STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

THE OFFICE OF THE GOVERNOR

INFORMATION TECHNOLOGY SERVICES

JULY 2003

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

THE OFFICE OF THE GOVERNOR

INFORMATION TECHNOLOGY SERVICES

JULY 2003

STATE OF NORTH CAROLINA

Office of the State Auditor

Ralph Campbell, Jr.
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) division of the Office of the Governor. This audit was conducted during the period from January 21, 2003 through March 28, 2003. 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 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,

Ralph Campbell, Jr.

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at the Information Technology Services (ITS), division of the Office of the Governor from January 21, 2003 through March 28, 2003. 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. 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 noted that an ITS employee is hosting a personal web page on an ITS personal computer. See Current Audit Results and Audit Responses, Audit Finding 1, A Personal Web Page Is Hosted On An ITS Personal Computer for additional information. We also found several other 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. We noted that formal, written program maintenance policies and procedures have not been completed. See Prior Audit Results and Audit Responses, Prior Audit Finding 1, No Formal, Written Program Change Control Procedures for additional 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. 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 note 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 noted that the business continuity plan for ITS is incomplete. See Prior Audit Results and Audit Responses, Prior Audit Finding 2, ITS Business Continuity Plan is Incomplete for additional information.

[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.[1]

[1] In 1992 the State created the Information Resource Management Commission to provide statewide coordination of information technology resources planning. The IRMC provides state enterprise IT leadership including increased emphasis and oversight for strategic information technology planning and management; policy development; technical architecture; and project certification. Pursuant to North Carolina General Statute 147-33.78 numerous state officials serve on the IRMC including four members of the Council of State who are appointed by the Governor. The State Auditor has been appointed a member of the IRMC and elected as chair of the IRMC by its members.

[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 (at the time called State Information Processing Services) by consolidating the State Computer Center, 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 July 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 IT assets.

General Statutes (GS) §147-33.82 stipulates, among other things, that ITS shall provide cities, counties, and other local governmental units with access to ITS information resource centers and services. These services are provided through use of mainframe computers, distributed computing servers, and statewide voice, data, and video networks. ITS operates as an internal service fund[2] and, as such, the costs of providing services are recovered through direct billings to clients.

Organizationally, ITS reports to the Governor's Office and the State CIO reports directly to the Governor. ITS can be thought of in three logical groupings. One group handles the operations of the organization and consists of ITS Operations (which includes Computing Services, Telecommunications Services, Enterprise Solutions, and Facilities) and Customer and Public Relationship Management. The second grouping carries responsibility for the State CIO's statewide IT responsibilities and includes Enterprise Technology Strategies, the Statewide IT Procurement Office, and the ITS Security Office. The third grouping is administration that consists primarily of Financial Services, Personnel Services and the offices of the State CIO and the Chief Operating Officer. All of these Divisions are described below.

Operational

Telecommunication Services (TS) plans, provides, manages, and maintains the state's extensive array of data, voice and video telecommunications systems and services. The customer base includes state agencies, universities, community colleges, cities and counties, as well as K-12 school systems. Customers receive consultative and planning support for determining and applying the best technology in attaining their program goals. TS also

[2] An "internal service fund" is a fund used to account for services provided exclusively to other state agencies on a cost reimbursement basis.

provides the resources to manage the implementation of voice, video and data systems as well as manage the daily operation of systems. The state's buying power is leveraged in the competitive establishment of efficient and effective systems and services for universal delivery throughout the state. Telecommunications Services offerings fall in the categories of voice, video, and data. TS consists of 129 positions.

Computing Services (CS) provides hosting services in both the mainframe and distributed environment for its clients. CS is dedicated to providing responsive, cost-effective, customer-oriented, centrally managed computing services to all State agencies and county and city governments. CS services offerings include: computer operations support, remote LAN management support, platform engineering, online systems, service coordination. CS consists of 146 positions.

Enterprise Solutions (ES) provides an array of systems development and support for state and local agencies. ITS Enterprise Solutions provides services that are common across agencies and the enterprise, such as Identity and Access Management, e-Procurement, NCMail, electronic calendaring, and electronic payment processing. It supports and maintains portals, Web sites and Web-enabled applications. Support is provided for mainframe applications and distributed systems. Enterprise Solutions consists of 26 positions.

Customer and Public Relationship Management (CPRM) provides support and services to all ITS customers, serving as a focal point for customer questions and for coordination of communication regarding ITS initiatives. The Office's mission is to provide strategic direction and tactical support for managing customer relationships and public relations through improving internal and external communications and facilitating cross-functional interactions. The Office is developing appropriate processes for communicating with and serving customers, increasing training and awareness for customer relations, and enhancing the ITS Customer Support Center (help desk) with new features and streamlined processes for quicker and more focused responses. CPRM consists of 30 positions.

Statewide

The **Enterprise Technology Strategies** section provides state-level leadership in managing information technology and telecommunications resources, including staff assistance to the Information Resource Management Commission (IRMC) as they formulate state-level information technology strategies, plans, policies, and procedures. There are 12 positions in the Enterprise Technologies Strategies section.

The **Security Office** ITS Security Office (ISO) oversees a comprehensive security and business continuity management program in order to provide a secure and sustainable operational environment for ITS clients that complies with the statewide technical security architecture, security policy, industry best practices, and legal and regulatory requirements. The ISO consists of 14 positions.

Statewide IT Procurement Office is responsible for the procurement of IT assets for North Carolina, subject to the rules published in Title 9 NC Administrative Code, Chapter 6. Recognizing the unique nature of IT procurement, ITS is implementing procurement reforms that should assist agencies in maximizing their ability to thrive in the changing IT environment. It consists of ten positions.

Administration

The **Personnel Services** section consists of seven positions with responsibility for overseeing all aspects of personnel management for ITS' 425 positions. Duties include recruiting, hiring, orientating, and training of staff. Personnel services also manage administration of state policies, procedures, and guidelines.

The **Financial Services** section handles financial transactions for ITS. This section is responsible for monitoring the agency's budget, processing payroll, check writing, and preparation of the agency's financial statements. Personnel within this section oversee the rate setting process, approval of contracts between ITS and vendors, and the procurement of assets. Additionally, staff is responsible for developing Request for Proposals and evaluating bids received for convenience contracts. There are 26 positions for the Financial Services section.

[This Page Left Blank Intentionally]

CURRENT AUDIT RESULTS AND AUDITEE RESPONSES

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.

Audit Finding 1: A PERSONAL WEB PAGE IS HOSTED ON AN ITS PERSONAL COMPUTER

As part of our testing for unauthorized web services, we identified an employee hosting, on an ITS personal computer, a web page that contains links to personal web pages. The web page included a link to a personal consulting business web page. Hosting a personal web page on an ITS computer constitutes a misuse of state property. In addition, unauthorized web services may expose the ITS network to unauthorized access and attacks.

Recommendation: The page should be removed from the ITS personal computer immediately. The computer should be examined to determine if there are any other files that are hosted that are inconsistent with State law. The annual training needs to reinforce that State property is not to be used in this manner.

Agency's Response: Management agrees with the recommendation. This was a violation of State and ITS policy by an individual employee. The page was immediately removed upon discovery and formal disciplinary action was taken against the employee. Additional files not identified in the audit were also found and removed. No data was compromised.

ITS has an ongoing effort to inform employees of acceptable use policies. This effort includes mandatory, annual security training.

We noted other 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. Formal, written program maintenance policies and procedures have not been completed. This is an unresolved finding from a prior audit. See Prior Audit Results and Audit Responses Audit Finding 1, No Formal, Written Program Change Control Procedures for additional information.

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 review.

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 would grind to a halt. 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. We noted that the business continuity plan for ITS is incomplete. This is an unresolved audit finding from a prior audit. See Prior Audit Results and Audit Responses Audit Finding 2, ITS Business Continuity Plan Is Incomplete for additional information.

[This Page Left Blank Intentionally]

PRIOR AUDIT RESULTS AND AUDITEE RESPONSES

The following presents the status of reportable findings, prior year findings, and recommendations presented in our April 2001 IS audit report.

PROGRAM MAINTENANCE

Prior Audit Finding 1: NO FORMAL, WRITTEN PROGRAM CHANGE CONTROL PROCEDURES

The Enterprise Solutions Division of ITS provides application development and maintenance for state and local agencies, as well as ITS. During our prior audit, we determined that Enterprise Solutions does not have formal, written application program change policies and procedures. The Enterprise Solutions Division is in the process of developing formal written and approved policies and procedures addressing application program change management. Each application development group follows their own unwritten program change policies and procedures. Without formally written and approved policies and procedures, the risk of unauthorized changes being made to application programs increases.

This finding remains unresolved. During the current audit, we determined that ITS still does not have a formal, written application program change policies and procedures.

Auditee's Response: Management partially agrees with this finding. There are policies, procedures, software tools, and methods in place presently for performing and supporting various software development and maintenance functions across the entire ITS-ES (Enterprise Solutions) application portfolio. Some of these controls and procedures are very mature (Mainframe applications for example) and others are still evolving (Web applications for example). Some of these procedures are in a written form and others that are not, but all are still understood by the people working in these functions. There is no doubt that a complete, end-to-end, fully documented SDLC (Software Development Life Cycle) Methodology is desirable. Over the next 12-24 months, we will be evaluating, designing, improving, and evolving - on an iterative basis – an SDLC Methodology that will accommodate the broad range of software applications and platforms that ITS-ES maintains and develops. It is important to note that a holistic approach will be taken for developing this SDLC Methodology so that the needs of each application and technology set will be represented both in terms of written procedures as well as software tools support. The basis for this SDLC Methodology will be the Software Engineering Institute's (SEI) Capability Maturing Model for Software (CMM-SW). The pace for developing and deploying this methodology will be strongly influenced by the availability of personnel and the funding necessary to support it.

DISASTER RECOVERY

Prior Audit Finding 2: ITS BUSINESS CONTINUITY PLAN IS INCOMPLETE

During our prior audit, we determined that ITS has a Business Continuity Plan that includes recovery procedures for the mainframe platform as well as the IBM Unix servers. However, the plan does not identify business recovery procedures for the Novell platform, NT platform, LAN platform and non-IBM Unix servers located at ITS. The Novell and NT platforms serve as the infrastructure for the NCWAN (Wide Area Network). The ITS LAN platform provides employees with office automation software as well as serves as the front-end for entry of financial data into the North Carolina Accounting System (NCAS). The non-IBM Unix servers contain important client applications, databases and data.

In addition, we noted that the existing business continuity plan does not include the following components:

- Alternative procedures to allow end-users to manage their workloads until processing resumes have not been identified.
- An inventory of equipment has not been documented and arrangements to acquire replacement equipment have not been made.
- Availability of special stock supplies has not been determined.
- Approval of the plan by the senior management including both information systems and user department managers has not been documented.

This finding is partially resolved. During the current audit, we noted that ITS has made great strides in the development of their Business Continuity Plan (BCP) since the last audit. The BCP has task lists that document the business recovery procedures for the mainframe platform. There was a separate recovery plan for each of the agency's critical services (applications). Also, there were recovery plans for the business support areas. The business recovery procedures for the platforms that were not in the last BCP are now incorporated in the agency's critical services individual plans. We reviewed the current ITS Business Continuity Plan for the following components that, at a minimum, a complete plan should at least include:

a) Statement of the assumptions, such as the maximum time without computing, underlying the plan for each ITS division.

b) Identification of critical applications for each ITS customer and the priority in which these applications will be restored if resources are limited.

c) Identification of key personnel and their assignments during the restoration of processing for each ITS division.

d) Alternative procedures to manage workloads until processing resumes for each ITS division.

e) Arrangements to use an alternate computer facility during the reconstruction of the replacement center, if needed, for each ITS division.

f) An inventory of equipment, and arrangements to acquire replacement equipment for each ITS division. This could include written agreements with vendors.

g) An inventory of telecommunications circuits and equipment, and arrangements to resume telecommunications required for each ITS division.

h) Availability of special stock supplies required for each ITS division.

i) Provisions for regularly updating and testing the plan.

j) Executive management has signed off on the plan. (A provision for formal update reviews to be signed off should be in place (i.e., once a year)

We noted that the current BCP has the following missing components:

- Executive management has not signed off on the Business Continuity Plan.
- Several of the ITS division plans did not contain the statement of the assumptions, such as the maximum time without computing, underlying the plan.
- Several of the ITS division plans did not contain alternative agency user department procedures to manage their workloads until processing resumes.
- Several of the ITS division plans did not provide for the availability of special stock supplies.

Recommendation: The various individual plans of the BCP should have the missing components incorporated and executive management should sign off on the BCP plan.

Auditee's Response: The Office of Information Technology Services has worked and will continue to work diligently to protect ITS information assets, facilities, and staff should a business disruption occur resulting from an emergency/disaster. The agency won national recognition for its efforts in October with a NASCIO 2002 Recognition Award for ITS Business Continuity Planning and Recovery Services Program. ITS received this national honor because its business recovery plan program framework and policy met or exceeded industry best practices.

Following this framework, ITS is continuously developing and updating business recovery plans for its critical services. The framework includes the categories recommended by COBIT (Control Objectives for Information and related Technology).

In response to the four missing components cited:

(1) Executive management has not signed off on the Business Continuity Plan.

ITS Policy 18.05 was revised on 4/9/2003 to require annual executive management signoff. The signature process has been developed effective June 1, 2003. The State CIO is expected to sign the plans by 7/31/2003.

(2) Several of the ITS division plans did not contain the statement of the assumptions, such as the maximum time without computing, underlying the plan.

ITS Agency Business Continuity Plan *Chapter 1 – Scope and Limitations* references required assumptions.

(3) Several of the ITS division plans did not contain alternative agency user department procedures to manage their workloads until processing resumes.

ITS is aware of this need and is developing these procedures. Several of the ITS division plans did not provide for the availability of special stock supplies.

(4) Several of the ITS Divisions did not provide for the availability of special stock supplies.

Stock supplies are not required for each system. Each plan will explicitly state the need for stock supplies or say they are not required.

DISTRIBUTION OF AUDIT REPORT

In accordance with G.S. § 147-64.5 and G.S. § 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
Mr. George Bakolia	State Chief Information Officer

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman
Senator Charlie Albertson
Senator Kever M. Clark
Senator Daniel G. Clodfelter
Senator Walter H. Dalton
Senator James Forrester
Senator Linda Garrou
Senator Wilbur P. Gulley
Senator Kay R. Hagan
Senator David W. Hoyle
Senator Ellie Kinnaird
Senator Jeanne H. Lucas
Senator William N. Martin
Senator Stephen M. Metcalf
Senator Eric M. Reeves
Senator Larry Shaw
Senator R. C. Soles, Jr.
Senator David F. Weinstein

Representative James B. Black, Co-Chairman
Representative Richard T. Morgan, Co-Chairman
Representative Martha B. Alexander
Representative E. Nelson Cole
Representative James W. Crawford, Jr.
Representative William T. Culpepper, III
Representative W. Pete Cunningham
Representative Beverly M. Earle
Representative Stanley H. Fox
Representative R. Phillip Haire
Representative Dewey L. Hill
Representative Maggie Jeffus
Representative Edd Nye
Representative William C. Owens, Jr.
Representative Drew P. Saunders
Representative Wilma M. Sherrill
Representative Joe P. Tolson
Representative Thomas E. Wright
Representative Douglas Y. Yongue

DISTRIBUTION OF AUDIT REPORT (CONCLUDED)

Other Legislative Officials

Senator Anthony E. Rand	Majority Leader of the N. C. Senate
Senator Patrick J. Ballantine	Minority Leader of the N. C. Senate
Representative N. Leo Daughtry	N. C. House of Representatives
Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

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

Telephone:	919/807-7500
Facsimile:	919/807-7647
E-Mail:	reports@ncauditor.net

A complete listing of other reports issued by the Office of the North Carolina State Auditor is available for viewing and ordering on our Internet Home Page. To access our information simply enter our URL into the appropriate field in your browser: http://www.osa.state.nc.us