STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

THE OFFICE OF THE GOVERNOR

INFORMATION TECHNOLOGY SERVICES

DECEMBER 2008

OFFICE OF THE STATE AUDITOR

LESLIE MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

THE OFFICE OF THE GOVERNOR

INFORMATION TECHNOLOGY SERVICES

DECEMBER 2008

STATE OF NORTH CAROLINA

Office of the State Auditor

Leslie 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
George Bakolia, State CIO

Ladies and Gentlemen:

We have completed our audit of the Information Technology Services (ITS). This audit was conducted during the period from February 4, 2008 through June 30, 2008. The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate Information Systems general controls at ITS. The scope of our IS general controls audit included general security, access controls, program maintenance, systems software, systems development, physical security, operations procedures, and disaster recovery. We also followed up on the resolution of previous audit findings and recommendations and determined the corrective action taken. Other IS general control topics were reviewed as considered necessary. Our audit was limited to the activities of ITS and did not include consideration of procedures performed by clients of ITS.

This report contains an executive summary and audit results which detail the areas where ITS 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 the Information Technology Services division 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 Merritt, Jr., CPA, CFP
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at the Information Technology Services (ITS) division of the Office of the Governor from February 4, 2008 through June 30, 2008. 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. Information Technology Services (ITS) has established a reasonable security program that addresses the general security of information resources. *We did not note any significant weaknesses in general security controls of information resources*.

The **access control** environment consists of access control software and information security policies and procedures. We found 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 North Carolina G.S. 147-64.6(c)(18).

Program maintenance primarily involves enhancements or changes needed to existing systems. *Our audit did not identify any significant weaknesses in program maintenance.*

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. *We did not identify any significant weaknesses in systems software during our audit.*

Systems Development includes the creation of new application systems or significant changes to existing systems. *We did not identify any significant weaknesses in systems development during our audit.*

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. *We did not identify any significant weaknesses in physical security during our audit.*

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

A complete **disaster recovery** plan that is tested periodically is necessary to enable ITS to recover from an extended business interruption due to the destruction of the computer center or other ITS assets. *We did not identify any significant weaknesses in disaster recovery.*

[This Page Left Blank Intentionally]

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 ITS.

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, systems development, physical security, operations procedures, and disaster recovery which directly affect ITS's computing operations. Other IS general control topics were reviewed as considered necessary.

ITS is a service bureau for many state agencies and several of these agencies are responsible for developing, maintaining, and securing their own applications. Our audit was limited to the general controls for which ITS has responsibility.

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 application controls. 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 General Assembly, "*. . . in recognition of the need to better manage the acquisition and use of information technology in general state government*, . . ." created the Office of Information Technology Services in 1983 by consolidating the State Computer Center, and the data centers of the Department of Transportation, the Department of Correction, and the Employment Security Commission. Originally placed within the Department of Administration, ITS was later moved by executive order to the Office of State Controller and the Department of Commerce on March 1, 1987 and April 14, 1997, respectively. Effective November 1, 2000, Senate Bill 1345 of the 1999 Session of the General Assembly transferred the Office of Information Technology Services from the Department of Commerce to the Office of the Governor as well as expanding its responsibilities to include enterprise management of information technology (IT) assets.

Legislation passed by the General Assembly in 2004 (Session Law 2004-129, more commonly known as Senate Bill 991) directed the Office of State Budget and Management, in conjunction with others, to develop a plan to consolidate information technology (IT) infrastructure, staffing, and expenditures in executive branch departments where a statewide approach would be more economical. The mission of the IT Consolidation program is to optimize information technology investments by focusing on the consolidation of local area network, voice, data center (servers), security, desktop, and service desk operations and services. The goal of the IT consolidation program is to augment consolidation with appropriate funding and organizational models that will support and sustain the consolidation effort and allow agencies to focus on applications to meet business and citizen needs.

The State CIO is appointed by the governor to set policy and direction for information technology and manage the delivery of IT services to state agencies. The State CIO also provides leadership for the state's technology initiatives, is responsible for IT procurement, and develops strategic IT partnerships with state agencies, colleges, universities, public schools, local governments, and others. During the period under review, the Office of Information Technology Services has almost 500 positions and an annual budget of approximately $204 million. By statute, North Carolina's Chief Information Officer has dual roles. The State CIO leads the Office of Information Technology Services, the state's information technology agency, and also has broad authority in planning and budgeting, purchasing, project approval and oversight, and security.

ITS is divided into three areas: Enterprise Services, ITS Operations, and the Office of the State CIO. Enterprise Services includes Statewide Technical Architecture and Engineering, Consolidation Initiatives, the Operational Excellence Program, and E911. ITS Operations includes ITS Service Desk / Business Relation Management, Computing Services, Enterprise Desktop Management Services, Enterprise Solutions, Telecommunication Services, and Information Security. The Office of the State CIO includes the Enterprise Project Management Office, the Enterprise Security and Risk Management Office, Financial Services, Personnel Services, Statewide IT Procurement, IT Policy and Programs, and Agency General Counsel.

[This Page Left Blank Intentionally]

AUDIT RESULTS

The following audit results reflect the areas where ITS 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. ITS has established a reasonable security program that addresses the general security of information resources. *We did not note any significant weaknesses in general security during our audit.*

ACCESS CONTROLS

The most important information security safeguard that ITS has is its access controls. The access controls environment consists of ITS' 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. We noted a number of 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 G.S. 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. *We did not note any significant weaknesses in program maintenance.*

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 system 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. ITS' 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. *We did not note any significant weakness in the operations procedures of the computer center during our audit.*

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, ITS' operations would be interrupted. To reduce this risk, computer service centers develop business continuity plans. Business continuity procedures should be tested periodically to ensure the recoverability of the data center. *Our audit did not identify any significant weaknesses in disaster recovery.*

ORDERING INFORMATION

Audit reports issued by the Office of the State Auditor can be obtained from the web site at www.ncauditor.net. Also, parties may register on the web site to receive automatic email notification whenever reports of interest are issued. Otherwise, copies of audit reports 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

Telephone: 919/807-7500

Facsimile: 919/807-7647