Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued July 14, 2011

Information Technology Controls Pertaining to Business Continuity Planning for the Office of the State Treasurer and Receiver General

For the period January 1, 2010 through December 31, 2010

TABLE OF CONTENTS/EXECUTIVE SUMMARY

The State Treasurer and Receiver General, an elected constitutional officer of the Commonwealth, has direct jurisdiction over the Office of the Treasurer and Receiver General (OST), the State Board of Retirement, the Alcoholic Beverages Control Commission, and the Veterans' Welcome Home Bonus program. In addition, the State Treasurer is the chairperson of the State Lottery Commission, the School Building Authority, the Massachusetts Water Pollution Abatement Trust, and the Pension Reserves Investment Management (PRIM) Board, and is the sole trustee of the Commonwealth's Deferred Compensation Plan. The OST is responsible for a variety of important financial functions, as established by Chapter 10, Sections 1 through 69, of the Massachusetts General Laws, including receiving, managing, and investing all funds paid to the Commonwealth; issuing and managing the state's debt; paying state employees and retirees; administering the pension system for state employees and retirees; oversight of tax-deferred retirement savings accounts for over 280,000 government workers; processing and paying the Commonwealth's bills in concert with the Office of the State Comptroller (OSC); managing the Unpaid Check Fund; receiving, safeguarding, and liquidating abandoned property; and making local aid distributions.

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of selected information technology- (IT) related controls regarding disaster recovery and business continuity planning at OST for the period January 1, 2010 through December 31, 2010. Our examination included a review of the 36 various application systems involved in the electronic data backup process of OST; the areas under its direct jurisdiction, including the State Board of Retirement, the Alcoholic Beverages Control Commission, and the Veterans' Welcome Home Bonus program; and the Massachusetts Water Pollution Abatement Trust. These application systems govern such functions as OST's cash management, state retirement, payment processing, legislative payroll, and unclaimed property systems.

Based on our review, we have concluded that, except for the issues addressed in the Audit Results section of this report, during the period January 1, 2010 through December 31, 2010, the OST maintained adequate disaster recovery and business continuity planning for business operations supported by technology and had adequate on-site and off-site storage of backup copies of magnetic media.

Our audit found that OST lacked sufficiently detailed and approved disaster recovery and business continuity plans. Although there is a reasonable likelihood that OST would be able to resume mission-critical business operations, and backup files are generated and electronically transferred to off-site locations, we found that the documentation of the strategies for recovering information technology (IT) capabilities needed to be strengthened given then critical nature of the data in OST"s systems (including data related to funds paid

to the Commonwealth, issuing and managing the state's debt, paying state employees and retirees, administering the pension system for state employees and retirees, etc.). The OST has taken steps to minimize the risk of being unable to recover IT processing should IT systems be rendered inoperable; however, further efforts at documenting its recovery strategies for IT and related business operations are needed to provide increased assurance that business operations can be recovered within an acceptable time period. We noted that the OST did have a draft disaster recovery plan, last updated January 2011, and a draft business continuity plan for the Division of Cash Management, last updated as of February 2011; however, an enterprise-based disaster recovery and business continuity plan for the entire OST did not exist. In addition, OST has not documented a risk assessment, taking into account different scenarios under which IT resources might be rendered inoperable or unobtainable.

INTRODUCTION

Background

The State Treasurer and Receiver General, an elected constitutional officer of the Commonwealth, has direct jurisdiction over the Office of the Treasurer and Receiver General (OST), the State Board of Retirement, the Alcoholic Beverages Control Commission, and the Veterans' Welcome Home Bonus program. In addition, the State Treasurer is the chairperson of the State Lottery Commission, the School Building Authority, the Massachusetts Water Pollution Abatement Trust, and the Pension Reserves Investment Management (PRIM) Board, and is the sole trustee of the Commonwealth's Deferred Compensation Plan. The OST is responsible for a variety of important financial functions, as established by Chapter 10, Sections 1 through 69, of the Massachusetts General Laws, including receiving, managing, and investing all funds paid to the Commonwealth; issuing and managing the state's debt; paying state employees and retirees; administering the pension system for state employees and retirees; oversight of tax-deferred retirement savings accounts for over 280,000 government workers; processing and paying the Commonwealth's bills in concert with the Office of the State Comptroller (OSC); managing the Unpaid Check Fund; receiving, safeguarding, and liquidating abandoned property; and making local aid distributions.

The fiscal year 2011 OST-approved state budget included seven appropriations, excluding the State Lottery Commission. The total amount for these seven appropriations for fiscal year 2011 was approximately $15 million.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of selected information technology (IT) related controls regarding disaster recovery and business continuity planning at the Office of the State Treasurer and Receiver General (OST) for the period January 1, 2010 through December 31, 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our audit was also conducted in accordance with generally accepted industry practices. Audit criteria included generally accepted management control practices as noted in Executive Order 490

and in Control Objectives for Information and Related Technology (CobiT version 4.1), as issued by the Information Systems Audit and Control Association, July 2007.

The scope of our audit was to assess the extent to which OST had addressed disaster recovery and business continuity planning for business operations supported by technology and had in place adequate on-site and off-site storage of backup copies of magnetic media. Our audit included an assessment of OST's capabilities to restore mission-critical application systems and related business processes and partner with the Commonwealth's Information Technology Division (ITD) for business continuity support. Our examination included a review of the 36 various application systems involved in the electronic data backup process of OST; the areas under its direct jurisdiction, including the State Board of Retirement, the Alcoholic Beverages Control Commission, and the Veterans' Welcome Home Bonus program; and the Massachusetts Water Pollution Abatement Trust. These application systems govern such functions as OST's cash management, state retirement, payment processing, legislative payroll, and unclaimed property systems.

We evaluated whether an effective disaster recovery and business continuity plan had been developed and adequate resources would be available to provide reasonable assurance that mission-critical and essential business operations would be efficiently recovered should IT operations be rendered inoperable or inaccessible for an extended period of time. We evaluated whether the disaster recovery and business continuity plan had been tested, reviewed, and approved to provide reasonable assurance of the plan's viability. In this regard, our objective was to also assess whether backup copies of electronic application systems and data files were being generated and stored at secure on-site and off-site locations.

Because OST is dependent upon Massachusetts Information Technology Division's (ITD) Massachusetts Information Technology Center (MITC) for the operation of application systems that support budgetary and human resource functions, we determined whether OST and ITD had collaborated on identifying IT recovery requirements to support implementation of appropriate business continuity plans. We also identified the degree of assistance provided by ITD to assist OST in developing viable business continuity plans. We determined whether ITD provided alternate processing and backup storage facilities and has disaster recovery plans in place to ensure timely restoration of those OST systems and data files supported by MITC.

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations and performing a preliminary review concerning disaster recovery and business continuity planning at OST. We obtained a high-level understanding of the OST's IT environment, identified mission-critical application systems, and conducted a high-level risk assessment pertaining to disaster recovery. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

We interviewed senior management to obtain an understanding of OST's internal control environment, primary business functions, and stated controls. We obtained an understanding of OST's mission-critical functions and application systems by requesting, obtaining, and reviewing IT-related documentation. We interviewed agency officials regarding contingency planning, and IT staff regarding the provision of IT functions for the OST. Documentation requested included OST's plans for the continuation of business operations, such as continuity of operations plans, business continuity plans, and disaster recovery plans. We also interviewed ITD staff who were assigned business continuity planning responsibilities to determine the extent of disaster recovery and business continuity services provided to the OST. In addition, we determined the extent to which OST complied with generally accepted control practices for disaster recovery.

Based on our review, we have concluded that, except for the issues addressed in the Audit Results section of this report, during the period January 1, 2010 through December 31, 2010, the OST maintained adequate disaster recovery and business continuity planning for business operations supported by technology and had adequate on-site and off-site storage of backup copies of magnetic media.

AUDIT RESULTS

BUSINESS CONTINUITY PLANNING

Our audit found that the Office of the State Treasurer and Receiver General (OST) lacked sufficiently detailed and approved disaster recovery and business continuity plans. Although there is a reasonable likelihood that OST would be able to resume mission-critical business operations, and backup files are generated and electronically transferred to off-site locations, we found that the documentation of the strategies for recovering information technology (IT) capabilities needed to be strengthened given then critical nature of the data in OST's systems (including data related to funds paid to the Commonwealth, issuing and managing the state's debt, paying state employees and retirees, administering the pension system for state employees and retirees, etc.). The OST has taken steps to minimize the risk of being unable to recover IT processing should IT systems be rendered inoperable; however, further efforts at documenting its recovery strategies for IT and related business operations are needed to provide increased assurance that business operations can be recovered within an acceptable time period. We noted that the OST did have a draft disaster recovery plan last updated January 2011 and a draft business continuity plan for the Division of Cash Management, last updated as of February 2011; however, an enterprise-based disaster recovery and business continuity plan for the entire OST did not exist.

OST's two data centers are located within five miles of each other at One Ashburton Place in Boston and the Massachusetts Information Technology Center (MITC) in Chelsea. Each data center functions as a primary processing location as well as a backup processing site for the other IT facility. OST utilizes the two data centers to ensure timely recovery of mission-critical and essential functions should an event render applications or data information inoperable or inaccessible at either of the locations. As a general rule, data centers that support mission-critical business operations and also serve as back-up sites are recommended to be located within separate power grids and at a sufficient distance where they would not be impacted by area-wide disasters.

OST has performed a successful self-failover recovery test exercise between the two data center locations using backup copies of data and system applications to restore processing capabilities. In addition, it participated in a successful recovery test of the Massachusetts Management Accounting and Reporting System (MMARS) in November of 2007 in conjunction with Massachusetts Information Technology Division (ITD) at MITC. Furthermore, four designated OST employees

have virtual private network (VPN) access capabilities to assist them in performing disaster recovery tasks in a timely manner.

Planning for a disaster can have many steps or phases in order to minimize the impact on business operations. A business continuity plan should be sufficiently detailed to guide an organization's recovery efforts and encompass a disaster recovery plan and user area plans. OST's business process owners and IT operations should collaborate with the ITD to develop formal documented and approved plans.

In the event of an emergency or disruption of IT services that is specific to either one of the two data centers, OST will execute its recovery effort rather than relying on ITD for restoration of the OST-owned application systems. We note that OST, like other state agencies, relies on technology not under its control. For example, OST relies on such technology to support the Commonwealth's accounts payable function to print hardcopy checks, generate electronic checks, and electronically transfer funds. During fiscal year 2010, OST printed over 1.2 million paper checks and generated almost 5 million electronic check transactions.

Regarding the generation and off-site storage of backup copies of application systems and data files, OST performs daily backups of its electronic processing systems at each location. Daily backups are generated at both OST data centers with backup copies sent to a secure vendor-owned storage facility outside of Boston. The off-site tapes are cycled regularly every two weeks. In addition, each data center electronically transfers transactions to the other data center.

OST is dependent on the Massachusetts Management Accounting and Reporting System (MMARS) and the Human Resources/Compensation Management Systems (HR/CMS) for financial accounting and human resource management, which are both located at MITC. In regards to MITC, although the ITD performs an annual disaster recovery test at the out-of-state vendor-supported Sungard facility in New Jersey, the recovery testing is limited to only a portion of the application systems supported at the center. At the time of the audit, the state did not have an alternative processing facility owned by the Commonwealth for the systems operated at MITC. However, ITD is in the process of establishing a second data center as an alternate processing and backup site in western Massachusetts.

State agencies, per executive orders of the governor, have been required to perform and document their planning efforts for the continuity of operations and government. However, OST is a

constitutional office and as such does not report to the governor. Per Executive Order 490, Executive Branch agencies are required to maintain plans for the continuation of government services in the event of a disaster. These business continuity plans should be incorporated into the daily operations of every secretariat and agency in the executive department, should be reviewed on a regular basis, and tested regularly for those agencies responsible for supplying services during emergencies. With respect to helping to minimize potential risks to IT operations caused by environmental conditions, we found that there were appropriate environmental protection controls in place over the IT environment for OST's two data centers. For example, OST's two data centers, which contain a total of 38 servers, were well maintained and had fire detection and suppression equipment, backup air-conditioning, and an uninterruptible power supply (UPS).

Business continuity plans should be tested to validate their viability and to reduce both the risk of errors and omissions as well as the time needed to restore computer operations. In addition, an effective recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios that would render IT systems inoperable. Specifically, the plan should identify how essential services would be provided for each scenario without the full use of the data processing facility, and the manner and order in which processing resources would be restored or replaced. Furthermore, the plan should identify the policies and procedures to be followed, including details of the logical order for restoring critical data processing functions, either at the original site or at an alternate site. The plan would also identify and explain the tasks and responsibilities necessary to transfer and safeguard backup magnetic copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Sound management practices, as well as industry and government standards, support the need for comprehensive and effective backup procedures and business continuity plans for organizations that depend on technology for information processing. Contingency planning should be viewed as a process to be incorporated within an organization, rather than as a project completed upon the drafting of a formal documented plan. Since the criticality of systems may change, a process should be in place that will identify a change in criticality and amend the contingency plans accordingly. System modifications to IT equipment configurations and user requirements should be assessed in terms of their impact to existing business continuity plans.

Recommendation

We recommend that OST strengthen its business continuity process by enhancing and documenting its recovery strategies to regain mission-critical and essential processing within acceptable time periods. OST needs to ensure that the office-wide disaster recovery and business continuity plan adequately documents recovery strategies with respect to various disaster scenarios, and contains all pertinent information required to effectively and efficiently recover IT and business operations. In addition, OST should develop user area plans to document contingencies and the steps to be followed to continue business operations to the extent possible should IT resources become unavailable. We recommend that all recovery and business continuity planning documents be available in hardcopy and electronic media and stored off-site in secure and accessible locations. In collaboration with ITD, OST should establish procedures to ensure that the criticality of systems is evaluated and business continuity requirements are assessed on an annual basis, or upon major changes to user requirements, the automated systems, or business requirements. As part of business continuity planning, OST should incorporate a strategy in which it collaborates with the Division of Capital Asset Management in the event that an additional alternate processing site is needed to ensure the continuity of operations.

Furthermore, although not explicitly required, we recommend that OST use Executive Order No. 490 for further guidance to address continuity of operations and business continuity planning.

Auditee's Response

> *The OST agrees that its office-wide disaster recovery and business continuity plan documents need to be strengthened. The OST is discussing internally the process to strengthen the documentation of its plan and has had discussions with the Office of the State Comptroller regarding collaboration between OST and OSC for certain key processes. OST will also utilize the recommendations provided by OSA in its process.*