



The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL. (617) 727-6200

NO. 2005-0085-3S

INDEPENDENT STATE AUDITOR'S INTERIM
REPORT ON CERTAIN ACTIVITIES OF THE
OFFICE OF THE TREASURER AND RECEIVER GENERAL

OFFICIAL AUDIT
REPORT
JANUARY 26, 2006

TABLE OF CONTENTS/EXECUTIVE SUMMARY

INTRODUCTION

1

The Treasurer and Receiver-General, an elected constitutional officer of the Commonwealth, has direct jurisdiction over the Office of the Treasurer and Receiver-General, the State Board of Retirement and the Alcoholic Beverages Control Commission. Chapter 10, Sections 1-69, of the Massachusetts General Laws establishes the powers and functions of the Office of the State Treasurer (OST). In addition, the Treasurer is the chairperson of the State Lottery Commission, the School Building Authority, the Massachusetts Water Pollution Abatement Trust, and the PRIM Board, and is the sole trustee of the Deferred Compensation Plan. Although not within the Treasurer's purview, the Massachusetts Cultural Council is also budgeted under the OST. The OST is responsible for various financial functions, including receiving and managing all funds paid to the Commonwealth, issuing and managing the state's long-term debt, issuing short-term debt and managing the Commonwealth's cash flow, paying retirees, administering the pension system for state employees and retirees, and processing and paying the Commonwealth's bills, in concert with the Office of the State Comptroller (OSC). Chapters 158 and 200A of the General Laws also assign to the OST the responsibility of receiving, safeguarding, and liquidating abandoned property that has been transferred to the OST. In addition, the Treasurer is required by statute to serve on various boards and commissions (on several of which the Treasurer is the ex officio chairman); he maintains ex officio appointment power vis-à-vis several Commonwealth boards and commissions, and is statutorily mandated to issue various annual reports regarding state finances to other state officials and institutions, including the Commissioner of the Department of Revenue, the General Court, and the Office of the Attorney General.

In accordance with Chapter 11, Section 12, of the General Laws, the Office of the State Auditor conducted a review of the OST. The purpose of our review was to evaluate and analyze financial and administrative activities of the OST, including the corrective actions implemented by the OST regarding the results of our prior audit (No. 2003-0085-3S).

AUDIT RESULTS

3

1. PRIOR AUDIT RESULTS RESOLVED

3

Our follow-up review disclosed that the OST has taken corrective action regarding the establishment of adequate internal controls over abandoned property (securities), contract management, long-term debt, and the inventory of furniture and fixtures, and has implemented an effective internal audit function.

a. Abandoned Property

3

Our prior audit recommended that the OST (1) develop an effective and efficient method to account for and track securities by recording the receipt date, (2) complete a competitive bid process for custodial bank securities services, and (3) develop a policy for liquidating securities and competitively procure a contractor to liquidate securities. Our follow-up review disclosed that the OST has (1) implemented procedures for recording securities by the receipt date, (2) conducted a competitive procurement for

custodial bank security services, and (3) implemented a liquidation-of-securities policy and completed a competitive bid process to liquidate securities.

b. Contract Management

4

Our prior report recommended that a comprehensive contract system be developed to include contract monitoring controls, a needs assessment to determine the need and relevancy for each contract, and a review for future competitive bid opportunities. Also, we noted that the OST should ensure that original invoices are prepared and signed by contractors. The OST has implemented improved contract management controls, including competitively bid contracts and original signed invoices. In addition, OST personnel monitor and maintain a contract register and a procurement log.

c. Long-Term Debt

5

Our prior audit recommended that the OST develop timely long-term debt reports to file with the Office of the Comptroller (OSC). Our follow-up review determined that the OST has improved procedures to provide timelier reports to the OSC to eliminate or reduce delays in reporting bond issuance information used for updating OSC records and for preparing year-end financial statements and the Commonwealth's annual financial report.

d. Inventory of Furniture and Fixtures

6

Our prior review determined that the OST did not comply with OSC inventory control requirements, including conducting an annual inventory and maintaining a non-GAAP (assets with original costs of under \$49,999) inventory listing. The OST has improved inventory controls in compliance with requirements, including conducting an inventory of non-GAAP property and equipment during April 2005, tagging all assets with a unique identification tag number, and establishing an inventory database. Department personnel are in the process of researching and inputting historical costs to the inventory database. A separate inventory is maintained of all information technology (IT) assets, including serial and tag numbers, location, and historical costs.

e. Internal Audit Function

6

The prior review of the OST's internal audit function recommended that the OST immediately implement an effective internal audit capacity, including conducting a comprehensive review of its duties and function, developing an audit plan based on a risk assessment, conducting scheduled reviews to test the OST's systems integrity, evaluating the effectiveness of the internal control system, implementing audit recommendations and following-up on management corrective actions. Our follow up review disclosed that the OST has established an effective internal audit function. The OST has implemented an audit review schedule, conducted various department reviews and has followed-up on prior issues to determine whether corrective actions have been taken by management.

2. PRIOR AUDIT RESULTS PARTIALLY RESOLVED

7

During our follow-up review, we determined that the OST has taken corrective action on many of our recommendations; however, additional measures are needed to address issues identified during our prior audit with regard to cash management, tangible

abandoned property; abandoned securities held by custodial funds; and risk assessment, agency internal control plan, and policies and procedures.

a. Cash Management**7**

Our prior review of cash management recommended that the OST take steps to integrate an upgraded Cash Management System (CMS) into the OSC's new Massachusetts Management Accounting and Reporting System (MMARS), ensure timely and accurate reconciliations of all funds and accounts through daily reconciliation comparisons of bank activity with its in-house cash balances, and ensure that adequate supervisory back-up exists to provide continuity over cash management. The OST has not integrated CMS with OSC's new MMARS but has improved controls, including creating a cross-walk between CMS and the new MMARS to identify transactions and codes. In addition, personnel have been cross-trained to cover necessary duties, and reconciliations are completed timely and reviewed by a supervisor. In response to our audit, the OST's management said it agrees that CMS should be upgraded and stated that it is committed to examining options for better integration of the two systems.

b. Tangible Abandoned Property**8**

Our prior review disclosed that internal controls over tangible abandoned property needed improvement. That review noted inadequate segregation of duties, incomplete recordkeeping, inadequate security and access controls, and inadequate inventory. In addition, a significant voicemail and email backlog existed for claims of abandoned property. Our follow-up review disclosed that the OST has implemented improved internal controls over property, including conducting a complete inventory, implementing a tracking system, improving the database recordkeeping, relocating property to a better secured facility, and implementing abandoned property receipt and processing controls. In addition, the reviews of and responses to voicemails and emails are up to date. However, during our March 2005 site visit, we noted that bank safe-deposit abandoned-property bags received as of November 2004 had not been inventoried or recorded into the database system. OST personnel stated that this situation was the result of a lack of storage space. According to management, the OST received expansion approval in March 2005 and will process the inventory once the facility renovations are complete. In response to the audit, the OST's Abandoned Property Division is expanding the tangible property storage area in Chelsea; once the expansion is completed, the OST will expedite the recording of the unprocessed bags' contents.

c. Abandoned Securities Held by Custodial Banks**11**

Our prior review disclosed that corrective action had not been taken to implement internal control procedures, which require a monthly reconciliation of custodian bank statements with OST records of securities held by custodial banks, in order to verify the accuracy of the statements and reduce the risk of unauthorized use or loss. Our follow-up review disclosed that the OST still needs to implement a process for reconciling securities held in the custodial bank with OST records to verify the accuracy of the securities reported as held by the custodian. The OST reconciles monthly receipts of securities to the custodial records; however, this reconciliation does not include all securities received nor does it verify the accuracy of the securities held in the account.

Therefore, the OST has limited assurance of an accurate accounting of securities held in custodial banks. In response to the audit, the OST's Abandoned Property Division has already taken steps to improve the process of reconciling the Division's records with those of the custodial bank, and states that it will perform such reconciliations on a monthly basis. The Division has initiated requests to its service provider to explore additional disbursement reports to assist in the process of reconciling delivered securities, and plans to have a process in place to reconcile securities by March 2006.

d. Risk Assessment, Agency Internal Control Plan, and Policies and Procedures**13**

Our prior review disclosed that the OST needed to improve its risk assessment, internal control plan (ICP), and policies and procedures to comply with OSC requirements. Although some improvements have occurred since our prior review, the OST must still make, and is in the process of completing, revisions to comply with these requirements. These changes have become necessary as a result of the implementation of the new MMARS and department procedure changes.

The prior review noted that the OST needed to improve its risk assessment to include a department-wide risk assessment, a discussion on risks and internal controls for mitigating risk for day-to-day operations, a cross-referencing of the assessment to OST policies and procedures, and a summarization of risks in the ICP. Five areas not included in the risk assessment were the Abandoned Property Department, Administration and Finance Department, Retirement Board, Human Resources, and the Deferred Compensation Program. Our follow-up review noted that the OST has since implemented a risk assessment that covers the applicable departments. The cross-referencing of the assessment to OST policies has not yet been completed. During our audit OST personnel were in the process of updating this risk assessment.

Our prior audit noted that the OST needed to improve its ICP to establish internal reporting procedures for compliance with Chapter 647 loss reporting; to document updates to its ICP; to conduct staff training regarding the existence and use of the ICP; to cross-reference OST's policies and procedures documenting internal controls to that plan; and to cross-reference the Business Continuity Plan to the internal control plan. Our follow-up review disclosed that the OST is in the process of updating and revising the ICP to comply with OSC requirements. This will include the identification of all of the OST's operating cycles and a discussion of the components of internal controls used to mitigate those risks for day-to-day operations. Once the plan is completed, it will be cross-referenced to the policies and procedures.

The prior report recommended that the OST improve the documentation of its written policies and procedures. The OST needed to ensure that standard operating procedures are dated, reviewed and approved; that they indicate the individual responsible for performing the tasks; and that they are cross-referenced to the ICP. Our follow-up review noted that the policies and procedures for the various departments reviewed have been updated since the prior review; however, the dates of policies and procedures range from 2003 to 2005, and because some are not dated, their effective date cannot be determined. The OST informed us that written policies and procedures are being updated for each department in conjunction with the update of the ICP and risk assessment. In response to the audit, the OST stated that it completed the ICP in June 2005 and is updating its policies and procedures and risk assessment, and that the

Internal Auditors will work closely with OST staff to ensure that each department's policies and procedures, risk assessment, and ICP are updated as changes are implemented.

3. INFORMATION TECHNOLOGY

16

During our follow-up review, we determined that the OST has not developed a comprehensive Business Continuity Plan; however, appropriate controls were found to be in place to provide reasonable assurance that IT resources were properly safeguarded.

a. Business Continuity Planning

16

The OST has not developed a sufficiently comprehensive Business Continuity Plan to address disaster recovery and business continuity planning for all OST departments. The objective of business continuity planning is to provide reasonable assurance of the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. At present, such assurances cannot be provided by the OST. Stated control practices regarding on-site and off-site storage of backup copies of magnetic media were found to be appropriate. Although our review revealed that certain control practices regarding the restoration of systems and data had been improved, we found that overall business continuity planning needed strengthening to ensure the availability of automated processing and electronic data should automated systems become unavailable for an extended period. In response to the audit, the OST stated that it agrees that a department-wide business continuity plan should be developed, and that it is discussing the development of that plan and will refer to the recommendations in this report in the development process.

b. Controls at Administration Office, Data Center, and Alcoholic Beverages Control Commission

24

Based on our follow-up review of selected IT-related controls at the OST Administration Office and data center in Boston, we found appropriate controls to be in place to provide reasonable assurance that IT resources were properly safeguarded, accounted for, and protected from loss or damage. Furthermore, our review noted that appropriate control practices were also in place at the Alcoholic Beverages Control Commission's (ABCC's) administrative offices in Boston and provided reasonable assurance that IT resources were properly secured and protected from loss or damage. Our review of access security to automated systems indicated that appropriate controls were in place to provide reasonable assurance that only authorized users were granted access to network resources and application systems used by the OST and residing on the mainframe computer at the Massachusetts Information Technology Center (MITC), in Chelsea. Access logs for security violations and unauthorized access attempts should be reviewed on a regular basis, and the OST should consider the purchase of a security software package to monitor and track unauthorized access attempts. We found that formal policies and procedures regarding physical security, environmental protection controls, and system access security had been improved. In addition, passwords assigned to access mainframe applications should be changed periodically. Also, written documentation related to inventory control over IT-related resources needed to be strengthened to provide sufficient, comprehensive direction and guidance so that staff could address operational and control objectives. In response to the audit, the OST

stated that it would (a) change alarm codes semi-annually, or more frequently when necessary, and maintain a management record of changes to the codes; (b) explore the cost of purchasing a security system to monitor and track unauthorized access attempts; (c) change passwords assigned to mainframe applications periodically; (d) document detailed instructions regarding physical inventory procedures; and (e) review, update, and sign policies and procedures.

APPENDIX I	31
Chapter 647, Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies	31
APPENDIX II	34
Chapter 647 Awareness Letter from the State Auditor and the State Comptroller	34

INTRODUCTION

Background

The Treasurer and Receiver-General, an elected constitutional officer of the Commonwealth, has direct jurisdiction over the Office of the Treasurer and Receiver-General, the State Board of Retirement, and the Alcoholic Beverages Control Commission. Chapter 10, Sections 1-69, of the Massachusetts General Laws establishes the powers and functions of the Office of the State Treasurer (OST). In addition, the Treasurer is the chairperson of the State Lottery Commission, the School Building Authority, the Massachusetts Water Pollution Abatement Trust and the PRIM Board, and is the sole trustee of the Deferred Compensation Plan. Although not within the Treasurer's purview, the Massachusetts Cultural Council is also budgeted under the OST. The OST is responsible for various financial functions, including receiving and managing all funds paid to the Commonwealth, issuing and managing the state's long-term debt, issuing short-term debt and managing the Commonwealth's cash flow, paying retirees, administering the pension system for state employees and retirees, and processing and paying the Commonwealth's bills in concert with the Office of the State Comptroller (OSC). Chapters 158 and 200A of the General Laws also assign to the OST the responsibility of receiving, safeguarding, and liquidating abandoned property that has been transferred to the OST. In addition, the Treasurer is required by statute to serve on various boards and commissions (on several of which the Treasurer is the ex officio chairman); he maintains ex officio appointment power vis-à-vis several Commonwealth boards and commissions, and is statutorily mandated to issue various annual reports regarding state finances to other state officials and institutions, including the Commissioner of the Department of Revenue, the General Court, and the Office of the Attorney General.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the General Laws, the Office of the State Auditor conducted a review of the OST. Our audit was conducted in accordance with applicable generally accepted government auditing standards. The purpose of our review was to evaluate and analyze financial and administrative activities of the OST, including corrective actions implemented by the OST regarding the results of our prior audit (No. 2003-0085-3S).

To accomplish our objectives, we reviewed and evaluated the following:

1. Controls over certain administrative expenditures, including expenses for travel, conferences, employee use of credit cards, consultants and equipment purchases
2. Oversight and monitoring of new contracts awarded for banking services
3. Administration of all bank accounts controlled by the OST
4. Compliance with applicable laws, rules and regulations.

We also performed a follow-up review of selected information technology (IT) control practices in order to determine whether:

- a. Appropriate physical security controls were in place to provide reasonable assurance that access to IT resources was restricted to only authorized users in order to prevent unauthorized use, damage, or loss of IT resources
- b. Appropriate environmental protection controls were in place to provide reasonable assurance that computer equipment was protected from damage or loss
- c. Appropriate controls were in place to provide reasonable assurance that only authorized users were granted access to network resources and mainframe applications and that procedures were in place to deactivate passwords in a timely manner when access is no longer needed or authorized
- d. Appropriate controls were in place to properly account for IT resources
- e. Appropriate business continuity plans were in place to restore mission-critical and essential business operations in a timely manner should automated systems be unavailable for an extended period
- f. Appropriate control procedures were in place regarding on-site storage of backup copies of magnetic media to properly safeguard and account for application software and data files and to generate backup copies for off-site storage.

Based on our review for the areas tested, we have determined that, except as reported in the Audit Results section of this report, the OST has taken corrective action on our prior audit results and has complied with applicable rules, laws, and regulations.

AUDIT RESULTS

1. PRIOR AUDIT RESULTS RESOLVED

Our follow-up review disclosed that the OST has taken corrective action regarding the establishment of adequate internal controls over abandoned property (securities), contract management, long-term debt, and the inventory of furniture and fixtures, and has implemented an effective internal audit function.

a. Abandoned Property

Abandoned Property Deposits Recorded by Date

Our prior audit recommended that the OST develop an effective and efficient method to account for and track securities to comply with statutory requirements for liquidating securities and transferring proceeds to the Commonwealth's General Fund. The two custodian banks did not record the date on which securities were delivered, which is critical to determining the date available for liquidation. One bank recorded the date of receipt only on the monthly statement during which the transaction originated, and the other maintained separate accounts but did not record the delivery date.

Our follow-up review found that as of November 2003, the OST contracts with one custodial bank, which maintains securities in segregated accounts by year of receipt. OST receives a report listing all securities received by the custodian by receipt date to identify those securities eligible for liquidation and the proceeds transferred to the General Fund. We had previously noted that receipt dates were not recorded in accordance with Chapter 200A, Section 9 (b) of the Massachusetts General Laws, Abandoned Property regulations. The dates are currently being recorded in compliance with those regulations. Our review noted that in fiscal years 2003 and 2004, \$53 million and \$41 million, respectively, in securities received prior to fiscal year 2001 were liquidated and the funds transferred to the General Fund.

Custodial Bank Abandoned Property Contracts Competitively Procured

Our prior report recommended that to promote competition, the OST should immediately review and complete the request for response (RFR) contract process to ensure

accountability and compliance with Abandoned Property regulations for custodial property. One custodial bank contract had commenced in July 1996, and the other in June 1999.

Our follow-up review found that the OST conducted a competitive procurement in fiscal year 2003 for custodial bank services and awarded a contract in November 2003 that included RFR requirements for reporting and recording the securities by receipt date for compliance with liquidation regulations. We reviewed the contract procurement file, the RFR, and bid documentation for compliance with competitive procurement procedures and noted no exceptions.

Abandoned Property Liquidated

Our previous review disclosed that the OST had not competitively procured a contractor to liquidate demutualization securities and had no policy for liquidating all types of securities in accordance with Chapter 200A, Section 9 (b), of the General Laws.

Our follow-up review found that the OST has conducted a competitive bid process for the liquidation of securities. We reviewed the transition management contracts for fiscal year 2003 and 2004 liquidations, which were competitively procured by the RFR process, including selection criteria and the selection team's evaluations. Demutualization securities are transferred to the securities custodial bank until liquidated. OST management has implemented a policy of liquidating all securities after the three-year holding period. Our review noted that the OST has conducted liquidations of securities held in excess of three years.

b. Contract Management

Our prior audit disclosed weaknesses in contract management, including noncompetitive, repetitive contract renewals and extensions and payments made to contractors without proper vendor invoices, including a vendor signature certifying services performed. We recommended that a comprehensive contract system be developed, including monitoring contracts for compliance to terms and conditions, establishing a contract register, conducting a needs assessment to determine the need and relevancy for each contract, performing reviews for future competitive bid contracts, and ensuring that original invoices are prepared and signed by the contractor.

Our follow-up review found that the OST implemented improved procurement procedures, including establishing a procurement manager whose responsibilities include maintaining a comprehensive contract register detailing terms, amounts, beginning and end dates, and the contract procurement process. In addition, an RFR log is maintained of procurements' open and close advertisement dates, changes, contract awards, award dates and copies of the advertisements requesting bids. All contracts now require department head approval and are signed by the Assistant Treasurer of Administration and Finance.

During our follow-up review, we reviewed the contracts and payments made to three individuals for lecturer fees for the "Savings Makes Sense" program and noted that all payments had original invoices signed by the speaker and included documentation signed by the bank or department official verifying the date and location of appearance by the speaker. We also selected 11 contracts to review for procurement compliance, including contract files, the RFR, and bid documentation on file. Of the 11 reviewed, eight were procured through either a statewide contract or a competitive bid process, and three were contracted on an emergency basis in compliance with 801 CMR 21.05. The OST is exempt from 801 CMR but elected to comply with the regulations. The 11 contracts reviewed were reasonable and relevant to the OST mission.

c. Long-Term Debt

Several prior audits had recommended that monitoring controls be implemented to eliminate or reduce delays in reporting bond issuance information to the OSC for updating records and preparing year-end financial statements for the Commonwealth's annual financial report. We also expressed concerns that one individual was responsible to manage the entire long-term debt program, including all debt transactions entered and the preparation of documentation, resulting in significant reporting delays. In addition, we recommended that the OST consider a competitive bid process when issuing bonds, if that is determined to be in the best interest of the Commonwealth.

Our follow-up review noted that the OST has improved controls over long-term debt reporting by increasing the responsibilities of an additional department staff person to include providing assistance in the preparation of documentation for timely reporting. We reviewed several bond issuances in the previous year and noted that OST continues to use a

competitive bid process for small bond issuances and a negotiated basis for larger bond issuances, which has involved primarily the refunding of bonds. The Deputy Treasurer of Debt Management stated that it has been in the Commonwealth's best interest to use a negotiated rate basis for these issuances.

d. Inventory of Furniture and Fixtures

Our prior review had found that the OST did not complete an annual inventory of non-GAAP fixed assets (those with original costs of under \$49,999) and did not maintain an inventory listing of individual assets, dates of acquisition and historical costs in compliance with OST Fixed Asset Guide requirements. In addition, each inventory item was not tagged with a unique property control identification number. We had recommended that the OST complete a physical inventory that includes the serial number, model number, purchase price and purchase date, and that it perform a physical inventory annually to prevent loss, theft, or misuse.

During our follow-up review, OST completed an inventory of non-GAAP property and equipment during April 2005, including tagging all assets with a unique identification tag number and establishing an inventory database in compliance with OSC requirements. The inventory database information recorded includes the identification number, location, value, and acquisition date. Department personnel are in the process of researching historical costs and inputting them into the inventory database. A separate inventory is maintained of all Information Technology (IT) assets, including serial and tag numbers, location, and historical costs. We reviewed the IT inventory listing and selected 10 non-GAAP items to review; we noted no issues.

e. Internal Audit Function

Our previous review found that the Internal Auditor (IA) had not developed and implemented an audit plan or schedules to fulfill the internal audit mission for the overall key financial and programmatic operations of the OST. We recommended that the OST immediately implement an effective internal audit capacity, to include conducting a comprehensive review of its duties and functions; develop an audit plan based on a risk assessment; conduct scheduled reviews to test OST's systems integrity, evaluate the

effectiveness of the internal control system, and recommend changes to be implemented; and follow up on management corrective actions.

During our follow-up review, we noted that OST has implemented an effective internal audit function that includes documented audit reviews and reports issued to OST management, including recommendations. In fiscal years 2003 and 2004, the IA conducted an agency risk assessment by OST department; during our follow-up review, that assessment was being updated and was slated for completion by June 30, 2005. The IA instituted risk assessment worksheets and assigned a risk value to departments and operations. An audit schedule was implemented that includes conducting OST operation reviews based on the assessed risk and other factors, including whether previous reviews of operations were conducted. The IA has conducted reviews that included the State Board of Retirement, Cash Management, Human Resources Department, Alcoholic Beverages Control Commission, Abandoned Property Division IT Department (risk assessment), and the Legal Department (risk assessment).

2. PRIOR AUDIT RESULTS PARTIALLY RESOLVED

During our follow-up review, we determined that although the OST has taken corrective action on many of our recommendations, further improvements are needed with regard to cash management, tangible abandoned property, abandoned securities held by custodial funds, risk assessment, agency internal control plan, and policies and procedures.

a. Cash Management

Our prior audit noted that the OST Cash Management System (CMS) was not integrated with MMARS, resulting in numerous adjusting and correcting entries between offices. In addition, the CMS accounting coding, numbering, and transaction codes were different from those for MMARS. We recommended that the OST take steps to integrate an upgraded CMS into the OSC's new Massachusetts Management Accounting and Reporting System (MMARS), ensure the timely and accurate reconciliation of all funds and accounts through daily reconciliation comparisons of bank activity with in-house cash balances, and work with OSC on correcting entries. The OST needed to ensure the independent integrity of its cash and investments while maintaining the control standards for segregation and authorization required by Chapter 647 of the Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies. We had also recommended that the OST ensure that

adequate supervisory back-up exists to provide continuity in cash management in case of turnover or extended absences of employees.

Our follow-up review noted that the CMS has not been upgraded, and department procedures continue to include reconciliations of the CMS cash balances to bank records. Discussions with the Cash Management department's management revealed that numerous monthly adjusting entries are prepared and sent to OSC for reconciling to new MMARS records. The systems continue to have different accounting and transaction codes; however, a crosswalk has been implemented in the new MMARS to track corresponding CMS transactions.

Also, our follow-up review noted that cash procedures include segregation of the banking, investment, and reconciliation processes. Daily reconciliations are processed between bank records and in-house cash records, and any variances are identified. Our review of the daily reconciliations noted supervisory and department head approval. Also, personnel have been cross-trained to ensure the continuity of the cash process and proper supervisory oversight.

Recommendation

We recommend that the OST, in collaboration with the OSC, consider a cost effective electronic solution to the reconciliation process to eliminate the monthly adjusting entries between their respective offices.

Auditee's Response

Management agrees that CMS should be upgraded. However, because system interface issues would exist with any stand-alone upgrade to CMS, the preferred option appears to be integration of cash management functions into the Comptroller's MMARS system. Cash Management staff worked with the Comptroller in early 2004 to prepare an investment brief for the bond bill that would have funded the integration of several elements of CMS into MMARS and examined the feasibility of integrating others as part of New MMARS phase two proposal by OSC. This investment brief was not approved for funding. Management remains committed to examining options for better integrating the two systems.

b. Tangible Abandoned Property

Internal control issues reported in the prior transition audit report included inadequate segregation of duties, incomplete recordkeeping, inadequate security and access controls, and inadequate inventorying that rendered abandoned property vulnerable to loss, misuse or

theft, without the knowledge of management. Furthermore, the OST did not know what it should have or what it did have for tangible abandoned property. Also, a backlog of voicemail existed, with over 8,500 unanswered emails for claims of abandoned property. We recommended that the OST take immediate steps to expeditiously take control of all abandoned property, and to the extent possible, return it to the rightful owners.

Our follow-up audit found that OST management has implemented improved internal controls over tangible property, including conducting an inventory of all held property, relocating and securing valuable items in a better-organized storage room with access limited to specific personnel, recording property individually by owner to the abandoned property database, and implementing a bar code system for tagging and tracking property in storage and the removal of property from storage. Additional internal controls in place include password security access and enhanced room security features, including video monitoring cameras.

The Abandoned Property Division receives abandoned property from bank safe-deposit boxes in bags, each of which contains a property log and its value as assessed by bank personnel. The OST has implemented pre-arranged scheduled delivery requirements, and OST personnel sign for the bank bag receipts and forward a copy to the Deputy Treasurer of Abandoned Property. Once received, the bags are placed in the storage room until they are opened and inventoried, which requires the two people assigned to the facility to process the bags together, with one person opening the bag and comparing the contents to the Bag Log while the other individual records the inventory to the Abandoned Property Database. A bar code is attached and recorded by storage location in the database. After the entry is made into the database, the owners are notified of the property held by the OST and their names are listed in the next OST publication. OST personnel stated that as of the next abandoned property transfer period, ending in June 2005, procedures have been changed to require banks to fax or email the bag log report to the Deputy Treasurer of Abandoned Property's office separately.

However, during our site review in March 2005, we noted that bank abandoned-property bags received by the OST in November 2004 were placed on top of file cabinets in the storage room and were not inventoried or entered into the Abandoned Property database.

The OST should process property bags when received to ensure that items of value are inventoried and properly secured. OST personnel stated that the bags were not processed because of the lack of storage space in the vault or file cabinets. The OST's management stated that the department has been seeking to expand storage space, that it received expansion approval at the end of March 2005, and the inventory will be processed once the expansion is complete. Our review noted that procedures were in compliance except for the bank property bags received during fiscal year 2005 but not processed.

Also, the OST has not conducted an auction of items or destroyed miscellaneous paper records since the prior review. Department personnel stated that a priority was placed on securing the assets and improving controls, including conducting a detailed inventory, recording the items to the abandoned property database, and moving abandoned property to a more secure facility. The abandoned property department is in the process of receiving appraisals for all items valued over \$500. This process will include two independent appraisals. In addition, House Bill 311 has been filed to amend the process by which banks, credit unions, and the OST administer the contents of unclaimed safe deposit boxes. This bill also includes a policy for the definition of items of no value and the disposal of such property.

Our review of the voicemail and email system noted that the OST implemented procedures to prevent backlogs, including a response tracking system that provides management daily reports, including the number of contacts received and average response time. Also, during busy claims periods, personnel and claim phone hours have been increased for better customer response. Our review noted that responses were current and the backlog had been cleared.

Recommendation

OST management should continue to fulfill its custodial fiduciary responsibility by inventorying (identifying the contents of property bags) and returning the property to its rightful owners as soon as possible. In addition, the OST should continue its plans to expand the storage facility in order to avoid delays in the process.

Auditee's Response

The Abandoned Property Division is in the process of expanding the tangible property storage area in Chelsea. Upon completion of the expansion, tangible property personnel will expedite the process of recording the contents of the unprocessed bags.

c. Abandoned Securities Held by Custodial Banks

Our prior audit disclosed that the Abandoned Property Division contracted with two banks to act as portfolio custodian for cash dividends, stocks, bonds, and other intangible property. We recommended that the OST implement internal control procedures to verify the accuracy of the monthly statements and to protect the securities from loss, theft, or misuse.

Our follow-up review disclosed that the OST still needs to implement a procedure for reconciling the securities held by the custodial bank with OST records to ensure that securities are adequately safeguarded. A partial monthly reconciliation is completed of security receipts and disbursements; however, a process is not in place to verify that the account holdings are in agreement with OST records of securities in OST custody. As of January 31, 2005, the market value of abandoned securities held was \$206,290,674.

As of November 2003, the OST contracted with a custodial bank, which has received the securities held by the two previous custodian banks and the subsequent securities received as abandoned property. Securities are received through a Depository Trust Company (DTC) via a wire transfer, or the physical securities are mailed to the custodial bank. OST personnel stated that a reconciliation was completed at the time securities were transferred to the holding company from the prior two companies, and monthly receipts and disbursements/deliveries have been reconciled on a go-forward basis. The OST's current reconciliation process is to reconcile security receipts by comparing the OST's monthly Holders Reporting Securities Report with the custodial monthly statement or the custodial report of security receipts by entry date for the year. However, our review noted that the

receipts were only partially reconciled. Our review noted that securities received from the major brokerage houses were reported in summary total on the OST report, preventing reconciliation with the custodian report that lists transactions individually. As a result of our inquiry, the individual responsible for completing the reconciliations had received, as of March 2005, the breakdowns of the summary, but had not yet completed the reconciliation. However, even though the reconciliation of receipts is accomplished on an ongoing basis, a process still needs to be implemented to ensure that the actual securities reported in the custodial account are in agreement with the OST's records. Until this process is implemented, OST has limited assurance that custodial records are accurate, resulting in a potential significant risk.

Chapter 647 of the Acts of 1989 requires agencies to establish internal control systems in accordance with internal control guidelines established by the OSC. Periodic comparisons are to be made between resources and resource records to reduce the risk of unauthorized use or loss and to protect against waste and wrongful acts. OST personnel stated that a monthly reconciliation of disbursements involves a cumbersome process due to volume and timing differences in the monthly reports of claim dates of up to three months for individual transactions, because OST records the disbursement as of the claim approval date, and the custodian report sometimes takes up to three months to report the security as disbursed/delivered. The lack of a periodic reconciliation could result in undetected errors or discrepancies. Treasury personnel have initiated discussions to conduct an electronic reconciliation of the database systems' information to identify, isolate, and investigate any differences.

Recommendation

The OST should improve internal control procedures to require an ongoing periodic reconciliation between Abandoned Property Division records and the custodial records, including all securities held, to verify the accuracy of the custodial records and ensure that securities are properly safeguarded. In addition, the OST should continue conducting a monthly reconciliation of all security receipts with custodial records to ensure that securities are properly received and recorded. The OST should continue to pursue an electronic reconciliation of the two database systems.

Auditee's Response

The Abandoned Property Division has already taken steps to improve the process of reconciling the Division's records to those of the custodian. All securities received to date in 2005 per the Division's records have been reconciled to the custodian's records. Going forward, the Division will perform this reconciliation on a monthly basis. The Division has initiated requests to its service provider to explore adding additional disbursement reports to aid in the process of reconciling delivered securities. The Division plans to have a process in place to reconcile delivered securities by March 2006.

d. Risk Assessment, Agency Internal Control Plan, and Policies and Procedures

The prior audit report noted that the OST needed to improve its risk assessment, internal control plan, and agency policies and procedures in order to be in compliance with OSC requirements. Although some improvements have been made since the prior review, the OST needs to make, and is in the process of completing revisions to comply with these requirements. These changes have become necessary as a result of the implementation of the new MMARS and department procedure changes.

Risk Assessment

Our prior review noted that the OST needed to expand its risk assessment to include a department-wide risk assessment, a discussion on risks and internal controls mitigating risk for day-to-day operations, a cross-referencing of the assessment to OST policies and procedures, and a summarization of risks in its Internal Control Plan (ICP). Five areas not included in the risk assessment were the Abandoned Property Department, Administration and Finance Department, Retirement Board, Human Resources, and the Deferred Compensation Program. The OSC Internal Control Guide defines a department-wide risk assessment as the identification and analysis of the risks that could prevent the department from attaining its goals and objectives.

Our follow-up review found that the OST has implemented a risk assessment that covers the applicable departments. The risk assessment identifies risk level for each department's day-to-day functions. In addition, a risk assessment worksheet is maintained that lists each department's functions, assessed by their value and financial impact on the OST as a whole, the complexity with which each operates, and the weight of any known risk factors that have the potential to impede certain departmental functions. However, the risk assessment is not dated, and it is not cross-referenced to OST policies and procedures.

The OST's IA stated that the risk assessment was revised in fiscal year 2004, and is currently being updated and linked to the internal audit function. A re-evaluation of each department's risks is in process in conjunction with the updating of the agency's ICP and policies and procedures.

Internal Control Plan

Our prior review noted that the OST needed to improve its internal control plan to (1) establish internal reporting procedures for compliance with Chapter 647 for unaccounted-for variances, losses, shortages, or thefts of funds or property; (2) to document updates to its ICP; (3) to conduct staff training regarding the existence and use of the ICP; (4) to cross-reference OST's policies and procedures documenting internal controls to the ICP; and (5) to cross-reference the Business Continuity Plan to the ICP. Chapter 647 requires that the OST have written documentation of its accounting and administrative controls in accordance with the guidelines issued by the OSC.

Our follow-up review disclosed that the OST is in the process of updating and revising the ICP to comply with OSC requirements. This will include the identification of all of the OST's operating cycles and a discussion of the components of internal control used to mitigate those risks for day-to-day operations. The plan is being streamlined to exclude department policies and procedures and become a department-wide summary of risks and controls. Once the plan is completed, it will be cross-referenced to the policies and procedures. Meetings have been held with all OST department heads to discuss the updating of the plan and the OST's policies and procedures. The ICP and policies and procedures documentation is in process, and we were provided with the department head meeting log for review. Subsequent to our review, the ICP was complete in June 2005.

The OSC's Internal Control Guide for Departments, II, defines an ICP as follows:

A high level summarization, on a department-wide basis, of the department's risks (as the result of a risk assessment) and of the controls used by the department to mitigate those risks. This high level summary must be supported by lower level detail, i.e. departmental policies and procedures. We would expect this summary to be from ten to fifty pages depending on the size and complexity of the department.

Responsibility for the department internal control plan resides with the department's Internal Control Officer (ICO). Chapter 647 describes the role of the ICO, in part, as follows:

an official, equivalent in title or rank to an assistant or deputy to the department head, whose responsibility...shall be to ensure that the agency has written documentation of its internal accounting and administrative control system on file. Said official shall, annually, or more often as conditions warrant, evaluate the effectiveness of the agency's internal control system and establish and implement changes necessary to ensure the continued integrity of the system.

Internal controls are also the responsibility of every manager and supervisor and any other staff member whose duties include being responsible for the activities, at least in part, of others.

Policies and Procedures

Our prior audit recommended that the OST improve the documentation of its written policies and procedures. The review noted that the Abandoned Property Department needed to document policies and procedures for the receipt and handling of safe-deposit box contents. In addition, the Cash Management Department had no formal written policies and procedures within its CMS functions over certain control activity, the procedures lacked the dates they were placed into operation, they did not indicate the individuals responsible for carrying out the outlined responsibilities, and they did not point to the necessary documentation of approval by an OST person authorized to review and approve operating procedures. Also, procedures were not incorporated into the ICP. We recommended that the OST ensure that standard operating procedures are dated, reviewed, and approved; that they indicate the individual responsible for performing the tasks; and that they are cross-referenced to the ICP.

Our follow-up review noted that policies and procedures for the various departments reviewed have been updated since the prior review. However, the dates of the policies and procedures range from fiscal year 2003 to 2005; and because some are not dated, their effective date cannot be determined. Both the Abandoned Property Department and the Cash Management Department have implemented written procedures with the individuals responsible to perform the task identified, although some of those are not dated. OST personnel stated that a department-wide update of departmental policies and procedures is

in progress, with a completion deadline of June 30, 2005, along with the ICP. Our review noted that meetings had been held with all department heads to discuss the revisions and updates; we discussed the status with the IA, who stated that several departments' policies and procedures have been completed and others are in the process of being completed. In addition, we were informed that the various policies and procedures will be maintained on file along with the ICP and will be cross-referenced to it.

Recommendation

OST should continue the ongoing process of implementing the agency's policies and procedures, risk assessment, and ICP to comply with Chapter 647 and OSC requirements. In addition, this process should be linked to the recommendations contained within the Information Technology section of this report in order to insure a fully integrated Risk Assessment and Internal Control Plan. OST should also ensure that the ICP, risk assessment, and policies and procedures are revised, dated, cross-referenced as needed, and reviewed annually.

Auditee's Response

As mentioned, the process of updating the OST's policies and procedures, risk assessment, and ICP was completed in June 2005. Going forward, the Internal Auditor will work closely with OST staff to ensure that each Department's policies and procedures, risk assessment and ICP are updated as changes are implemented.

3. INFORMATION TECHNOLOGY

a. Business Continuity Planning

Our follow-up review found that, although the OST had strengthened certain IT control practices to support recovery of mission-critical and essential business functions and updated the Department of Cash Management's Business Continuity and Contingency Plan, it had not yet developed a sufficiently comprehensive, tested business continuity plan to address disaster recovery and business continuity planning for all OST departments. We acknowledge that OST was aware of the need for business continuity planning and had, since our prior review, continued to document and improve certain IT-related tasks and activities that are an integral part of business continuity planning to provide reasonable assurance of regaining operations in an acceptable period of time.

We found that since fiscal year 2003 the OST's Internal Audit Division had performed a risk assessment of selected information technology controls. The "Internal Auditor's Risk Assessment Report," as of December 2003, evaluated selected IT control practices, such as physical security over the data center in Boston, scheduled password changes, monitoring of computer violations, and business continuity planning. The report included recommendations for corrective action to improve certain control procedures, such as monitoring of unauthorized access and business continuity planning. The risk assessment did not address OST's mission-critical operations, such as cash management, or provide additional review and follow-up of the "Department-wide Risk Assessment" for cash management, debt management, and computer services performed for fiscal year 2002. This risk assessment documented specific financial and IT-related risks as well as the activities intended to mitigate the risks to reduce any loss of resources and the ability to perform normal business operations. In addition, Computer Services had documented "Disaster Recovery Status," as of March 2005, that was limited to recovery of IT functions for the OST. The status report documented control practices for on-site and off-site storage of backup media in Boston and the Massachusetts Information Technology Center (MITC) in Chelsea, as well as certain recovery procedures, such as redundant file servers, purchase of an additional mainframe computer, upgrades to hardware and software, and limited descriptions of contact lists and the alternate processing site at MITC. In addition, our review noted that the OST had strengthened certain IT control practices. An additional check printer was installed in Boston as backup for the printer located at MITC; a StorageTek file server that backed up and stored 40 tapes was installed in the computer room in Boston; and backup tapes were no longer stored in the unlocked cabinet in the computer room. Although the Computer Services' status report documented important recovery activities and additional control practices had been improved, the OST lacks an overall enterprise-based business continuity plan. Moreover, we found at the date of our follow-up review that a senior official had not been assigned the responsibility of managing the overall business continuity planning process across the OST and providing a single point of accountability for business continuity planning.

Based on our follow-up review of documents provided to us by the OST and limited interviews with OST management, we determined that the OST continued to rely on a

business continuity plan, included in the OST's ICP, that had been developed in response to Y2K issues. The business continuity plan included important information, such as OST's responsibilities regarding the receipt and disbursement of approximately \$28 billion per year, cash management business practices, and continuity plans; a description of the six systems designated as mission-critical; an assessment of potential risk areas and mitigation of selected risks; and a hierarchy of contingency planning for selected types of disruptions. The business continuity plan had not been updated since May 2000. Accordingly, the OST may not be able to rely on the plan's viability today, due to factors such as changes in the risks and threats to the IT environment, IT infrastructure vulnerabilities, IT application systems, network and communication changes, security requirements, electronic interfaces, personnel, logistics, and organizational changes. In addition, because it has not adequately tested a comprehensive business continuity plan, the OST has no reasonable assurance that the recovery plan would effectively address various disaster scenarios.

Another business continuity plan, developed by the Department of Cash Management, had been updated as of June 2005. It included a detailed description of the Department of Cash Management's business functions, a risk assessment of important operations, such as cash disbursements and wire transfers, and various disaster scenarios and contingency plans to address specific loss of functions. Furthermore, as of December 2003, OST had required the Commonwealth's main depository, Sovereign Bank, to document specific steps to recover operations should OST and/or Sovereign systems fail. Sovereign Bank has provided its "Business Resumption Plan," as of January 2005, to OST. In addition, Sovereign Bank provides monthly updates regarding changes to business continuity planning, including description of proposed modifications, status of testing, and timeframes for implementation of the changes. According to OST management, OST reviews the monthly updates, recommends any changes, and approves changes to be made to Sovereign Bank's system that would impact OST. Our follow-up review found that the OST had not documented similar continuity plans for other mission-critical systems, nor had it incorporated the specific needs of these systems into a cohesive, comprehensive business continuity plan.

The objective of business continuity planning is to provide reasonable assurance of the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Furthermore, the purpose of business continuity planning is to ensure

that mission critical and important processing can be regained in a timely manner. Business continuity planning for information services is part of business continuity planning for the entire organization. Business continuity plans need to be developed to effectively address short-, medium-, and long-term recovery requirements. In the short term, mission-critical systems and services should be restored. Medium-term plans address recovery of systems and services on a temporary basis, including leased equipment; long-term plans involve the total recovery of the IT processing environment.

The business continuity plan should also incorporate user-area plans describing the procedures for user departments, such as cash management and their staffs, to follow when changing to alternate-processing activities should a disaster render the automated systems inoperable. Furthermore, the recovery plan should identify contingency procedures that could be used during an interim recovery period. The recovery plan should address procedures for the restoration of critical IT functions and should indicate the logical order of system implementation and integration. The plan should be distributed to appropriate staff, such as OST officials, senior management, IT administrators and staff, and Internal Audit. In addition, the plan should address tasks and responsibilities to move and safeguard backup data files and software, and program and system documentation, from the off-site storage location. A copy of the plan should be stored in a secure off-site location and should be available in electronic and hardcopy form. The OST should consider whether additional copies of the business continuity plan should be stored in other secure locations.

Generally accepted practices and industry standards for IT operations support the need for each entity to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. To that end, the entity should assess the extent to which it is dependent on the continued availability of information systems for all required processing and operational needs and develop its recovery plans based on the critical components of its information systems and other factors, such as risk assessment of mission-critical and essential systems, analysis of various disaster scenarios, and security over the IT infrastructure.

The success of the business continuity planning process requires senior management commitment. Senior management and system users should be closely involved in business

continuity planning to help ensure that there is a clear understanding of the entity's information systems environment, and that determinations of system criticality and the risks and exposures associated with the systems are correct. In addition, appropriate information technology and user area plans should be developed based on the relative criticality and importance of systems, and adequate resources should be made available. Resources should include appropriate hardware and communication equipment; supplies; space in which to resume operations; backup copies of all required application programs, data files, and system utilities; documented policies and procedures; and sufficient personnel. A risk analysis should identify the relevant threats that could damage the systems and supporting IT platforms and environments, the likelihood of the threat and frequency of occurrence, and the cost of recovering the systems.

The business continuity plan for IT should include sufficient information to recover mission-critical and essential operations in a timely manner. The IT plan should contain, but should not be limited to, the following information:

- Description of the OST's automated systems operating environment, including the identification of IT platforms, networks, interfaces, information systems, and other IT-related resources
- Description of the communication components, local area network (LAN) and wide-area network (WAN), electronic interfaces, and Virtual Private Networks (VPN)
- Identification and description of administrative, processing, resource, operational, and user requirements
- Identification of and operational specifications for mission-critical, essential, and less-essential application systems and processing requirements and a statement of recovery objectives and strategies for each system
- Classification of types of delays and disruptions in information technology/systems services
- Description of recovery strategies and designated timeframes for mission-critical and essential systems under various disaster scenarios
- Identification of essential data files and software for each critical application according to impact (i.e., catastrophic, severe, serious, or limited)

- Documentation of responsibilities and activities of functional areas supported by critical and essential information technology operations
- Names, addresses, and phone numbers of key emergency recovery personnel; composition of recovery teams and user management; detailed description of their responsibilities; and identification of any known limitations on the availability or travel restrictions of key staff under various time scenarios with regard to alternate processing
- Contact information regarding important vendors and essential personnel from state agencies critical to the OST's operations, such as the Information Technology Division and the OSC, and other entities providing critical services, such as Sovereign Bank
- Procedures for notifying management, users, and other parties who oversee or are dependent on the computer operations should processing capabilities be disrupted or lost
- Documented user-area contingency plans for departments supported by critical and important systems, with completion and/or latest revision dates and provisions to ensure that the user-area plans are kept current
- Emergency supplies inventory, including the quantity and location of each item
- Contact information for vendors, including copies of agreements for service and hardware replacement (access to the agreements could become critical during an emergency)
- Procedures for the purchase and/or lease of hardware and other specialized equipment
- Emergency drill procedures and test criteria

We determined that appropriate control practices regarding on-site and off-site storage of backup media were in place to provide reasonable assurance that backup tapes could be accessed within a reasonable period. We found that physical security and environmental protection controls over on-site storage in Boston were appropriate. We did not visit the off-site storage location.

Recommendation

The OST should designate a senior official to be responsible for the business continuity plan process and to manage the development of a department-wide business continuity plan. It should also assign duties and responsibilities and establish points of accountability for

recovery team(s), steering committee, and business process areas. Appropriate teams, such as a business continuity team, should be established with membership from key departments of the OST, including Computer Services, and chaired by senior management.

The OST should establish a business continuity planning framework outlining business continuity, recovery, and contingency objectives for mission-critical and essential business operations. The framework should include a criticality assessment and risk analysis, policies, procedures, defined responsibilities, and documented management control practices; organizational controls, such as steering committee, recovery teams, and oversight functions; and assurance mechanisms. Assurance mechanisms would include internal reviews, testing, internal audit examinations, and independent examination and verification. The framework should also include senior management assignment of enterprise responsibility for business continuity planning.

The OST should perform an enterprise-based risk analysis and criticality assessment to ensure that all functional areas and business processes are evaluated, and update, if necessary, the risk analysis results for Computer Services. The risk analysis and criticality assessment should include all external partners and outsourced services.

The OST should review the list of disaster scenarios it has already documented to determine whether all potential scenarios have been identified, and thereafter update the list accordingly with respect to likelihood and impact. It should develop and update recovery and business continuity strategies for each of the disaster scenarios identified.

The OST should reconfirm its understanding of the relative importance of business functions and the potential impact of a loss of IT processing support. The OST should formally rank mission-critical, essential, and less-essential business process functions and IT processes for development and update of disaster recovery, business continuity, and contingency plans.

The OST should obtain an adequate level of assurance of the viability of the disaster recovery and business continuity plans for required services and support from all mission-critical and essential business partners and third-party providers.

The OST should update existing recovery and business continuity plans to ensure adequate coverage of OST as a whole. A single organizational framework should be established to which business process area plans and Computer Services plans can be linked to an overall business continuity plan. While a single document is not necessarily required, standard formats, syntax rules, linkages, and cross-references should be provided. A multipart business continuity plan should identify all subcomponents. In conjunction with the development of the business continuity plan, OST should establish targets for acceptable time periods by which mission-critical and essential IT operations need to be recovered.

The OST should develop and perform appropriate levels of testing to obtain sufficient assurance regarding the viability of recovery and business continuity plans. Test scripts should be developed by business process areas and Computer Services and be reviewed and approved by senior management and the business continuity steering committee. Once tests are completed, test results should be reviewed against expected test plan results, and reviewed and approved by business process operations and IT.

Given the critical interrelationships of OST to the OSC and ITD and certain external partners, such as Sovereign Bank, business continuity planning should be performed on a collaborative basis with these critical IT processing partners.

The OST should ensure that all key business process and Computer Services management and staff have adequate skill and knowledge to carry out all tasks and activities outlined in recovery and business continuity plans.

The OST should develop a framework for the business continuity plan, including policies and procedures and assurance mechanisms. Duties and responsibilities for development of the plan should be assigned to business process and IT managers. The IT components of the plan should be coordinated with the business continuity planning for the Department's operational functions.

We further recommend that the OST review and evaluate already-developed business continuity planning-related documents. Based on that review, the Department should ensure that the business continuity plan includes the designation of alternate processing sites, required user area plans, communication components, and instructions regarding

replacement of file servers and other IT resource components. The plan should also include a listing of contact information of key personnel and documented scenarios regarding minor to major loss of systems and appropriate responses to each situation. Business continuity requirements should be assessed on an annual basis or upon major changes to the IT environment or user requirements regarding the automated systems.

With respect to the development of the business continuity and contingency plan, the OST should document specific deliverables, with dates for completion, for portions of the plan. Should third-party contractors be used to assist OST, all work should be reviewed and approved by OST management before payments are made.

In summary, the business continuity plan should document the OST's recovery strategies with respect to various disaster scenarios for all operational functions within the OST. The recovery plan should contain all pertinent information needed to effectively and efficiently recover mission critical operations within the needed time frames. At a minimum, the OST should develop documented user area plans for functional units to continue their operations at an acceptable level should the file servers or mainframe become unavailable. Moreover, the business continuity plan should be tested to ensure its viability and then periodically reviewed and updated when needed, to provide reasonable assurance that it is current, accurate, and complete. The OST staff should be trained in the execution of the plan under emergency conditions. The completed plan should be distributed to all appropriate staff members, including OST officials, senior management, IT administrators and staff, and Internal Audit.

Auditee's Response

The OST agrees that a department-wide business continuity plan should be developed. The OST is discussing the development of this plan and will utilize the recommendations provided by the OSA in the development process.

b. Controls at Administration Office, Data Center, and Alcoholic Beverages Control Commission

Our follow-up review of selected IT-related controls at the OST administration office and data center in Boston found appropriate controls in place, to provide reasonable assurance that IT resources were properly safeguarded, accounted for, and protected from loss or damage. Our review also noted that appropriate control practices were in place at the

Alcoholic Beverages Control Commission's (ABCC's) administrative offices in Boston, to provide reasonable assurance that IT resources were properly secured and protected from loss or damage. ABCC has operated within the purview of the OST since fiscal year 2003. Our review of system access security to automated systems found that appropriate controls were in place to provide reasonable assurance that only authorized users were granted access to network resources and mission-critical application systems, including Cash Management, State Retirement, and Payment Processing, that reside on the mainframe computer at the Massachusetts Information Technology Center in Chelsea. In addition, we found that the OST had taken corrective action regarding documented control practices for card key management and the documentation of controls for physical security. We found that stated control practices regarding on-site and off-site storage of backup copies of magnetic media were appropriate. We found that formal policies and procedures regarding physical security, environmental protection controls, and system access security had been improved. However, written documentation related to inventory control procedures over IT-related resources needed to be strengthened in order to provide sufficient, comprehensive direction and guidance so that staff can address operational and control objectives.

Physical Security

Based on our review of selected physical security control practices, we determined that appropriate controls were in place to provide reasonable assurance that only authorized persons could access the OST's Administration Office and data center in Boston, including the computer room. We found that controls over the check printer and check stock located in the Administration Office were appropriate and in place. Our review also revealed that appropriate physical security control practices were in place at ABCC's administrative offices. Furthermore, we found that certain control practices, including policies and procedures, had been strengthened.

Selected compliance tests found appropriate controls, such as designated managers responsible for physical security at the Administration Office and data center; doors to the Administration Office, Abandoned Property area, and State Board of Retirement were locked and alarm systems activated after normal business hours; a punch keypad system and alarm system were installed at the main entrance to the Administration Office; and visitor

registration was in place. Only the senior managers were authorized to change the alarm codes at the Administration Office and data center. We found that the data center was located in a non-public area, the entrance door was locked 24/7, a punch keypad and an alarm system were installed, and only authorized staff were allowed access to the data center. We found that a card-key access system was in place. According to IT management, formal periodic reviews of card-key users to the access list had been implemented.

Our review disclosed that certain control practices had been improved. We found that the OST had documented "Treasury Security Procedures" that included control practices regarding intrusion detection (alarm codes) policy and procedures and the card-key system used to access inner business offices at the Administration Office and the data center in Boston. Furthermore, the OST had instituted a form, "Departing Employee Information," that documented information, such as the return of Commonwealth ID badges, card-keys, and physical keys. We found that the codes for the punch keypad system and alarm codes at the Administration Office had been changed since the prior review (February 2003); however, certain alarm codes had not been changed, and no consistent control practices were in place regarding scheduled changes to punch keypad system codes and/or alarm codes in the Administration Office and data center in Boston.

Our review found that the ABCC had implemented appropriate controls regarding physical security over automated systems installed at its administrative offices and computer room. The Executive Director was responsible for key management. The computer room, in which the file server was installed, was found to be locked at all times. Only the Executive Director and OST IT staff were authorized to access the computer room. The Executive Director controls the only key to the room. According to the Executive Director, ABCC complies with all documented control procedures issued by OST.

Recommendation

The OST should implement a schedule regarding frequency of changes to the punch keypad system code and/or alarms codes installed at the Administration Office, data center, and ABCC offices in Boston. Keypad and/or alarm codes should be changed when staff who have knowledge of the code leave employment and are no longer authorized to access

restricted areas. A management record of periodic changes to the codes should be maintained.

Auditee's Response

The OST agrees with this recommendation. The OST will change alarm codes semi-annually or sooner if an employee with the code is no longer authorized to access restricted areas. A management record of changes to the codes will be maintained.

Environmental Protection Controls

Our review revealed that appropriate environmental protection, such as temperature controls, smoke detectors, fire alarms, sprinkler systems, and fire extinguishers were in place at the Administration Office and data center in Boston. Selected staff had been assigned to manage evacuation procedures in the event of an emergency, and new exit signs had been posted at the Administration Office. In addition, surge protection to prevent power spikes, an uninterruptible power supply (UPS) to prevent loss of data should power suddenly fail, and emergency generators were in place to support the Administration Office and data center. Regarding the computer room, we determined that appropriate controls, such as a raised floor, air-conditioning, hand-held fire extinguishers, and good housekeeping procedures, were in place. Our review found that the OST had posted the Bureau of State Office Buildings' "Emergency Evacuation Plan" in the data center. To prevent damage to equipment installed in the computer room, water pipes were modified to fill with water only when fire was detected.

Our review found that OST had taken corrective action regarding on-site storage of backup media in an unlocked file cabinet located in the computer room. At the time of our review, backup copies of magnetic media for current processing and/or archival tapes were stored in a separate room in the data center. The file cabinet was used to store blank tapes.

Our review disclosed that appropriate environmental protection controls, including smoke detectors, fire alarms, and sprinkler systems, were in place at ABCC administrative offices and the computer room.

System Access Security

With respect to system access security, our review disclosed that the processes for granting and recording authorization to access the automated systems and activation and deactivation of logon IDs and passwords were appropriate. Our limited compliance tests indicated that formal authorization procedures for granting access privileges to users were appropriate and in place. Access privileges to the OST application systems on the mainframe were assigned to users based on predetermined levels of access related to position, job title, and associated responsibilities. Furthermore, logon IDs and passwords were used to access the network and the OST's application systems. We found that, although passwords for network access were required to be changed every 60 days, passwords for access to mainframe applications were not required to be changed periodically. We acknowledge that systems in place at the OST cannot electronically require that the passwords to mainframe applications be changed; however, sound management practices regarding logon ID and password administration hold that passwords should be changed periodically. Users were required by OST to comply with the "Executive Office for Administration and Finance (EOAF) policy on the Use of Information Technology Resources," such as password protection, data confidentiality, and use of the Internet and email. The OST had strengthened controls by requiring users to sign an "Employee Agreement" regarding compliance with OST policies, including password protection, data confidentiality, and use of IT resources. Additional controls had been implemented, including restrictions on remote access through the use of VPN and the implementation of a firewall to prevent unauthorized access to the OST's network in Boston.

Users are locked out after three unsuccessful attempts to access the systems. Our review found that the OST had not implemented formal reviews of access logs for security violations or unauthorized access attempts. As a result, the OST cannot be assured that unauthorized users have not accessed data residing on the network or the level of unauthorized attempts to access the systems.

Recommendation

Access logs for security violations and unauthorized access attempts should be reviewed on a regular basis, and the OST should consider the purchase of a security software package to

monitor and track unauthorized access attempts. In addition, passwords assigned to access mainframe applications should be changed periodically.

Auditee's Response

The OST agrees with this recommendation. The OST will explore the cost of purchasing a security software package to monitor and track unauthorized access attempts. Additionally, passwords assigned to access mainframe applications will be changed periodically.

Inventory Control Over IT-Related Resources

We found that control practices regarding inventory control over computer equipment and software were appropriate. Our review disclosed that a manager was assigned overall responsibility for computer equipment and software. We found that the OST had improved internal control by assigning duties regarding the maintaining, updating, and reconciling of the inventory record to different employees. An inventory record was being maintained for computer equipment and software. According to OST management, in addition to “data fields”, such as state identification number, serial number, and location, information regarding “purchase date” and “cost” for pieces of equipment purchased after 1999 were included on the inventory record as of March 15, 2005. Information regarding “purchase date” and “cost” for equipment purchased by ABCC was not listed on the OST’s inventory record. One test of a statistical sample of 56 (6.17%) of 907 pieces of equipment listed on the inventory record as of March 15, 2005 indicated that with few exceptions, the record accurately reflected actual equipment installed at the OST Administration Office, data center, State House, and ABCC offices. Furthermore, a limited test of purchase documentation for the 2004 fiscal year and the 2005 fiscal year as of March 15, 2005, indicated that of 40 pieces of equipment selected, 27 microcomputer workstations, four printers, two Unisys file servers, and seven laptops, valued at \$174,668, were listed on the inventory record. According to IT management, a physical inventory and reconciliation was performed as of June 30, 2004, and the OST complied with Operational Services Division regulations regarding surplus property. The appropriate control procedures were in place, including a sign-out/in log to account for laptop computers.

Regarding software inventory, licenses were kept on file. According to IT management, a software inventory record was maintained and an annual inventory review and reconciliation

was performed. Cost information was not listed on the software inventory record. Only authorized software was allowed on the system. IT management stated that a software program had been installed that continually reviewed all hardware and software installed on the network.

Recommendation

To strengthen controls, we recommend that the OST initially document detailed instructions regarding the performance of the annual physical inventory and reconciliation. In conjunction with the annual physical inventory and reconciliation, the OST should document all additions and deletions from the inventory record during the prior fiscal period.

Auditee's Response

The OST agrees with this recommendation and will document detailed instructions regarding physical inventory procedures. The Administration and Finance Department already maintains a list of items that are deleted from the inventory record in a given period; however, the IT Department will begin to maintain this list as well.

Documentation of Policies and Procedures

Our review found that the OST had improved its documented operating procedures regarding physical security and system access security. As noted earlier, IT management stated that the OST complied with Bureau of State Office Buildings' "Emergency Evacuation Plans" and the evacuation plans were posted in the data center.

Recommendation

The OST official or manager who authorizes policies and procedures should sign all written documentation and the effective date should be recorded. Policies and procedures should be periodically reviewed and updated when needed; also, the OST staff should be trained in their use.

Auditee's Response

In conjunction with the updating of the Internal Control Plan, policies and procedures will be reviewed, updated and signed and dated by the appropriate department head. The Internal Auditor has conveyed the importance of this exercise to OST staff.

APPENDIX I

Chapter 647, Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies

H 5

Chapter 647

THE COMMONWEALTH OF MASSACHUSETTS

In the Year One Thousand Nine Hundred and Eighty-nine

AN ACT RELATIVE TO IMPROVING THE INTERNAL CONTROLS WITHIN STATE AGENCIES.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

Notwithstanding any general or special law to the contrary, the following internal control standards shall define the minimum level of quality acceptable for internal control systems in operation throughout the various state agencies and departments and shall constitute the criteria against which such internal control systems will be evaluated. Internal control systems for the various state agencies and departments of the commonwealth shall be developed in accordance with internal control guidelines established by the office of the comptroller.

(A) Internal control systems of the agency are to be clearly documented and readily available for examination. Objectives for each of these standards are to be identified or developed for each agency activity and are to be logical, applicable and complete. Documentation of the agency's internal control systems should include (1) internal control procedures, (2) internal control accountability systems and (3), identification of the operating cycles. Documentation of the agency's internal control systems should appear in management directives, administrative policy, and accounting policies, procedures and manuals.

(B) All transactions and other significant events are to be promptly recorded, clearly documented and properly classified. Documentation of a transaction or event should include the entire process or life cycle of the transaction or event, including (1) the initiation or authorization of the transaction or event, (2) all aspects of the transaction while in process and (3), the final classification in summary records.

(C) Transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority. Authorizations should be clearly communicated to managers and employees and should

Chapter 647, Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies

H 5

include the specific conditions and terms under which authorizations are to be made.

(D) Key duties and responsibilities including (1) authorizing, approving, and recording transactions, (2) issuing and receiving assets, (3) making payments and (4), reviewing or auditing transactions, should be assigned systematically to a number of individuals to ensure that effective checks and balances exist.

(E) Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved. The duties of the supervisor in carrying out this responsibility shall include (1) clearly communicating the duties, responsibilities and accountabilities assigned to each staff member, (2) systematically reviewing each member's work to the extent necessary and (3), approving work at critical points to ensure that work flows as intended.

(F) Access to resources and records is to be limited to authorized individuals as determined by the agency head. Restrictions on access to resources will depend upon the vulnerability of the resource and the perceived risk of loss, both of which shall be periodically assessed. The agency head shall be responsible for maintaining accountability for the custody and use of resources and shall assign qualified individuals for that purpose. Periodic comparison shall be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts. The vulnerability and value of the agency resources shall determine the frequency of this comparison.

Within each agency there shall be an official, equivalent in title or rank to an assistant or deputy to the department head, whose responsibility, in addition to his regularly assigned duties, shall be to ensure that the agency has written documentation of its internal accounting and administrative control system on file. Said official shall, annually, or more often as conditions warrant, evaluate the effectiveness of the agency's internal control system and establish and implement changes necessary to ensure the continued integrity of the system. Said official shall in the performance of his duties ensure that: (1) the documentation of all internal control systems is readily available for examination by the comptroller, the secretary of administration and finance and the state auditor, (2) the results of audits and recommendations to improve departmental internal controls are promptly evaluated by the agency management, (3) timely and appropriate corrective actions are effected

Chapter 647, Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies

H 5

by the agency management in response to an audit and (4), all actions determined by the agency management as necessary to correct or otherwise resolve matters will be addressed by the agency in their budgetary request to the general court.

All unaccounted for variances, losses, shortages or thefts of funds or property shall be immediately reported to the state auditor's office, who shall review the matter to determine the amount involved which shall be reported to appropriate management and law enforcement officials. Said auditor shall also determine the internal control weaknesses that contributed to or caused the condition. Said auditor shall then make recommendations to the agency official overseeing the internal control system and other appropriate management officials. The recommendations of said auditor shall address the correction of the conditions found and the necessary internal control policies and procedures that must be modified. The agency oversight official and the appropriate management officials shall immediately implement policies and procedures necessary to prevent a recurrence of the problems identified.

House of Representatives, December 21, 1989.

Passed to be enacted, *George Furman*, Speaker.

In Senate, December 22, 1989.

Passed to be enacted, *William W. Budge*, President.

January 3, 1990.

Approved, *Richard Riordan*, Governor.

APPENDIX II

Chapter 647 Awareness Letter from the State Auditor and the State Comptroller



The Commonwealth of Massachusetts

Office of the State Auditor
State House
Boston, MA 02133

Office of the Comptroller
One Ashburton Place
Boston, MA 02108

September 19, 2000

Legislative Leadership
Judicial Branch Administrators
Elected Officials
Secretariats
Department Heads

The State Auditor and the Comptroller are both committed to departmental improvements in the Internal Control structure of the Commonwealth. A good system of controls, as you know, assists management in meeting objectives while avoiding serious problems. Chapter 647 of the Acts of 1989, *An Act Relative To Improving Internal Controls Within State Agencies*, establishes acceptable Internal Control systems for state government operations and constitutes the criteria against which we will evaluate internal controls. With the passage of this law, we began a campaign to educate all department staff on the significant role of internal controls in department operations.

In the past few years, departments have made significant progress in the area of internal controls. Every department has certified that they have documented internal controls in the form of an Internal Control Plan. In Fiscal Year 2001, we are focusing our Internal Control Campaign on the review of department risk assessments, as documented within the departments' internal control plans. Internal control plans must, of course, include all aspects of a department's business, programmatic operations as well as financial.

A major requirement of Chapter 647 is that "an official, equivalent in title or rank to an assistant or deputy to the department head, shall be responsible for the evaluation of the effectiveness of the department's internal controls and establish and implement changes necessary to ensure the continued integrity of the system". This official, whom we refer to as the Internal Control Officer, is responsible for ensuring that the plan is evaluated annually or more often as conditions warrant.

During this annual Statewide Single Audit, we continue with our review of the Commonwealth's internal controls. We analyze and evaluate information obtained during the audit process in our continuing effort to educate agencies regarding both the need for internal controls and the risks of not having adequate internal controls in place.

Chapter 647 Awareness Letter from the State Auditor and the State Comptroller

To assist departments with this effort, we provide the following support activities:

- ◆ The Office of the Comptroller offers departments free monthly training on internal controls. These classes are listed in the *OSC Training Bulletin*.
- ◆ The Office of the Comptroller provided a new document entitled the *Internal Control Guide for Managers* on the Office of the Comptroller's Web page: <http://www.osc.state.ma.us/>. Part II of the guide will be available shortly and will replace the current *Internal Control Guide for Departments*, currently available on the Web.
- ◆ Upon request, the Office of the Comptroller provides assistance to departments in the process of redefining or reviewing their internal control plans.
- ◆ As part of the Statewide Single Audit, auditors will review and comment upon departments' internal control plans, risk assessments, and the reporting level of the Internal Control Officers.
- ◆ We have updated and automated the Internal Control Questionnaire (ICQ) for easier submission. These changes to the ICQ will enable OSA and OSC to evaluate department internal controls and monitor their progress.

Chapter 647 also requires that "all unaccounted for variances, losses, shortages, or thefts of funds or property be immediately reported to the Office of the State Auditor" (OSA). The OSA is required to determine the amount involved and the internal control weaknesses that contributed to or caused the condition, make recommendations for corrective action, and make referrals to appropriate law enforcement officials. In order to comply with this law instances must be reported on the *Report on Unaccounted for Variances, Losses, Shortages, or Thefts of Funds or Property* and be submitted to the OSA. Reporting forms can be obtained by contacting the Auditor's office, Room 1819, McCormack State Office Building, or Web Site:

<http://www.magnet.state.ma.us/sao/>.

In conjunction with the above requirement, please note that management is responsible for financial records and systems and must inform, disclose and make representations to the auditors with regards to their management of funds, account activities, programs and systems.

The Offices of the State Comptroller and the State Auditor are committed to the goal of improving the Internal Control structure of the Commonwealth. Thank you for your cooperation and attention on this worthwhile task. Please do not hesitate to call upon the staff of either office for assistance.



A. JOSEPH D. NUCCI
Auditor of the Commonwealth



MARTIN J. BENISON
State Comptroller