



Report of the Vermont State Auditor

March 27, 2008

INTERNAL CONTROLS

Results of Review at the Office of
the State Treasurer

Thomas M. Salmon, CPA
Vermont State Auditor
Rpt. No. 08-2

Mission Statement

The mission of the Auditor's Office is to be a catalyst for good government by promoting reliable and accurate financial reporting as well as promoting economy, efficiency, and effectiveness in state government.

This report is a work of the Office of the State Auditor, State of Vermont, and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from the State of Vermont or the Office of the State Auditor. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately. Please contact the Office of the State Auditor if you have questions about reproducing this report.

**THOMAS M. SALMON, CPA
STATE AUDITOR**



**STATE OF VERMONT
OFFICE OF THE STATE AUDITOR**

March 27, 2008

The Honorable Gaye Symington
Speaker of the House of Representatives

The Honorable Peter D. Shumlin
President Pro Tempore of the Senate

The Honorable James Douglas
Governor

The Honorable George B. (Jeb) Spaulding
Vermont State Treasurer

Dear Colleagues,

As part of our audit of the Comprehensive Annual Financial Report (CAFR) for the fiscal year ending June 30, 2007, we reviewed internal controls over financial reporting and compliance with laws and regulations at several State organizations, including the Office of the State Treasurer. Our work was performed for the limited purpose of planning and performing this audit and would not necessarily identify all deficiencies in internal control over financial reporting.

In general, we found that the controls that we reviewed at the Office of the State Treasurer were designed appropriately. In particular, I want to commend the Office for its active Internal Audit Committee, which is comprised of staff from its various divisions and which has been responsible for enhancing the Office's control environment. Nevertheless, we also found areas of internal control deficiencies in which improvements could be made. These areas related to the entity-level, cash management, pensions, and information technology controls. Some of the control weaknesses that we found have been fixed and others are in the process of being addressed, which is a credit to the State Treasurer and his staff.

I would like to thank the management and staff of the Office of the State Treasurer for their cooperation and professionalism. If you would like to discuss any of the issues raised by this audit, I can be reached at (802) 828-2281 or at auditor@state.vt.us.

Sincerely,

Thomas M. Salmon CPA

Thomas M. Salmon, CPA
State Auditor

Contents

Report

Introduction	1
Highlights	3
Background	4
Entity-level Controls	6
Pension and Related Control Activities	8
Non-pension Cash and Investment Management Control Activities	12
Debt Management Control Activities	18
Conclusions	19
Recommendations	19
Management's Comments	21
Appendix I: IT General Controls (confidential)	22
Appendix II: Response by the State Treasurer	23

Tables

Table 1: Summary of IT General Control Exceptions	10
---	----

Abbreviations

CAFR	Comprehensive Annual Financial Report
COSO	Committee of Sponsoring Organizations
IT	Information Technology
SAS	Statements of Auditing Standards
VIC	Vermont Information Consortium
VISION	Vermont Integrated Solution for Information and Organizational Needs
VRS	Vermont Retirement System

Introduction

The Office of the State Treasurer plays a major financial role in Vermont's State government, including:

- administering three major pension plans for State employees, teachers, and participating municipalities;
- overseeing the investment of about \$4 billion in State and pension trust fund monies;
- performing statewide cash management activities, such as managing the State's cash balances, processing manual checks and electronic fund transfers, and reconciling most of the State's core bank accounts;
- issuing State bonds authorized by the General Assembly; and
- safeguarding and returning unclaimed or abandoned personal or financial property being held in trust by the State until the rightful owner is found.

In consideration of the Office of the State Treasurer's financial role and in accordance with our internal control audit obligations¹ related to the State's fiscal year 2007 Comprehensive Annual Financial Report (CAFR), our objectives were to assess the Office's internal controls over financial reporting, and compliance with laws and regulations related to its (1) entity-level controls,² (2) pensions and related control activities,³ (3) non-pension

¹*Generally Accepted Auditing Standards* AU Section 150.02 (American Institute of Certified Public Accountants, Inc.). These standards require that auditors obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures.

²Entity-level controls can have a pervasive effect on the overall system of control activities and pertain to the organization as a whole. It encompasses the organization's control environment, risk assessment, information and communication, and monitoring activities.

³Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives.

cash and investment management control activities, and (4) debt management control activities.⁴

Auditing standards define three types of control findings.⁵ First, a control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. According to auditing standards, the auditor must evaluate identified control deficiencies to determine whether these deficiencies, individually or in combination, are significant deficiencies or material weaknesses. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote⁶ likelihood that a misstatement of the entity's financial statements that is more than inconsequential⁷ will not be prevented or detected. A material weakness is a significant deficiency, or combination of significant deficiencies, that result in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

⁴The scope of our fiscal year 2007 audit excluded the control activities related to unclaimed property because this area was reviewed during the fiscal year 2006 audit and it was not material to the State's overall financial statements.

⁵*Statement on Auditing Standards (SAS) 112, Communicating Internal Control Related Matters Identified in an Audit* (American Institute of Certified Public Accountants, Inc., May 2006).

⁶SAS 112 states that the likelihood of an event is "more than remote" when it is at least reasonably possible.

⁷The term "more than inconsequential" describes the magnitude of potential misstatement that could occur. A misstatement is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when aggregated with other misstatements, would clearly be immaterial to the financial statements.

Highlights: Report of the Vermont State Auditor

Internal Controls: Results of Review at the Office of the State Treasurer

(March 2008, Rpt. No. 08-2)

Why We Did This Audit

As part of our audit of the State's fiscal year 2007 CAFR, we evaluated the internal controls over financial reporting, and compliance with laws and regulations at the Office of the State Treasurer because of its central financial role in State government. As part of our evaluation, we reviewed the design of the Office's entity-level controls, pension and related control activities, non-pension cash and investment management control activities, and debt management control activities, but did not perform tests of effectiveness.

What We Recommend

We made a variety of recommendations pertaining to several control and compliance areas, including strategic planning, the validation of participant data for the Vermont Municipal Employees' Retirement System and the Vermont State Teachers' Retirement System, and the oversight of other departments' bank accounts.

Findings

The control areas at the Office of the State Treasurer that we reviewed were largely designed appropriately. Moreover, in several cases, fiscal year 2007 control deficiencies have already been addressed by the Treasurer's Office. For example, passwords to access certain on-line banking and investment systems that had not been changed in a timely manner or not at all were directed to be changed and procedures were put in place to help ensure that they would be changed more frequently in the future.

Notwithstanding these actions, a variety of control deficiencies were found in each area, except for debt management. For example,

- *Entity-level Controls.* The Treasurer's Office does not have a strategic plan, which can be viewed as an important starting point for effective results-oriented management. The Office has elements of such a plan in various documents, but agreed that a more formal plan should be developed and stated that it would begin a strategic planning process in early 2008.
- *Pensions and Related Control Activities.* There was little or no verification to source documents of the participant data reported by the municipalities for the Teachers' and Municipal Employees' Retirement Systems. The Treasurer's Office stated that it planned to begin to conduct field audits in the first half of 2008.
- *Non-pension Cash and Investment Management Control Activities.* 32 V.S.A. §431 requires State agencies and departments to obtain the State Treasurer's approval of bank accounts and reconciliation procedures. The Treasurer's Office did not effectively review the information provided by State organizations regarding these bank accounts. The Office plans a variety of initiatives to improve its oversight of these accounts.

We evaluated each of the control deficiencies contained in this report and consider none to be significant deficiencies or material weaknesses either separately or in combination.

Background

Internal control can be broadly defined as a process, affected by an entity's governance structure, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- effectiveness and efficiency of operations,
- reliability of financial reporting, and
- compliance with applicable laws and regulations.¹

Internal control is a major part of managing an organization. Such controls comprise the plans, methods, and procedures used to meet missions, goals, and objectives. In addition, internal control serve as the first line of defense in safeguarding assets and preventing and detecting errors and fraud.

Scope and Methodology

As part of our audit of the State's fiscal year 2007 CAFR, we gained an understanding of internal controls at the Office of the State Treasurer. Our work was performed for the limited purpose of planning and performing this audit and would not necessarily identify all deficiencies in internal control over financial reporting. We considered the design of the Office's controls and whether they were in place and operational, but did not test the effectiveness of the controls.

To assess the Office of the State Treasurer's entity-level controls, we used guidance developed by the U.S. Government Accountability Office² to develop a set of questions that addressed the control environment, risk assessment, information and communications, and monitoring. We discussed these questions with the Deputy Treasurer and others and reviewed

¹This definition generally comes from the Committee of Sponsoring Organizations of the Treadway Commission (COSO), but we substituted the term governance structure for board of directors used in the original definition to make it more applicable to State government.

²*Internal Control Management and Evaluation Tool* (U.S. Government Accountability Office, GAO-01-1008G, August 2001).

applicable documentation, such as the Office's 2006 annual report (issued January 2007), *Guidelines for State Treasurer's Office Staff* (as amended February 14, 2005), budget documents, and various human resources documents. In addition, we reviewed documentation related to the activities of the Office of the State Treasurer's Internal Audit Committee, such as draft risk assessments.

To review the Office of the State Treasurer's pensions and related control activities, we reviewed procedure documents and performed walkthroughs of major activities, such as receipt of contributions, pension cash and investments, and retirement processing, with applicable staff and management personnel. We also employed a specialist to review the State's actuarial analysis of future pension liabilities. In addition, we gained an understanding of information technology (IT) general controls³ for the Vermont Retirement System (VRS) application system environment. In particular, we assessed whether there were weaknesses in the design of controls in the areas of (1) access to programs and data, (2) application and system software changes, and (3) computer operations. To make this assessment, inquiries were made of management and applicable IT staff and system and other documentation, such as IT policies and procedures, were reviewed.

To assess the non-pension cash and investment management control activities at the State Treasurer's Office, we reviewed procedure documents and performed walkthroughs of the major activities in these areas, such as bank reconciliations, payment and receipt processing, and short-term investing with applicable staff and management personnel. We also contacted the banks and investment firm with which the State performs electronic transactions and obtained information on which State employees had access to their automated banking and investment systems and the type of access granted. We compared this information to the State's record of approved access levels. In addition, we reviewed the State's contracts related to accepting credit cards for payment and discussed the implementation of the terms of these contracts with the Deputy Treasurer, the State's Chief Information Officer, and others.

With respect to debt management control activities, we reviewed the Treasurer Office's written procedures related to bond issuance and other related functions, such as the payment of debt service. We discussed these

³General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They create the environment in which application systems and controls operate.

procedures with the Director of Finance and Investment and the Cash and Investment Manager. We also obtained and reviewed documentation related to the fiscal year 2007 bond issuances, such as the bond offerings. In addition, we assessed the financial reporting of bonds, including the Office's debt service schedule.

We performed this audit in accordance with generally accepted government auditing standards between August and November 2007 in Montpelier.

Entity-level Controls

In general, we found that the entity-level controls of the Office of the State Treasurer to be a strength although we believe that some improvements could be made, particularly in the risk assessment area. The Treasurer Office's entity-level controls encompass its control environment, risk assessment, information and communication, and monitoring activities.⁴ For example,

- *Control environment.* The control environment sets the tone of an organization. It is the foundation for all other components of internal control. Among the factors that influence an evaluation of an organization's control environment are ethical values and integrity, management philosophy and operating style, commitment to competence, and structure. The Treasurer's Office has a variety of mechanisms in place to demonstrate an ethical "tone at the top," such as documented core values and supportive behaviors that have been incorporated into its employee performance evaluation process. Candid and constructive performance evaluations are an important element to demonstrating a commitment to competence. The Treasurer's Office tracks when employee performance evaluations are due, however, it does not have a tracking process in place to ensure that the evaluations are completed in a timely manner. According to the Treasurer's Office, it planned to put a tracking process in place by February 2008.⁵

⁴To guide our assessment of entity-level controls, we generally utilized the internal control frameworks and definitions promulgated by COSO and the U.S. Government Accountability Office. These concepts are also included in State guidance on internal controls, *Internal Control Standards: A Guide for Managers* (Department of Finance and Management).

⁵In its March 2008 response to a draft of this report, the Treasurer's Office reported that it has implemented this tracking process. We have not validated this assertion.

-
- *Risk assessment.* Risk assessment is the identification and analysis of relevant risks to the achievement of the objectives of an organization, which forms the basis of determining how these risks should be managed. According to the State's internal control guidance, after risks are identified, they should be evaluated in terms of likelihood and impact.⁶ In addition, the guide contains an example of a simple evaluation scale that can be used by departments. Although the Treasurer's Office has an active internal audit committee that works on internal control improvements and has begun to document its assessment of risks, the risk assessment methodology being used does not require the use of common criteria that defines what constitutes a high, medium, or low risk area. This would likely result in the inconsistent assessment of risk and make it more difficult to prioritize proposed actions that can be the result of such an assessment. The Treasurer's Office stated that it plans to develop such criteria.

In addition, the Treasurer's Office does not have a strategic plan, which can be viewed as an important starting point for effective results-oriented management. While strategic planning and the plan itself can take different forms, some key elements include (1) a comprehensive mission statement that defines what the agency does, (2) long-term goals and objectives that explain what outcome-oriented results are expected from the agency's major functions and when to expect these results, and (3) strategies to achieve these goals and objectives. The Treasurer's Office has pieces of these elements in various documents. For example, it has developed a mission statement that it has published and is prominently displayed in its offices. Nevertheless, the Office agreed that a more formal strategic plan should be developed and stated that it plans to begin the process in the January to March 2008 timeframe.

- *Information and communication.* For an entity to run and control its operations, it must have relevant, reliable information, both financial and non-financial, related to both internal and external events. Effective communication must occur in a broad sense, flowing down, across, and up the organization. In addition, it is important for management to ensure that effective external communications occur with groups that can have a serious impact on programs, projects, operations, and other activities. For

⁶*Internal Control Standards: A Guide for Managers* (Department of Finance and Management). Likelihood is defined as the probability that an unfavorable event would occur if there were no (or limited) internal controls to prevent or reduce the risk. Impact is a measure of the magnitude of the effect to a department if the unfavorable event were to occur.

example, the Treasurer's Office has critical relationships with external service providers that furnish banking and investment services. The Deputy Treasurer and the Director of Finance and Investment performed a variety of due diligence activities related to the Office's providers, such as reviewing reports filed with the Securities and Exchange Commission and other financial and internal control reports and holding discussions with management.

- *Monitoring.* Internal control environments need to be monitored. Ongoing monitoring occurs in the course of operations, including regular management and supervisory activities. For example, as a result of the initiatives sponsored by the internal audit committee, the Treasurer's Office has implemented improvements in its controls. In particular, in 2007 the Office instituted a daily report to compare expected and actual cash balances in certain major accounts to confirm that expected financial transactions had taken place.

In addition to the entity-level control deficiencies discussed above, the Treasurer's Office did not employ two common mechanisms that can assist in preventing and detecting fraud, particularly from internal sources. Specifically, while the Treasurer's Office provided evidence that it evaluated fraud considerations in its operations, it did not conduct background checks on employees with a high level of fiscal responsibility or provide a formal mechanism for staff to report suspected fraud or for dealing with whistleblowers. However, because we found that the State as a whole lacked these mechanisms, we will be addressing these issues on a statewide rather than on an organization-by-organization basis.

Pensions and Related Control Activities

The Office of the State Treasurer was largely able to demonstrate that its control activities related to its administration of the pension trust funds were adequately designed. However, several IT general control exceptions were found as part of our review of the VRS application system environment. The State Treasurer has generally agreed to fix these exceptions and, in some cases, has already taken action.

Administration of Pension Trust Funds

No control deficiencies were found in our review of control activities related to (1) pension cash and investments, (2) contributions received and related

receivables, (3) benefit obligations and payments, and (4) operating expenses. Examples of the controls enacted by the Office of the State Treasurer in these areas are:

- requiring the submission of, and reviewing, an independent auditor's assessment of internal controls surrounding the custody and recordkeeping functions of State Street Corporation, which provides investor services for the pension funds;
- using lockbox⁷ services for contributions to the Vermont Municipal Employees' Retirement System and the Vermont State Teachers' Retirement System; and
- requiring that the initial calculation of retirement benefits be validated by a second individual to lessen the likelihood of error.

The one area in which a control deficiency was found relates to participant data. In the case of the Teachers' and Municipal Employees' Retirement Systems, there was little or no verification to source documents of the participant data reported by the municipalities. There are mechanisms in place that somewhat reduce the likelihood or effect of incorrect data being reported. Namely, both the Municipal Employees' and Teachers' retirement statutes state that if employers file inaccurate reports, they are responsible for providing reimbursement for any costs incurred as a result of the inaccuracy. Further, if an employer willfully files an inaccurate report it is required to pay an administrative penalty of up to 50 percent of the amount that was not accurately reported. To emphasize this requirement, a pop-up screen informs users entering participant data of these penalties. Moreover, for the Municipal Employees' Retirement System, the State is not financially responsible for the pension obligation. Notwithstanding these mitigating conditions, by not performing periodic reviews of participant data reported for these pension systems, the State is at greater risk of erroneous reporting and fraudulent activity. The State Treasurer's Office acknowledged the need for a participant data verification process. The Office noted that, in the past, the implementation of its new pension system had taken precedence over the establishment of such a process. Nevertheless, the Office stated that it

⁷A lockbox is a bank service that includes processing payments sent to a post office box and making necessary bank deposits. Lockbox services reduce float and provide safeguards related to the collection of funds.

planned to begin to conduct field audits in the first 6 months of calendar year 2008.

IT General Controls

As part of our review of IT general controls at several departments, we reviewed controls related to the VRS applications environment. Because of the potentially sensitive nature of some of the findings related to IT security, we are providing the detailed results to the Office of the State Treasurer in a confidential appendix (appendix I). Table 1 is a high-level summary of the areas reviewed and the extent to which there was reasonable assurance of the controls' existence or exceptions found.

Table 1: Summary of IT General Control Exceptions

Control Objective Description	Number of Controls Reviewed	Number of Exceptions
ACCESS TO PROGRAMS AND DATA: Access controls should provide reasonable assurance that computer resources are protected against unauthorized modification, disclosure, loss, or impairment.		
Information security is managed to promote consistent implementation of security practices, and users are aware of the Vermont State Treasurer's Office's position with regard to information security, as it pertains to VRS reporting applications and data.	2	0
Physical access to IT computing resources, particularly those used to process and report on financial activity, is restricted by the implementation of appropriate identification, authentication and authorization procedures that reduce the risk of unauthorized and/or inappropriate access.	5	0
Logical access to IT computing resources, particularly those used to process and report on financial activity, is restricted by the implementation of appropriate identification, authentication and authorization procedures that reduce the risk of unauthorized and/or inappropriate access.	9	2
Procedures have been established that ensure user accounts are added, modified and deleted in a timely manner and which reduce the risk of unauthorized access and/or inappropriate use of the VRS application and data.	3	1
Controls are in place to monitor the management and maintenance of access rights to the Vermont State Treasurer's Office's financial applications and data.	2	2
Appropriate segregation of duties within the VRS applications and system processes have been identified and have been put into operation.	2	2
Security violations including unauthorized access attempts to the VRS system and application are monitored and reported.	2	0
PROGRAM CHANGES: A disciplined process for testing and approving modified programs prior to their implementation is essential to make sure programs operate as intended and that no unauthorized changes are introduced.		
Changes to the VRS application have been authorized by an appropriate level of management prior to development and migration into production.	2	0
System software and configuration changes to the computer systems that run the VRS application have been authorized by an appropriate level of management.	1	0

Control Objective Description	Number of Controls Reviewed	Number of Exceptions
Changes to the VRS application have been tested, validated, and the results approved prior to being moved into production.	3	0
Operating system software and configuration changes that affect the Vermont State Treasurer's Office's financial computer systems have been tested, validated, and the results approved prior to being moved into production.	4	0
The ability to migrate VRS application changes into production is restricted to authorized staff.	2	2
The ability to migrate system software and configuration changes that affect Vermont State Treasurer's Office's financial computer systems is restricted to authorized staff.	1	1
Emergency changes made to a Vermont State Treasurer's Office's VRS application, system and infrastructure configurations are appropriately managed and approved.	3	0
VRS application documentation is maintained in a timely fashion and access to the documentation restricted to authorized staff.	2	0
COMPUTER OPERATIONS: Controls in this area address a wide variety of issues, such as controls over job processing, backup and recovery procedures, and problem management procedures.		
The VRS application job runs including batch jobs, interface runs and system backups are accurate, complete, and timely.	4	0
Backup and recovery procedures have been implemented that permit databases, transactions feeds and application programs that are necessary for the VRS reporting to be recovered.	5	0
Periodic testing of the VRS system and data file restoration process is conducted and the quality of backup media used to store Vermont State Treasurer's Office's financial applications and data is monitored.	2	1
The back up media for systems and applications used by the VRS application is safeguarded, and only authorized staff have access to the backup media.	2	0
The VRS application hardware, software, and media inventory is tracked and kept current.	2	1
Operations documentation is maintained and access restricted to authorized staff.	1	0
Incidents, problems and errors arising from the VRS application are analyzed and underlying causes resolved.	2	0

The Treasurer's Office has agreed to implement the detailed recommendations that were provided. In some cases the Office stated that it would add additional review procedures or controls and/or draft policies. For example, in its response to a draft of this report, the Treasurer's Office reported that it had begun a review of system, network, and application access, which it expected to complete in March. The Office also reported that it planned to perform a test of its off-site data restoration capabilities shortly. Lastly, the Treasurer's Office stated that it believes that its planned implementation of its Vermont Pension Administration System later in 2008 should eliminate certain IT segregation of duties issues.

Non-pension Cash and Investment Management Control Activities

The Office of the State Treasurer's non-pension cash and investment management encompass a variety of activities, many of which we were able to determine had adequately designed controls. Examples of control activities used by the Office included the following:

- Written procedures were in place for many activities, such as to approve bank accounts opened by other State organizations, perform reconciliations, and to purchase short-term investments.
- Bank account reconciliations were tracked, performed in a timely manner, and reviewed by a supervisor.
- The Treasurer's Office utilized a "positive pay" process for certain bank accounts as a fraud deterrent. This is a process in which the State sends a data file with information on issued checks to TD Banknorth, which provides the State's core banking services. When checks are presented for payment, TD Banknorth checks whether the information on the check is the same as what is in the file. Information on checks with exceptions are faxed to the Treasurer's Office, which is responsible for instructing the bank whether or not to disburse the funds.
- The Treasurer's Office developed a duties matrix that helps it maintain adequate segregation of duties for major financial activities, such as reconciliations, receipts, and disbursements as well as to ensure that it has identified staff that can provide backup support for many of these activities.
- As required by 32 V.S.A. §433, the State Treasurer's Office adopted short-term investment guidelines that we found were followed for the investments held on the five days we reviewed.

Notwithstanding the controls that were in place, we found several control deficiencies in fiscal year 2007 that warrant attention. In some cases, the Treasurer's Office has already taken action to address the deficiency. For example, we brought to the attention of the Deputy Treasurer that the keypad access number that allowed entry to the room in which manual check processing is performed had never been changed and the password used to

log onto the PC that housed these systems had not been changed in several years. The Deputy Treasurer immediately directed that the keypad number and the password be changed and established a policy that they be changed every 30 days. In another case, in fiscal year 2007 the Treasurer's Office had not billed municipalities about \$16,000 in statutorily required interest charges related to the semiannual payments of the statewide nonresidential tax and homestead education tax.⁸ It appears that this was an oversight due to, at least in part, procedures that did not address late payments and the assessment of interest. Once the Treasurer's Office was informed of this deficiency, it implemented revised procedures in time for the December 2007 receipts and collected interest charges from municipalities that did not make timely payments.

The remaining control deficiencies can be categorized into activities for which the Office of the State Treasurer has direct responsibility and those for which it has oversight responsibility. Regarding the former, the deficiencies related to (1) the process the Office uses to ensure that it is aware of, and has approved, all State bank accounts, (2) controls over access to the checkwriter systems, (3) controls over access to on-line banking and investment systems, and (4) segregation of duties.

- To ensure that it is aware of, and has approved, all of the State's bank accounts, the Treasurer's Office sends an annual letter to financial institutions requesting that these entities provide the Office with a list of State depository accounts. However, the 2007 letter was not sent to 31 financial institutions that have a presence in Vermont and did not contain one of the State's Employer Identification Numbers,⁹ which are the numbers that can be used by banks to ascertain what accounts belong to the State. In addition, bank responses to this letter were not tracked and two banks did not respond to the Treasurer's 2007 request. The staff member responsible for maintaining a list of all State government bank accounts stated that she did not track responses to the annual letter because she did not have a list of financial institutions to which the letter was sent. The Treasurer's Office stated that it would expand the

⁸32 V.S.A. §5402(c) requires that the Commissioner of Education determine a municipality's net nonresidential education tax payment and net homestead education tax payment. According to this statute, twice a year (June and December), municipalities are required to pay to the State Treasurer 50 percent of the statewide nonresidential tax and 50 percent of the homestead education tax as determined by the Commissioner. In addition, 32 V.S.A. §5409 requires that municipalities that do not meet these dates be assessed an interest charge of 8 percent per annum of the amount due.

⁹An Employer Identification Number, also known as a Federal Tax Identification Number, is used to identify a business entity.

distribution of the annual letter to include all financial institutions that have a presence in Vermont and would verify the Employer Identification Numbers used.

- In those cases when electronic funds transfers¹⁰ are not used to make payments, the Treasurer's Office prints hard copy vendor checks from the State's principal financial system, the Vermont Integrated Solution for Information and Organizational Needs system (VISION), and utilizes two checkwriting systems that were developed internally to print payroll and pension checks. Recognizing that strong password controls are fundamental to restricting and managing access to computer systems and data, the State's policy is that passwords not be shared. The Office of the State Treasurer was not following this policy. Namely, users share a single user ID and password to log on to the PC containing the checkwriter applications in order to print checks. This weakness is mitigated for VISION payments because this system requires a separate logon and password for each user. However, the retirement and payroll checkwriter applications were not built with this security feature and, therefore, the risk of inappropriate access is higher for these systems. The Treasurer's Office reported that it has put additional controls in place over the paper check process to mitigate the risks associated with the shared user ID and password. Also, the Office is in the process of looking at a third-party software solution to process payroll and pension checks that would address this deficiency.
- The Treasurer's Office makes extensive use of on-line banking and investment systems at TD Banknorth (eCashManager), Chittenden Bank (eBanking), and Fidelity (SLAMNet) to transfers funds, obtain account information, and perform other account activities. There were a variety of control deficiencies related to the management of these accounts. First, there were large discrepancies between the Office of the State Treasurer's records of which State staff has been granted what type of access and TD Banknorth and the Chittenden Bank's records. Second, users of the eBanking and SLAMNet systems were not changing their passwords in a timely manner. For example, for the eBanking system, two users had never changed their passwords and five users had last changed their passwords in 2005. Third, although the Treasurer's Office required users

¹⁰According to the Office of the State Treasurer's 2007 annual report, 49 percent of vendor payments were made via electronic transfer. In addition, in December 2007, 86 percent of the State workforce utilized direct deposit services and 86 percent, 93 percent, and 95 percent of retired municipal employees, state employees, and teachers, respectively, utilized direct deposit services.

of eCashManager to sign user agreements that acknowledged their security obligations, users of eBanking and SLAMNet were not required to sign such agreements. In addition, according to the Office's records, about 25 percent of eCashManager users had not signed the required user security agreements. Lastly, the Office relies on departments, such as the Department of Taxes, that have staff with access to eCashManager to inform them about employees who no longer need such access rather than periodically and regularly requesting that the need for such access be reviewed and approved by the departments. These deficiencies may be traced to the lack of sufficient attention that access to these systems have been given. For example, the Office's IT security plan addresses access to its internal systems, but not to critical external systems such as these on-line banking and investment systems. The Treasurer's Office has begun to take action to address these deficiencies. For example, staff were immediately directed to change their passwords and in October the Office initiated a process to remind staff to change their passwords. In addition, the Treasurer's Office reported that it is in the process of realigning user profiles and plans to require other departments with access to eCashManager to include notification of the Office of staff terminations as part of their termination checklists.

- Segregation of duties is the division of key duties and responsibilities among different people to reduce the risk of error or fraud. No one individual should control all key aspects of a transaction or event. In general, our analysis found that the Office of the State Treasurer had adequate segregation of duties, particularly for those staff that performed bank reconciliations. However, the staff member that is primarily responsible for printing checks had incompatible duties in that she is also responsible for processing invoices for the Office, including entering invoices into VISION. Although the Treasurer's Office had established an approval process for these invoices, the staff member's VISION access included approval authority and, therefore, this control could have been circumvented. Moreover, this staff member had the authority to request that a new vendor be established in VISION, which adds to the risk that improper behavior would be undetected. After we brought this situation to the attention of the State Treasurer's Office, it implemented a process to require authorization for requests to add or change vendor information in VISION. In addition, the Office has been working on a solution to further

restrict the staff member's access authority within VISION while not interfering with her ability to perform required tasks.¹¹

Regarding its oversight activities, the Office of the State Treasurer has statutory responsibilities related to bank accounts and the acceptance of credit cards by the State. In some cases the actions that the Office took in response to these requirements were not complete. First, with respect to the oversight of bank accounts, 32 V.S.A. §431 requires State agencies and departments to obtain the approval of the Treasurer for (1) the establishment and maintenance of bank accounts and (2) bank reconciliation procedures. In this oversight role, the Treasurer's Office requires the departments to submit information related to their bank accounts, including the names of individuals who are the authorized signers and who perform the reconciliations and authorize expenditures or withdrawals from the account. In addition, the Treasurer's Office requires the departments to submit their reconciliation procedures. Moreover, in 2005 the Treasurer's Office instructed the departments that their reconciliation procedures must include signatures by the persons performing and approving the reconciliation. Our analysis found that the State Treasurer's Office did not effectively review the information provided by the departments. For example, regarding 30 bank accounts managed and reconciled by other departments,

- 12 department reconciliations did not indicate who performed the reconciliation and 15 did not have evidence of supervisory approval.
- There was inadequate segregation of duties for 22 accounts. For example, in some cases, the same person authorized expenditures, signed checks, and reconciled the bank account. The Treasurer's Office did not check whether the departments had the same individual performing incompatible duties (e.g., authorized signer and reconciling the account). In addition, the Treasurer's Office guidance on the management and reconciliation of bank accounts did not include guidance or instructions on proper segregation of duties.
- Although the Treasurer's Office had copies of each of the departments' reconciliation procedures, (1) not all of the reconciliation procedures contained each of the procedural elements in the office's 2005 instructions

¹¹In its March 2008 response to a draft of this report, the Treasurer's Office reported that it has implemented a corrective action to restrict the staff member's access within VISION. We have not validated this assertion.

and (2) very few of the procedures contained evidence of review and approval by the Treasurer's Office.

The Treasurer's Office plans a variety of initiatives to address the above condition, including (1) reviewing the remaining department accounts to determine whether segregation of duties are adequate, (2) as applicable, contacting departments to ensure that corrective action is taken, (3) providing additional guidance to the departments, and (4) conducting spot checks of department account reconciliations to ensure that proper procedures are in place throughout the year.

With respect to the Treasurer's Office oversight of the State's acceptance of credit cards for payment, 32 V.S.A .§583 states that the State Treasurer shall (1) contract with banks and bank credit card companies or others to provide for the use of credit or debit cards for payment and (2) assist those who elect to accept credit card payments with establishing procedures for accepting these payments. Although the Treasurer's Office had taken action related to these requirements additional actions are needed for full compliance.

- As required by the statute, the Treasurer's Office contracted with TD Banknorth Merchant Services Group on July 1, 2003 to provide debit and credit card processing services to multiple State organizations. This contract explicitly excludes Internet credit card transactions. Internet credit card transactions are handled by the State's Web portal manager, the Vermont Information Consortium (VIC), through a contract signed by the Chief Information Officer. The State Treasurer's Office did not take part in negotiating this contract nor did it sign the agreement. In addition, as part of this contract, VIC negotiates service level agreements with State organizations, which can address electronic transactions, such as the acceptance of credit cards through the Internet. The Treasurer's Office also has not been a party to these agreements. The Treasurer's Office stated that it will shortly begin working on a memorandum of understanding with the Chief Information Officer's office and plans to establish protocols and procedures for the Treasurer's Office to review and approve future service level agreements.
- The TD Banknorth Merchant Services Group contract requires specific security procedures for entities that conduct "card-not-present" transactions, including the use of firewalls, security patches, anti-virus software, unique user IDs, security testing, security policies, and physical security over cardholder data. The departments were provided only limited guidance regarding these security requirements. Treasurer's Office officials stated that training on accepting credit cards and the security

requirements in the contract was provided to departments at the beginning of the Merchants Services contract. However, no supporting documentation was provided. The Treasurer's Office also noted that periodic security notices have been provided by the Merchants Services Group and provided copies of five notices issued between September 30, 2004 and October 31, 2006, but only the earliest notice provided a partial summary of its information security requirements. Because of the sensitivity of credit card data and how such information can be abused if stolen, we believe that a more aggressive approach is warranted to ensure that the State is adequately securing this data.¹² The Treasurer's Office agreed that a more comprehensive system of monitoring compliance, training, and the encouragement of best practices is needed. The Office reported that it has met with the Merchants Services Group to develop a plan towards that end. For example, in February 2008, the Office held a training session for departments accepting credit card payments. In addition, the Treasurer's Office reported that it planned to issue quarterly newsletters in conjunction with TD Banknorth focusing on security issues and best practices.

Debt Management Control Activities

Once authorized by the Legislature, the State Treasurer, with the approval of the Governor, may issue general obligation bonds. In fiscal year 2007, the Treasurer's Office issued three series of general obligation bonds totaling \$44.5 million to fund capital projects throughout the State. In addition, by statute, the Treasurer's Office is responsible for paying the principal and interest on such bonds as they come due.¹³

We reviewed the design of controls related to the (1) issuance of the fiscal year 2007 bonds, (2) monitoring of existing debt and payments of principal and interest, and (3) financial reporting of bond obligations. Among the controls utilized by the Treasurer's Office were the (1) establishment of separate investment accounts to hold the amount of the bonds sold in order to invest such funds until the money is needed to pay expenses, (2) use of a debt service schedule to validate invoices that are received two weeks before a payment due date, and (3) use of a third-party professional organization to

¹²We are not expressing an opinion as to whether adequate security measures are being taken by the departments because such an assessment was beyond the scope of this audit.

¹³32 V.S.A. §902.

assist in the preparation of relevant documents supporting the offering. We found no control deficiencies related to the Office of the State Treasurer's debt management activities that affected financial reporting.

Conclusions

The Office of the State Treasurer has implemented a myriad of internal controls related to the entity-level controls, pensions and related control activities, non-pension cash and investment management control activities, and debt management control activities. Such controls improve the likelihood that the Office is positioned to achieve effectiveness and efficiency of operations, reliability of financial operations, and compliance with laws and regulations. Nevertheless, there were a number of areas in which improvements can be made. These improvements are expected to further enhance the Office's controls and ensure compliance with laws and regulations.

Recommendations

Entity-level Controls

We recommend that the State Treasurer:

- Track the completion of employee performance evaluations to ensure that they are accomplished in a timely manner.
- As part of the risk assessment process, define and use common criteria as to what constitutes a high, medium, and low risk.
- Develop a strategic plan that includes an overarching vision for the Office, strategies on how it plans to meet its major objectives, and outcome-oriented performance measures to demonstrate results.

Pensions and Related Control Activities

We recommend that the State Treasurer:

- Periodically test participant data related to the Teachers' and Municipal Employees' Retirement Systems on a sample basis for completeness, accuracy, and existence.

-
- Implement the IT general control recommendations related to its Vermont Retirement System application environment contained in the confidential appendix.

Non-pension Cash and Investment Management Control Activities

We recommend that the State Treasurer:

- Send the annual bank account verification letter, with a complete list of the State's Employer Identification Numbers, to all financial institutions that have a presence in Vermont and track responses to ensure that requested information is provided.
- Expeditiously implement a checkwriting system(s) in which the actions of each user can be authenticated.
- Expeditiously review and confirm the appropriateness of access levels of all State staff (including those of other departments) who have access to on-line banking systems to ensure that such access is needed and is commensurate with job responsibilities. The office should also establish a process to periodically and regularly review such access levels.
- Establish a process, in conjunction with applicable departments, to ensure the timely reporting of terminated staff with on-line banking access to the Treasurer's Office.
- Eliminate the segregation of duties violation related to the staff member who is responsible for printing checks and processing invoices for the Office.
- Review the segregation of duties established by departments with their own bank accounts and assess whether adequate segregation of duties are being maintained and, if not, notify the applicable department(s) of this control weakness.
- Issue guidance to the departments on segregation of duties related to bank accounts.
- Review and explicitly approve that departments' reconciliation procedures are in compliance with the Office of the State Treasurer's instructions and

periodically assess whether such reconciliations are being performed in accordance with the approved procedures.

- Review and approve future service level agreements associated with the VIC contract that include the acceptance of credit card transactions over the Internet.
- Request that the departments that accept credit cards certify that they meet the security requirements in the TD Banknorth Merchants Services Group contract and provide periodic reminders to the departments of their security responsibilities and additional guidance on an as-needed basis.

Management's Comments

On March 6, 2008, the State Treasurer provided comments on a draft of this report (reprinted in appendix II). The Treasurer stated that his office was in general agreement with the findings in the report and had taken, or planned to take, action on the issues in the report. We noted these actions, or planned actions, in applicable sections of the report.

- - - - -

In accordance with 32 V.S.A. §163, we are also providing copies of this report to the Secretary of the Agency of Administration, Commissioner of the Department of Finance and Management, and the Department of Libraries. In addition, the report will be made available at no charge on the State Auditor's web site, www.auditor.vermont.gov.

Appendix I: IT General Controls

This appendix was provided solely to the Office of the State Treasurer due to the potentially sensitive nature of the information.

Appendix II: Response by the State Treasurer

JEB SPAULDING
STATE TREASURER

RETIREMENT DIVISION
TEL: (802) 828-2305
FAX: (802) 828-5182



STATE OF VERMONT
OFFICE OF THE STATE TREASURER

UNCLAIMED PROPERTY DIVISION
TEL: (802) 828-2407

ACCOUNTING DIVISION
TEL: (802) 828-2301
FAX: (802) 828-2884

TO: Tom Salmon, Auditor of Accounts
FROM: Jeb Spaulding, State Treasurer 
DATE: 6 March 2008
RE: Comments -- Internal Control Review Report

Deputy Treasurer Beth Pearce and I have had the opportunity to study the Internal Control Review Report issued by your office; we thank you for the thorough work by you and your staff. Below are our Comments in response to the Report; should you wish to discuss anything in this memo, please feel free to contact Beth at 828-5197 or me at 828-1452.

Summary

The Treasurer's Office has reviewed the Internal Control Review Report conducted by the Office of the Vermont State Auditor. As noted in the report, there were no significant deficiencies or material weaknesses, either separately or in combination. As the Auditor has reported, the Treasurer's Office has implemented a "myriad of internal controls" that "improve the likelihood that the Office is positioned to achieve effectiveness and efficiency of operations, reliability of financial operations, and compliance with laws and regulations." Much of this has been accomplished through the work of an Internal Audit Committee and a commitment by all the office staff to continually evaluate and improve our internal controls.

The report does identify a number of deficiencies or areas for improvement and includes recommendations related to our internal controls. We appreciate the time and effort of the Auditor's office staff in completing the multiple reviews, their professional approach, and their willingness to discuss findings with our staff through an open and productive dialogue. Substantial progress has been made as a result. Our office is in general agreement with the findings presented by the Auditor and has taken immediate steps to address the issues noted. We will continue to work cooperatively with all parties to further enhance the levels of internal controls at the Office of the State Treasurer.

As noted in the response below, all recommended changes have been made and/ or appropriate remediation plans have been developed and are in the process of implementation.

Appendix II: Response by the State Treasurer

Entity Level Controls

The Auditor's Office made three recommendations in this area specific to the Treasurer's Office, as noted on page 19 of the report. The first recommendation relates to tracking the completion of employee performance evaluations. The Auditor noted that the Treasurer's Office maintains a tracking document that includes the dates when the performance evaluation of each staff is due but did not track when evaluations are completed. A tracking mechanism is now in place. The second recommendation is related to the definition of common criteria in risk assessment. The Treasurer's Office Internal Audit Committee will define common criteria of what constitutes a high, medium, and low risk as part of its risk assessment/mitigation approach. Finally, the Auditor recommended that the Treasurer's office develop an office-wide strategic plan, and has identified components of that plan. The Treasurer's Office had previously developed a mission statement and a set of organizational values. In addition, goals and objectives are outlined in a number of documents including the budget presentation, the annual report, and individual performance reviews. We agree, however, that a more formal strategic plan should be developed. This has been discussed with senior staff and the Office will begin this process in the third quarter of FY08.

Pension Related Control Activities

A control deficiency has been identified in the verification of participant data related to the teachers' and municipal employees' retirement systems. This refers to payroll data submitted by the various municipal and school payroll officers to support the employee and, in the case of the municipal system, employer contributions. This data is reported quarterly from over 700 reporting entities. Historically, this data was reported in manual reports, requiring considerable effort to total and reconcile, leaving little time for analysis. Over the last several years, the Treasurer's Office has developed Web-based employer reporting modules which are now used to report this information. In addition to creating efficiencies in the reconciliation process, this system has afforded the enhanced capacity to review and analyze the data for unusual trends. It also includes a set of balancing requirements, improving the accuracy of the data provided by the locally-based payroll officers. In addition, our consulting actuary reviews this data for unusual trends as part of the annual valuation process. This includes changes in pay from one year to the next over the expected threshold, and questions pertaining to service credit, including breaks in service.

The automated system includes a pop-up screen that informs users of penalties that could be incurred if incorrect data is reported. Moreover, as noted by the Auditor, the State is not financially responsible for the pension obligation and, by statute, if a municipality willfully files an inaccurate report it is required to pay an administrative penalty of up to 50 percent of the amount that was not accurately reported. Notwithstanding these mitigating controls, we agree with the Auditor's recommendation that the Treasurer's Office periodically test participant data on a sample basis for completeness, accuracy, and existence and, in fact, began working on a plan to address this matter in January 2006. A field audit plan was developed and finalized in 2006. Our plan was to begin auditing a sample of reporting entities in both the teachers' and municipal employees' retirement systems in 2006. However, given our staffing limitations, the required activities associated with the implementation of the Vermont Pension Administration System (VPAS) took precedence. Our plan at this point is to begin the field audits in the first six months of calendar 2008. We have recently submitted a copy of the audit protocol to the Auditor's office for review and comment prior to initiating the field audits.

Appendix II: Response by the State Treasurer

As part of this audit, the Auditor's office completed an assessment of IT general controls related to the pension systems. Because of the sensitive nature of the IT data, only summary data was included in the report. The Treasurer's Office has reviewed these findings extensively with the Auditor's Office and specialists employed by them. A brief overview of our actions relative to these findings follows, using the reference points provided in the summary on page 10 of the report.

IT/Access to Programs and Data

There were seven control objectives related to access to programs and data, and 25 controls were reviewed. Seven exceptions were noted; two related to password length, syntax, and the frequency of change. As a result of these findings, the network log-on password was improved (in length, lockout frequency, and complexity) in October 2007 to meet Microsoft's current best practices recommendations. Staff training has been held on password management. The issues inherent in the mainframe's RACF security and in the retirement legacy application will be rectified in 2008 by the implementation of the new VPAS retirement system (a multi-year project implemented by the State Treasurer's Office in 2004), utilizing the improved network password referenced above. A third exception was an insufficient process for identifying the termination of employment of payroll officers who report retirement contributions via the Web. It should be noted that the access is for information only; receipts and other transactions are processed through other mechanisms. In response, policy/procedure guidance was established requiring prior notification of payroll officer terminations and distributed to payroll officers, school business managers, and superintendents, and appropriate senior management.

Two additional exceptions were noted relative to the need to perform periodic reviews of system, network, and application access. While the Treasurer's Office does have various tracking reports and log systems to prevent and detect unauthorized use, we agree that a more formal review procedure was needed. Procedures have been developed and most of these reviews were performed in February 2008. The balance will be completed in early March.

Two exceptions related to insufficient segregation of duties between the development and production implementation of programming changes, and periodic review of same. Given the small IT staff (three) with its specialized roles, achieving an optimum level of segregation is difficult. The office has, however, initiated a number of risk mitigation steps and downstream controls. The implementation of additional controls will be explored. The implementation of the VPAS retirement system in later in calendar year 2008 should eliminate significant issues, because programming changes will be made by the vendor through a formal process.

IT/Program Changes

In total, eight control objectives related to program changes were identified and 18 controls were reviewed; three exceptions were noted. All three relate to the same segregation of duties issue between the development and production implementation of programming changes, similar to the above comment. Again, risk mitigation controls have been implemented and additional controls will be explored.

IT/Computer Operations

In total, seven control objectives related to computer operations were identified and 18 controls were reviewed; two exceptions were noted. One related to the lack of a formal off-site data restoration

Appendix II: Response by the State Treasurer

testing policy, and the performance of such a test. As a result of considerable developmental effort, the Office of the State Treasurer has had a comprehensive business continuity plan for the last three years. The plan is frequently updated to reflect additional improvements and to identify appropriate linkages with our business partners. The Treasurer's Office has reached out to its partnering institutions and departments, including DII, and has established a functional remote site at McFarland State Office Building in Barre. As statewide standards and redundant emergency systems continue to evolve, the Office has recently reached the point where practical restoration scenarios can be created. These are in development, and a test is expected to be performed in March 2008.

The second exception referenced hardware/software asset inventory management. While the Office of the State Treasurer complies with a statewide policy requiring an annual update and submission of its hardware/software inventory through the VISION system, has written procedures and maintains a file of software licenses, we agree that a more formal procedure for periodic reviews would be helpful and will implement such a procedure.

Non-Pension Cash and Investment Control Activities

The findings can generally be grouped into four categories: delegated agency bank accounts (bullet points one and six through eight on pages 19 and 20), access to online banking systems (bullet points 3 and 4), controls related to departments accepting credit card (bullets 9 and 10), and various operations at the Treasurer's Office (bullets 2 and 5). These have been grouped together for a more comprehensive response.

Delegated Agency Bank Accounts

The findings related to non-pension cash and investment controls demonstrate that the Office of the State Treasurer has adequate internal control over the core banking and investment accounts that reside at the Treasury and that are used to manage the cash operations of the state. These include timely reconciliation and review of accounts, detailed reconciliation procedures, a duties matrix to help ensure adequate segregation of duties within the Office of the State Treasurer, and controls over bank accounts, such as positive pay. The audit did identify issues related to bank accounts approved by the Treasurer's Office and delegated to outside agencies and departments. These accounts generally have smaller value and lower transaction volumes than the major accounts that are used and directly managed by the Office of the State Treasurer. The delegated accounts generally are established to fit specific needs for the department, such as escrow accounts, court bail accounts, patient accounts, and Corrections inmate accounts. We do, however, recognize the existence of an internal control deficiency and a need to improve our communication, monitoring, and oversight with respect to these accounts. The Treasurer's Office has taken significant steps and developed additional plans to address these matters.

The Office of the State Treasurer sends an annual confirmation letter to financial institutions doing business in Vermont requesting that they identify all bank accounts attached to the State of Vermont's Employer Identification Numbers (EIN). The annual distribution of the bank account confirmation letter will include all financial institutions with a presence in Vermont. The BISHCA listings of financial institutions doing business in Vermont will be used to create the confirmation letter distribution list. In addition, the list of EIN numbers to be used in the letter will be verified with the Department of Finance and Management (DFM) to ensure accuracy and completeness. Receipt of

Appendix II: Response by the State Treasurer

responses will be verified to the distribution list, and timely follow-up will be done for any responses outstanding after the requested reply date.

One of the controls that the Office of the State Treasurer maintains over these delegated bank accounts is to send an annual year-end questionnaire and request for current account reconciliation for each delegated account. The questionnaires and reconciliations are to be reviewed by the Office of the State Treasurer staff to assure that adequate controls are in place, such as timely reconciliation, appropriate reviews and approvals, and segregation of duties. The audit findings indicate that the Office of the State Treasurer did not adequately review the delegated bank accounts for adequate controls for the year-end 2007. The Office of the State Treasurer has reviewed the sample from the audit, agrees with the findings, and has begun the review of the remaining accounts to assess whether there is adequate segregation of functions in each account. This review will be documented, and the Office of the State Treasurer will contact individual departments to assure that corrective action is taken as necessary. Staff at the Office of the State Treasurer has revised guidance practices on management and reconciliation of bank accounts to reflect these concerns and other best practices, and is in the process of distributing the information to agencies delegated to manage such bank accounts. In addition, during the course of the year the Office of the State Treasurer staff will conduct spot checks of delegated account reconciliations to ensure that proper procedures are in place throughout the year.

Further, the Office of the State Treasurer began a review of departmental bank accounts in general to determine which services and associated transactions might be more appropriately serviced directly through the core bank accounts managed by the Office of the State Treasurer and on the VISION system, eliminating the need for separate bank accounts where feasible. We requested information from the departments beginning in April 2007, in addition to the annual questionnaires. We have met with DFM to discuss these issues and, with DFM in attendance, met with the one of the major users of departmental bank accounts (the Courts). There was general agreement that many of the accounts could be eliminated, and the Office of the State Treasurer is currently working with this department, and will work with others, to reduce the number of delegated bank accounts.

Within the newly reorganized Treasury Operations Division, the Cash Management Unit will be responsible for the receipt, review, and approval of the opening/closing of departmental bank accounts. The Cash Management Unit will assess the need for the account and provide the appropriate guidance to the departments. Our request forms and questionnaires will be revised as needed to support this functionality. Departments will be asked to acknowledge that continued approval to keep the account active is contingent upon compliance with the procedures. All new accounts will be reviewed at 60-day, 90-day, and six-month intervals, in addition to the annual review and the audit steps noted above, to assure that appropriate and agreed upon practices are in fact in place. The intent is to assure that good practices are in place when new accounts are established.

Access to Online Banking Systems

The audit findings also indicated that there were improvements that could be made regarding control of users' access to the electronic banking systems that the Office of the State Treasurer and other departments use to assist in managing bank accounts. The Office of the State Treasurer requested and received user information from TD Banknorth, Chittenden, and Fidelity on all electronic banking systems, and has taken or is taking the appropriate steps to realign user profiles. We will continue to

Appendix II: Response by the State Treasurer

request the user access profile information, for verification and review purposes, from Chittenden and Fidelity on a six-month basis, as recommended. The TD Banknorth system has the largest number of users, and TD Banknorth is currently rolling out a new electronic banking system. With this roll-out, the responsibility for managing users in the TD Banknorth electronic banking system will pass from TD Banknorth to the Office of the State Treasurer.

The Office of the State Treasurer is developing policies and procedures to ensure that user access is granted, periodically reviewed, and revoked appropriately and timely. A user maintenance form will be developed and rolled-out so that requests to add or change user access will be in writing and approved by an appropriate supervisor. The ability to maintain users will be under dual control in the system and will also include output review and sign-off. The Office of the State Treasurer will verify that persons for whom access is requested are active employees within the requesting department prior to granting access. The Office of the State Treasurer has revised its termination checklist to incorporate removal of access to these systems and the updated form is in use. As part of our guidance to departments, we will require that their "termination checklists" include notification to the Office of the State Treasurer to terminate access as appropriate. Training of departments in the new TD Banknorth electronic banking system occurred in late January and February.

Additionally, all the Office of the State Treasurer staff members with access to these electronic banking systems have signed security agreements. For department staff, we will be requiring new agreements for all staff as we convert to the new TD Banknorth system in February. All departmental staff will be required to sign security agreements at or subsequent to their training. Staff in the Cash Management Unit will monitor receipt of these security agreements. New users will be required to sign and return a security agreement prior to their user access being activated. Any user delinquent in completing a security agreement will be locked out of the electronic banking system until the security agreement is received by the Office of the State Treasurer.

Controls Related to Departments Accepting Credit Card Payments

According to state statute, the Office of the State Treasurer shall assist those who elect to accept credit card payments with establishing procedures for accepting these payments. The Treasurer's Office contracts with TD Banknorth Merchant Services, a division of TD Banknorth, to provide credit card and bank card services. In addition, the Department of Information and Innovation (DII) has contracted with the Vermont Information Consortium (VIC) to administer the State's Web portal, which includes building online services that allow state agencies and departments to accept credit cards via the Internet. The Auditor has recommended that the Treasurer's Office should review and approve those future service level agreements associated with the VIC contract that include the acceptance of credit card transactions over the Internet. The Treasurer's Office is in agreement with this recommendation and has contacted DII. DII concurs and will work with the Treasurer's office to write a brief MOU and establish protocols and procedures. In the meantime DII, VIC, and the Office of the State Treasurer have coordinated a number of credit card-related issues including discussion relative to interface with VISION and training of credit card processing staff at the various agencies as noted below.

In addition, the Auditor recommended that the Treasurer's Office request departments which accept credit cards certify that they meet the security requirements in the Merchants Services Group contract, and provide periodic reminders to the departments of their security-related responsibilities

Appendix II: Response by the State Treasurer

under the contract and additional guidance on an as-needed basis. To improve the integrity and security of the payment system, the leading credit card associations have collaboratively developed policies requiring that merchants and service providers comply with Payment Card Industry (PCI) Data Security Standards (DSS). When accepting electronic payments, each department in the State of Vermont operates as a "merchant." The primary focus of the PCI standards is to help merchants (departments) improve the safekeeping of cardholder information by tightening overall security standards. The PCI Security Standards Council mandates compliance with certain information security requirements for any merchant that "transmits, stores, accesses, or processes" cardholder information. Both the Department of Information and Innovation and the Treasurer's Office take these concerns seriously and have taken proactive steps to assure our compliance with PCI/DSS standards and generally to encourage best practices.

The Merchants Services Group has provided updates in the form of notices with the department monthly statements. For instance, the 9/30/04 statement included a notice plus an attached guidance for "Merchant Requirements for Securing Cardholder Information." To improve security, the Treasurer's Office met with Merchant Services, including their risk management staff and other TD Banknorth staff, in a series of meetings beginning April 2007 to review the State's compliance with payment card industry (PCI) standards. Merchant Services advised us at that time that we were PCI-compliant. The Treasurer's Office also contacted the Vermont Information Consortium (VIC) to verify their compliance with standards and found them to be compliant.

We do agree that a more comprehensive system of monitoring continued compliance, training, and the encouragement of best practices should be put into place, as recommended by the Auditor.

In an effort to encourage best practice and to ensure continued compliance, DII and the office of the State Treasurer jointly hosted a training session for all departments accepting credit card payments in February 2008. We reviewed best practices and provided guidance on security standards, including presentations by industry experts. Although not required under current industry standards, we now require all user departments to complete the Payment Card Industry (PCI) Data Security Standard "Self - Assessment Questionnaire." Ongoing annual submissions will also be required. The annual questionnaire was developed by the Payment Card Industry Committee and includes an attestation of compliance which must be completed by all departments. Departments are in the process of completing these materials and submitting them to the Office of the State Treasurer. In addition, a quarterly update newsletter will be prepared jointly by TD Banknorth and Treasury staff for distribution to user departments focusing on security issues and best practices. Finally, new department staff will be required to complete a PCI orientation. The Treasurer's Office is currently assessing the feasibility of some form of field audit program and will discuss this with the Auditor's Office, as well.

Various Operations at the Treasurer's Office

The Auditor has recommended expeditious implementation of check-writer system(s) in which the actions of each user can be authenticated. As noted by the Auditor, the Treasurer's Office performs the check-writing function in VISION for vendors who receive paper checks. It also utilizes two check-writing systems that were developed internally to perform check-writing for payroll and retirement. The logical access controls related to the check-writer system are insufficient in that there is a single-user ID and password used by all users to access the PC containing the check-writer applications. This

Appendix II: Response by the State Treasurer

weakness is mitigated for VISION payments because VISION requires a separate logon and password for each user. However, the retirement and payroll check-writer applications do not have this added level of protection.

The Treasurer's Office is in the process of looking at a third-party software solution to process checks for payroll and retirement that will address these issues. In addition, the following controls have also been implemented. The Treasurer's Office immediately put into effect a daily check inventory sign-off, to be completed by the individual operator. In addition, this log is reviewed each day by a supervisor. The ending check numbers and inventory control number on the log are verified to the actual check stock inventory by the supervisor. The combination to the keypad outside the check processing room is changed every 30 days, as is the password to the check-writer application.

Finally, while the Auditor's Office noted that, in general, this office has adequate segregation of duties, one violation was observed related to the staff member who is responsible for printing checks and processing invoices for the Office. We have evaluated this finding as it relates to adding vendors and the processing of invoices. While no one in the Treasurer's Office has the ability to add, change, or delete a vendor in VISION (this function is completed by DFM), Treasury staff have the ability to request this action by DFM, using the standard request format. To enhance controls, the Treasurer's Office has revised its procedures requiring that all requests to add a vendor or change vendor information be submitted to DFM only with approval by a supervisor/manager. DFM staff members have been notified not to act on any requests that do not have the appropriate approvals. In addition, we have taken steps with DFM to develop and implement a new VISION profile that eliminates the ability to approve invoices for payment, yet permits the staff member to run pay cycles. We believe this eliminates the exception.

\\CAudit\mem\jeb0315.08