STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

FAYETTEVILLE STATE UNIVERSITY

FAYETTEVILLE, NORTH CAROLINA

FEBRUARY 2002

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

FAYETTEVILLE STATE UNIVERSITY

FAYETTEVILLE, NORTH CAROLINA

FEBRUARY 2002

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Board of Trustees, Fayetteville State University
Dr. Willis B. McLeod, Chancellor, Fayetteville State University

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the Information Technology Services department at Fayetteville State University. 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 University. The scope of our IS general controls audit included general security issues, access controls, program maintenance, physical security, operations procedures, system software, telecommunications, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary that highlights the areas where Fayetteville State University has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at Fayetteville State University 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.
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an information system (IS) audit at Fayetteville State University (FSU) from May 21, 2001 through July 13, 2001. The primary objective of this audit was to evaluate the IS general controls in place during that period. We conducted a follow-up review through February 5, 2002, to determine the updated status of IS controls in place as of that date. 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. There was inappropriate separation of duties for application programmers. An application project development manager was also performing security administration functions. See Audit Finding 1, *Segregation of Duties*.

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for the mainframe system and local area network (LAN). We did not identify any significant weaknesses in access controls over the mainframe and LAN servers during our audit.

Program maintenance primarily involves enhancements or changes needed to existing systems. We did not note any significant weaknesses in program maintenance during our audit.

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

System 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 system software control weaknesses during our audit.

The computer service center's **telecommunications** activities should be operated in a way that protects the security and completeness of data being transmitted. We not identify any significant telecommunications control weaknesses during our audit.

A complete **disaster recovery plan** must be developed, approved by management, and tested for the protection of data and the continuity of the entity's operations. This should enable the University to recover from an extended interruption due to the destruction of the computer center or other University assets. The University has a disaster recovery plan for the computer center. However, we identified some deficiencies in the disaster recovery plan during our audit. See Audit Finding 2, *Incomplete Disaster Recovery Plans*.

[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. This IS audit was designed to ascertain the effectiveness of general controls at Fayetteville State University.

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

METHODOLOGY

This IS audit was performed in accordance with *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. Our methodology included:

- Reviews of policies and procedures.
- Interviews with key administrators and other personnel.
- Examinations of system configurations.
- Tours of the computer facility.
- On-line testing of system controls.
- Reviews of appropriate technical literature.
- Reviews of computer generated reports.
- Use of security evaluation software.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

Fayetteville State University (FSU) is a coeducational, public state-supported institution located in Fayetteville, North Carolina. Founded in 1867, FSU was initially created as an institution for the education of black youth. In 1877 an act of the North Carolina legislature provided for the establishment of a teacher training institution for black North Carolinians. FSU was selected to become the State Colored Normal School and thus becoming the first and oldest state-supported institution of its kind in North Carolina. Fayetteville State University became part of the University of North Carolina (UNC) system of higher education in 1972. It is one of the historically black college/universities within the UNC system. The University provides affordable education to approximately 4,000 undergraduate and graduate students. It is a liberal arts University that offers degrees at the baccalaureate, masters, and doctoral levels.

The mission of Information Technology Services (ITS) is to provide computer access and capabilities for staff, faculty, and students, through Management Information Systems and various college and department computer systems. The University relies heavily upon these systems to meet operational, financial, educational and informational needs.

The ITS department is divided into four areas of support for campus users. The Enterprise System unit provides technical support to the University in its usage of the administrative software components. The User Services unit provides support for academic computing and students. The Network Telecommunications unit is responsible for administering several phases of the campus network. These include network installation and construction, network maintenance and repair, network upgrading, network data/voice/video communications and personal computer hardware recommendations. Network Telecommunications also provides desktop design, engineering, and support for all computers on campus. The Web and Instructional Technology Services unit is responsible for coordinating the training of faculty, staff and their designees in HTML/web page creation and development.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where Fayetteville State University 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, a security organization and resources, policies regarding access to the computer systems and a security education program.

AUDIT FINDING NUMBER 1: SEGREGATION OF DUTIES

Proper segregation of duties is not logically enforced for the staff of the information system services for the University. We found that one individual performs application programming functions as well as security administration for the application system and system software. Improper segregation of duties, whether organizational or logical, may provide an individual the opportunity to circumvent internal control procedures. In addition, poor segregation of duties may allow an individual to commit illegal acts and limit the ability of management to detect that activity.

Recommendation: Management should implement a division of roles and responsibilities that exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are only performing those duties stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained where feasible between security administration and application systems development and maintenance. The small staff size for information system services at the University may not allow management to fully segregate duties. In the absence of proper segregation of duties, management should ensure that compensating controls have been implemented and that the individual's system activities are highly monitored.

Auditee's Response: Fayetteville State University agrees with this finding and has implemented the necessary compensating controls. Also, because of the small staff size, the Information Technology Systems Department is reorganizing to take full advantage of every opportunity to segregate duties.

ACCESS CONTROLS

The access control 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. The University uses the built-in security features of the mainframe operation system to control access. We did not identify any significant weaknesses in access control during our audit.

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 identify any significant weaknesses in program maintenance during our audit.

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. The University's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. We did not identify any significant weaknesses in physical security during our audit.

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 identify any significant weaknesses in the operations procedures of the computer center during our audit.

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. Our audit did not identify any significant weaknesses in system software.

TELECOMMUNICATIONS

Telecommunications is the electronic transmission of any kind of information by radio, wire, fiber optics, microwave, laser, or any other electromagnetic system. It can be evaluated along several lines including the type of system, the geographical organization and the service environment. The computer service center's telecommunications activities should be operated in a way that protects the security and completeness of data being transmitted. The University has implemented controls over the access to telecommunications hardware and the transmission of data. We did not note any significant weaknesses for telecommunications.

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 of the University 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.

AUDIT FINDING 2: INCOMPLETE DISASTER RECOVERY PLANS

The current disaster recovery plans for the user departments are incomplete. These plans and the computer center plan have not been fully tested.

- The computer center has developed a plan for restoring data processing services in the event of a disaster. However, the key user departmental plans do not include alternative processing procedures for operating during the recovery of data processing services. The departmental plans do not have procedures for recovery of data, retaining data during the recovery period, and entering data once data processing services are restored. User departmental plans do not define strategies and procedures for recovery from disasters affecting their department and departmental data processing equipment.

- The current disaster recovery plan for the computer center and the departmental plans have not been tested to ensure that the plans provide sufficient details to allow the University to recover from a disaster.

Recommendation: The University should continue its efforts to develop and implement a comprehensive business continuity plan for the University for data processing services and the user departments. The user departmental plans should include alternative processing procedures for operating during the recovery of data processing services based on the priority and timeframes defined in the computer center's plan. These procedures should include recovery of data, retaining data during the recovery period, and entering data once data processing services is restored. The user departmental plans should include procedures to implement their strategies for recovery from disasters that may affect their department. Once the disaster recovery plans are complete and updated, they should be tested and updated at least annually or when major changes in the data processing environment occur.

Auditee's Response: Management agrees with this finding and will continue its efforts toward developing and implementing a comprehensive business continuity plan for the University's data processing services and user departments.

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
Ms. Molly Corbett Broad	President, The University of North Carolina
Dr. Willis B. McLeod	Chancellor Fayetteville State University

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman	Representative James B. Black, Co-Chairman
Senator Charlie Albertson	Representative Martha B. Alexander
Senator Frank W. Ballance, Jr.	Representative Flossie Boyd-McIntyre
Senator Charles Carter	Representative E. Nelson Cole
Senator Daniel G. Clodfelter	Representative James W. Crawford, Jr.
Senator Walter H. Dalton	Representative William T. Culpepper, III
Senator James Forrester	Representative W. Pete Cunningham
Senator Linda Garrou	Representative Beverly M. Earle
Senator Wilbur P. Gulley	Representative Ruth M. Easterling
Senator Kay R. Hogan	Representative Stanley H. Fox
Senator David W. Hoyle	Representative R. Phillip Haire
Senator Luther H. Jordan, Jr.	Representative Dewey L. Hill
Senator Ellie Kinnaird	Representative Mary L. Jarrell
Senator Howard N. Lee	Representative Maggie Jeffus
Senator Jeanne H. Lucas	Representative Larry T. Justus
Senator R. L. Martin	Representative Edd Nye
Senator William N. martin	Representative Warren C. Oldham
Senator Stephen M. Metcalf	Representative William C. Owens, Jr.
Senator Fountain Odom	Representative E. David Redwine
Senator Aaron W. Plyler	Representative R. Eugene Rogers
Senator Eric Miller Reeves	Representative Drew P. Saunders
Senator Dan Robinson	Representative Wilma M. Sherrill
Senator Larry Shaw	Representative Ronald L. Smith
Senator Robert G. Shaw	Representative Gregg Thompson
Senator R. C. Soles, Jr.	Representative Joe P. Tolson
Senator Ed N. Warren	Representative Russell E. Tucker
Senator David F. Weinstein	Representative Thomas E. Wright
Senator Allen H. Wellons	Representative Douglas Y. Yongue

DISTRIBUTION OF AUDIT REPORT (CONCLUDED)

Other Legislative Officials

Representative Philip A. Baddour, Jr.	Majority Leader of the N.C. House of Representatives
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	Minority Leader of the N.C. House of Representatives
Representative Joe Hackney	N.C. House Speaker Pro-Tem
Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

February 27, 2002

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