STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

DEPARTMENT OF STATE TREASURER

RALEIGH, NORTH CAROLINA

APRIL 2005

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

DEPARTMENT OF STATE TREASURER

RALEIGH, NORTH CAROLINA

APRIL 2005

STATE OF NORTH CAROLINA
Office of the State Auditor

Leslie W. Merritt, Jr., CPA, CFP
State Auditor

2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601
Telephone: (919) 807-7500
Fax: (919) 807-7647
Internet http://www.osa.state.nc.us

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
The Board of Directors of Department of State Treasurer
The Honorable Richard H. Moore, State Treasurer

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the Department of State Treasurer. This audit was conducted from November 18, 2004, through February 21, 2005. The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards.*

The primary objective of this audit was to evaluate IS general controls at the Department of State Treasurer. The scope of our IS general controls audit included general security, access controls, program maintenance, system development, systems software, physical security, operations procedures, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary and audit results which detail the areas where the Department of State Treasurer has performed satisfactorily relevant to our audit scope, where improvements should be made, and where further study is necessary.

We wish to express our appreciation to the staff of Department of State Treasurer for the courtesy, cooperation, and assistance provided to us during this audit.

North Carolina General Statutes require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Leslie W. Merritt, Jr.

Leslie W. Merritt, Jr., CPA, CFP
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at Department of State Treasurer from November 18, 2004, through February 21, 2005. The primary objective of this audit was to evaluate the IS general controls in place during that period. Based on our objective, we report the following conclusions.

General security involves the establishment of a reasonable security program that addresses the general security of information resources. Our audit identified two significant weaknesses in general security. See Audit Finding 1, *Website Content Displays Sensitive Information* for further information, and See Audit Finding 2, *Information on the Mainframe is not Classified* for further information.

The **access control** environment consists of access control software and information security policies and procedures. We noted several weaknesses in access controls. Due to the sensitive nature of the conditions found in these weaknesses, we have conveyed these findings to management in a separate letter pursuant to the provision of the North Carolina General Statute 147-64.6(c)(18).

Program maintenance primarily involves enhancements or changes needed to existing systems. We found that modified programs did not receive user approval prior to placement into the production environment. Our audit identified one significant weakness in program maintenance. See Audit Finding 3, *Application Programmers' Access to Production Source Libraries* for further information.

Systems software is the collection of programs that drive the computer. The selection of systems software should be properly approved and the software should be maintained by the computer center**.** Our audit did not identify any significant weaknesses in systems software.

Systems development includes the creation of new application systems or significant changes to existing systems. Systems development projects can be expensive and affect the operations of the agency in significant ways. Consequently, the agency should have a strategic or master plan for systems development. Each development project should be managed using project management techniques and should adhere to a clearly defined systems development methodology. When a project is completed, the finished product should include a comprehensive set of documentation so that the users, operators and programmers each have the information they need to do their jobs. Our audit did not identify any significant weaknesses in systems development.

Physical security primarily involves the inspection of the agency's computer center for the controls that should reasonably secure the operations of the computer center from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. Our audit did not identify any significant weaknesses in physical security.

The **operations procedures** of the computer center include all of the activities associated with running application systems for users. Our audit did not identify any significant weaknesses in operations procedures.

A complete **disaster recovery** plan that is tested periodically is necessary to enable the Department of State Treasurer to recover from an extended business interruption due to the destruction of the computer center or other agency assets. Our audit identified one significant weakness in disaster recovery. See Audit Finding 4, *Access to Offsite Storage Documentation and Facility is Inadequate* for further information.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the North Carolina General Statutes chapter 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. IS general control audits are examinations of controls which effect the overall organization and operation of the IS function. This IS audit was designed to ascertain the effectiveness of general controls at the Department of State Treasurer.

SCOPE

General controls govern the operation and management of computer processing activities. The scope of our IS general controls audit was to review general security issues, access controls, program maintenance, systems software, system development, physical security, operations procedures, and disaster recovery which directly affect Department of State Treasurer's computing operations.

METHODOLOGY

We audited policies and procedures, interviewed key administrators and other personnel, examined system configurations, toured the computer facility, tested on-line system controls, reviewed appropriate technical literature, reviewed computer generated reports, and used security evaluation software in our audit of information systems. We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

The primary mission of the Department of State Treasurer is to serve the citizens of North Carolina as the state's banker and Chief Investment Officer, administer the public employee retirement systems and other employee benefit plans for public employees, which are assigned to the department. In addition, the agency assists units of local government in the state with maintaining strong fiscal health and the agency administers the escheated and abandoned property program for the state.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where the Department of State Treasurer has performed satisfactorily and where recommendations have been made for improvement.

GENERAL SECURITY ISSUES

General security issues involve the maintenance of a sound security management structure. A sound security management structure should include a method of classifying and establishing ownership of resources, proper segregation of duties, a security organization and resources, policies regarding access to the computer systems and a security education program. The Department of State Treasurer has established an adequate security program that addresses the general security of information resources. However, our audit identified two significant weaknesses in general security.

AUDIT FINDING 1: WEBSITE CONTENT DISPLAYS SENSITIVE INFORMATION

We found sensitive information posted on the Department of State Treasurer's website, which could allow hackers to gain and use information from the website to exploit Department of State Treasurer systems. The Department of State Treasurer's current security policies do not address security standards for website content.

Recommendation: The Department of State Treasurer should review information currently posted on the website for appropriateness and immediately edit or move this information to a secure location, such as an intranet. The Department of State Treasurer should update their policies to address security standards for website content to ensure that the website does not reveal sensitive information.

Auditee's Response: DST has updated its Web Content policy to require a formal review process to prevent any future information leakage.

AUDIT FINDING 2: INFORMATION ON THE MAINFRAME IS NOT CLASSIFIED

The Department of State Treasurer has not classified information on the mainframe. The Department of State Treasurer policy requires that all data be classified into the following three categories: sensitive, confidential, or public. Data classification ensures that only authorized users view information containing confidential information such as Social Security numbers or bank accounts. Without classifying data, users may gain unauthorized access to sensitive or confidential information.

Recommendation: The Department of State Treasurer should classify data on this system as required by their policy to ensure that sensitive and confidential information is protected from unauthorized access.

Auditee's Response: DST has performed a risk analysis on this finding and does not plan on implementing changes for the following reasons: 1) we are in the process of replacing the mainframe in its entirety by the end of 2007, 2) we have concluded that the level of effort to classify mainframe information would provide only a small benefit to the department, and 3) the level of risk is acceptable.

ACCESS CONTROLS

The most important information security safeguard that The Department of State Treasurer has is its access controls. The access controls environment consists of access control software and information security policies and procedures. An individual or a group with responsibility for security administration should develop information security policies, perform account administration functions and establish procedures to monitor and report any security violations. During our audit, we noted network architecture controls that strengthen the control environment at the agency. However, we also found several weaknesses in access controls. Due to the sensitive nature of the conditions found in the weaknesses, we have conveyed these findings to management in a separate letter pursuant to the provision of North Carolina General Statute 147-64.6(c)(18).

PROGRAM MAINTENANCE

Program maintenance consists of making changes to existing application systems. Programmers should follow program change procedures to ensure that changes are authorized, made according to specifications, properly tested, and thoroughly documented. Application programmers should be restricted to a test environment to ensure that all changes to production resources are tested and approved before moving the changes into production. Changes to application system production programs should be logged and monitored by management. Our audit identified one significant weakness in program maintenance.

AUDIT FINDING 3: APPLICATION PROGRAMMERS' ACCESS TO PRODUCTION SOURCE LIBRARIES

The application programmers can move programs from test into production. As a result, application programmers could make unauthorized changes to programs on the mainframe. The Department of State Treasurer policies require that duties be segregated between programming, approving program changes, and placing these changes into the main computing environment. This is normally achieved by restricting the application programmer's access to the test environment. The programmers will then make all necessary changes and submit the source code to the quality assurance staff. The quality assurance staff will then review and approve changes, compile and test, and move these program changes into the mainframe environment. However, The Department of State Treasurer has not restricted application programmer's access to only the test environment. The Department of State Treasurer identified this risk in 2001, but has not implemented a permanent solution and has not implemented an interim compensating control, such as monitoring for unauthorized changes to programs currently residing on the mainframe.

Recommendation: The Department of State Treasurer should implement their permanent software solution to control and segregate a programmer's ability to make unauthorized program changes. The Department of State Treasurer should also scan through current programs residing on the mainframe for modification dates which do not correspond with quality assurance's approval documentation.

Auditee's Response: DST has already implemented a permanent software solution to address this finding. DST has also established a scanning process to assure that all changes are authorized.

SYSTEMS SOFTWARE

Systems software is the collection of programs that the computer center uses to run the computer and support the application systems. This software includes the operating system, utility programs, compilers, database management systems and other programs. The systems programmers have responsibility for the installation and testing of upgrades to the system software when received. Systems software changes should be properly documented and approved. Our audit did not identify any significant weaknesses in systems software.

SYSTEMS DEVELOPMENT

Systems development includes the creation of new application systems or significant changes to existing systems. Systems development projects can be expensive and affect the operations of the agency in significant ways. Consequently, the agency should have a strategic or master plan for systems development. Each development project should be managed using project management techniques and should adhere to a clearly defined systems development methodology. When a project is completed, the finished product should include a comprehensive set of documentation so that the users, operators and programmers each have the information they need to do their jobs. Our audit did not identify any significant weaknesses in systems development.

PHYSICAL SECURITY

Controls over physical security are designed to protect a computer center from service interruptions resulting from fire, water, electrical problems, vandalism, and other causes. Physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. Our audit did not identify any significant weaknesses in physical security.

OPERATIONS PROCEDURES

The operations of the computer center include all of the activities associated with running application systems for users. Procedures should be in place to control the scheduling and running of production jobs, restarting production jobs when problems occur, storing, handling and mounting of tapes, and maintaining computer equipment. Our audit did not identify any significant weaknesses in operations procedures.

DISASTER RECOVERY

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, many agency services would grind to a halt. To reduce this risk, computer service centers develop disaster recovery plans. Disaster recovery procedures should be tested periodically to ensure the recoverability of the data center. Our audit identified one significant weakness in disaster recovery.

AUDIT FINDING 4: ACCESS TO OFFSITE STORAGE DOCUMENTATION AND FACILITY IS INADEQUATE

A review was conducted to determine if backup tapes, offsite tape inventory, and recovery documentation are stored offsite in a secure facility. This review checked for completeness and timeliness of stored back-up information. As a result, the following weaknesses were identified that may compromise the Department of the State Treasurer's ability to recover critical systems in the event of an emergency:

- A complete set of the most current backup tapes was not stored offsite.
- Access to backup tapes is limited only to weekdays during business hours.
- The terms of the storage services contract for recovery documentation do not include delivery to the alternate computing site(s).
- The offsite storage facility is not of sufficient distance from the Department of State Treasurer to minimize the potential for simultaneous disaster prohibiting access to both locations.

The above weaknesses existed in part because testing of the Disaster Recovery Plan has historically bypassed actual pickup of current backup tapes and recovery documentation.

Recommendation: The Department of State Treasurer should perform the following:

- Ensure that a complete set of backup tapes are selected and delivered to the office storage facility per the established schedule
- Review access to the offsite storage facility to ensure that emergency access is timely and meets the agency's business requirements.
- Review the storage services contract for recovery documentation to ensure that delivery to alternate site(s) can be achieved in an emergency.

- Evaluate if the distance from the Department of the State Treasurer to the offsite facility is sufficient to ensure the recovery of critical systems in the event a disaster affects an area close to the Department of State Treasurer.
- Include as a future test the actual pick-up and test of backup tapes and documentation from offsite locations to ensure that these materials will be available.

Auditee's Response: DST is addressing this finding by: 1) negotiating a new contract with a secure storage facility which will provide adequate access to DST employees, 2) reviewing the tape rotation process and making changes to insure accuracy, and 3) we will be using offsite tape sets in all future disaster recovery tests.

[This Page Left Blank Intentionally]

DISTRIBUTION OF AUDIT REPORT

In accordance with General Statutes 147-64.5 and 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable Michael F. Easley	Governor of North Carolina
The Honorable Beverly M. Perdue	Lieutenant Governor of North Carolina
The Honorable Richard H. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. David T. McCoy	State Budget Officer
Mr. Robert L. Powell	State Controller

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

President Pro Tempore
Senator Marc Basnight, Co-Chair
Senator Charles W. Albertson
Senator Thomas M. Apodaca
Senator Daniel G. Clodfelter
Senator Walter H. Dalton
Senator Charlie S. Dannelly
Senator James Forrester
Senator Linda Garrou
Senator Kay R. Hagan
Senator Fletcher L. Hartsell, Jr.
Senator David W. Hoyle
Senator John H. Kerr, III
Senator Ellie Kinnaird
Senator Jeanne H. Lucas
Senator Anthony E. Rand
Senator R. C. Soles, Jr.
Senator Richard Y. Stevens
Senator A. B. Swindell, IV
Senator Scott Thomas

Speaker of the House
Representative James B. Black, Co-Chair
Representative Alma S. Adams
Representative Martha B. Alexander
Representative Harold J. Brubaker
Representative Lorene T. Coates
Representative E. Nelson Cole
Representative James W. Crawford, Jr.
Representative William T. Culpepper, III
Representative W. Pete Cunningham
Representative Beverly M. Earle
Representative Pryor A. Gibson, III
Representative Joe Hackney
Representative R. Phillip Haire
Representative Dewey L. Hill
Representative Lindsey H. Holliman
Representative Julia C. Howard
Representative Howard J. Hunter, Jr.
Representative Margaret M. Jeffus
Representative Daniel F. McComas
Representative Charles L. McLawhorn
Representative Henry M. Michaux, Jr.
Representative Richard T. Morgan
Representative Edd Nye
Representative William C. Owens, Jr.
Representative Deborah K. Ross
Representative Drew P. Saunders
Representative Wilma M. Sherrill
Representative Joe P. Tolson
Representative Edith D. Warren
Representative Thomas E. Wright
Representative Douglas Y. Yongue

Other Legislative Officials

Mr. James D. Johnson	Director, Fiscal Research Division

April 21, 2005

ORDERING INFORMATION

Copies of this report may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Internet: http://www.ncauditor.net

Telephone: 919/807-7500

Facsimile: 919/807-7647