worked fell below the threshold for leave accrual and/or insurance benefits;
- the Human Resources section appropriately included the risk of leave without pay in its risk assessment and documented related controls; and
- the Human Resources section properly handled requests for personnel action, with minor discrepancies.

INFORMATION SYSTEMS

The Information Technology (IT) section within the Office of Management Services (OMS) provides centralized services for all divisions and offices in the Comptroller's Office in the areas of technical planning and research; network access; electronic data protection, storage, and retention; technical hardware and software usage; and communication devices and software. The IT section also oversees the 41 Comptroller computer applications. In addition to the Comptroller computer applications, Comptroller's Office employees use Edison, the state's enterprise resource planning system. The OMS Human Resources section is responsible for

assigning employee access to Edison's Human Capital Module, while the OMS Fiscal Services section oversees the assignment of employee access to the Financial and Supply Chain Management module.

Our objectives in reviewing information systems were to determine whether

- policies and procedures were in place to provide reasonable assurance that the office would experience a minimal loss of data and function in case of an emergency;
- key employees were aware of the disaster recovery plan and prepared to carry it out in case of an emergency;
- the office had performed appropriate testing of its emergency preparedness procedures;
- access to the Edison and Comptroller computer applications was granted based on employees' job responsibilities;
- user access levels were updated as necessary as a result of recent organizational changes;
- access was set up to prevent a user from having incompatible duties;
- management followed information systems' industry best practices regarding computer access;
- employees changed their computer passwords every 90 days (30 days for system administrators) as prescribed by policy;
- the office had appropriately considered the risk of not changing passwords with the frequency prescribed by policy in its risk assessment;
- the IT section had a viable plan to address known issues with the office's voicemail system; and
- the IT section had procedures in place to determine the priority for addressing computer system issues reported by users.

To gain an understanding of the controls over emergency preparedness and to determine if key employees were aware of the disaster recovery plan and prepared to carry it out, we interviewed key personnel and observed some of the procedures followed by the IT section. We also reviewed the business continuity plan, the disaster recovery plan, a listing of Business Continuity Work Group members, and the Office for Information Resources' disaster recovery website. To determine whether the office had performed appropriate testing of its emergency preparedness procedures, we had discussions with key personnel and reviewed IT's Integrated Multi Processing of Administrative and CAMA Technology system testing procedures.

To evaluate whether access to the Edison and Comptroller computer applications was granted based on employees' job responsibilities, user access levels were updated as necessary as a result of recent organizational changes, and access was set up to prevent a user from having incompatible duties, we obtained a listing of the Edison access roles as of September 20, 2012, and the Comptroller application access roles as of November 1, 2012, granted to 16 key OMS personnel and fiscal staff. We inspected Edison security forms and Comptroller application security requests submitted for those 16 employees from June 30, 2012, to the date the access role listings were provided. We reviewed the OMS organizational charts, which listed employees' job duties, as well as memoranda and e-mails describing organizational changes. We examined manuals and other documentation detailing Edison role definitions and standard roles, and we also discussed employees' access roles with management. To determine whether management followed information systems' industry best practices, we compared management's internal control activities to the industry's best practices.

We scrutinized the office's password security and guidance policy and discussed the office's password procedures with key personnel. To assess whether employees changed their computer passwords every 90 days (30 days for system administrators) as prescribed by policy, we obtained a list of all Comptroller network accounts as of October 31, 2012, including the user's last password change date and last log-in date. We calculated the number of days since the user's last password change as of October 31, 2012, and consulted with key personnel about any discrepancies noted. To determine whether the office had appropriately considered the risk of not changing passwords with the frequency prescribed by policy in its risk assessment, we examined the OMS IT risk assessment.

To determine whether the IT section had a viable plan to address known issues with the office's voicemail system, we conducted interviews with key personnel and inspected IT's deployment schedule for the Microsoft Lync phone system. To evaluate whether the IT section had procedures in place to determine the priority for addressing computer system issues reported by users, we made inquiries of key IT personnel, checked a listing of Comptroller applications, and conferred with representatives from other Comptroller's Office divisions.

Based on the procedures performed, we determined that

- policies and procedures were in place which provide reasonable assurance that the office would experience a minimal loss of data and function in case of an emergency;

- key employees were aware of the disaster recovery plan and were prepared to carry it out in case of an emergency;

- since the office's emergency preparedness plans were still in transition, they had not yet been formally tested, although the office planned to conduct such testing in the future;

- with one exception, access to the Edison and Comptroller computer applications was granted based on employees' job responsibilities;

- user access levels were updated as necessary as a result of recent organizational changes;

- access was set up to prevent a user from having incompatible duties, with a minor exception;

- management did not follow information systems' industry best practices regarding computer access (see finding 2);

- employees changed their computer passwords every 90 days (30 days for system administrators), with immaterial differences;

- the office had appropriately considered the risk of not changing passwords with the frequency prescribed by policy in its risk assessment;

- the IT section had a viable plan to address known issues with the office's voicemail system; and

- the IT section had procedures in place to determine the priority for addressing computer system issues reported by users.

2. The office did not follow information systems' industry best practices regarding computer access, resulting in the increased risk of fraudulent activity or loss of data

Finding

Based on our computer access testwork, the Office of the Comptroller of the Treasury did not follow information systems' industry best practices, resulting in increased risk of fraudulent activity or loss of data. The wording of this finding does not identify specific vulnerabilities that could allow someone to exploit the office's systems. Disclosing those vulnerabilities could present a potential security risk by providing readers with information that might be confidential pursuant to Section 10-7-504(i), *Tennessee Code Annotated*. We provided office management with detailed information regarding the specific vulnerabilities we identified as well as our recommendations for improvement.

Recommendation

The Director of Management Services and the Assistant Director of Information Technology should ensure that these conditions identified to management are remedied through procedures that encompass all aspects of effective access controls. Although the risks associated

with these conditions were identified and assessed in the office's risk assessment, management should continue to assess computer access risks and ensure controls are in place to mitigate those risks.

Management's Comment

We concur and will continue to assess computer access risks and create or modify existing controls to mitigate any identified risks.

APPENDICES

BUSINESS UNIT CODES

Office of the Comptroller of the Treasury divisions and business unit codes:

307.01	Division of Administration
307.02	Office of Management Services
307.04	Division of State Audit
307.05	Division of Local Government Audit
307.06	Division of Investigations
307.07	Office of State and Local Finance
307.08	Office of Local Government
307.09	Division of Property Assessments
307.10	Tax Relief Program
307.11	State Board of Equalization
307.14	Offices of Research and Education Accountability
307.15	Office of State Assessed Properties
307.50	Telecommunications Ad Valorem Tax Equity

BOARDS AND COMMISSIONS

The Comptroller of the Treasury (or a representative of the Office) is by statute a member of the following:

	Tennessee Code Annotated
Access Improvement Project Committee	54-2-207
Advisory Council on State Procurement***	4-56-106
Basic Education Program Review Committee	49-1-302
Board of Claims	9-8-101
Chairs of Excellence Endowment Fund	49-7-501
Council on Children's Mental Health Care***	37-3-111
Council on Pension and Insurance**	3-9-101
Emergency Communications Board	7-86-302
Governor's Council on Physical Fitness and Health	4-40-101
Health Services and Development Agency	68-11-1604
Information Systems Council**	4-3-5501
Judicial Information System Advisory Committee***	16-3-809
Local Education Insurance Committee	8-27-301
Local Government Insurance Committee	8-27-207
Procurement Commission**	4-56-102
Public Records Commission	10-7-302
State and Local Government Advisory Committee to Monitor Internet Use*	12-3-1101
State Board of Equalization**	4-3-5101
State Building Commission**	4-15-101
State Capitol Commission	4-8-301
State Funding Board**	9-9-101
State Government Quality Improvement Task Force*	4-3-5302
State Insurance Committee	8-27-101
State Trust of Tennessee	9-4-806
Tennessee Advisory Commission on Intergovernmental Relations**	4-10-103
Tennessee Baccalaureate Education System Trust	49-7-804
Tennessee Broadband Task Force	7-52-408
Tennessee Consolidated Retirement System Board of Trustees**	8-34-302
Tennessee Governmental Accountability Commission*	9-4-5614
Tennessee Higher Education Commission**	49-7-204
Tennessee Highway Officials Certification Board***	54-7-104
Tennessee Housing Development Agency	13-23-106
Tennessee Interagency Cash Flow Committee***	9-4-610
Tennessee Industrial Development Authority*	13-16-301
Tennessee Industrial Finance Corporation*	4-17-405
Tennessee Law Enforcement Advisory Council*	38-13-103
Tennessee Local Development Authority	4-31-103
Tennessee Rehabilitative Initiative in Correction Board Certification Committee***	41-22-119

Tennessee State School Bond Authority	49-3-1204
Tennessee Student Assistance Corporation	49-4-202
Tuition Guaranty Fund Board	49-7-2018
Utility Management Review Board	7-82-701
Water and Wastewater Financing Board	68-221-1008
Workers Compensation Insurance Fund Board Review Committee*	50-6-623

* Inactive
** Comptroller of the Treasury only, no proxy
*** Comptroller appoints staff representative

Additionally, the Comptroller appoints a director for the nonprofit Local Government Data Processing Corporation pursuant to the terms of its charter.