STATE OF NORTH CAROLINA

AUDIT OF THE IS GENERAL CONTROLS

AT

NORTH CAROLINA A & T STATE UNIVERSITY

GREENSBORO, NORTH CAROLINA

JANUARY 2001

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE IS GENERAL CONTROLS

AT

NORTH CAROLINA A & T STATE UNIVERSITY

GREENSBORO, NORTH CAROLINA

JANUARY 2001

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Board of Trustees, NC Agricultural and Technical State University
Dr. James C. Renick, Chancellor

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the administrative computer operations at North Carolina Agricultural and Technical State University (N.C. A&T). 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 North Carolina Agricultural and Technical State University has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at North Carolina Agricultural and Technical 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

[This Page Left Blank Intentionally]

EXECUTIVE SUMMARY

We conducted an information system (IS) audit at North Carolina Agricultural and Technical State University from June 14, 2000 through August 11, 2000. 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 identify 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. The University has several individuals with responsibility for administering security functions. In addition to the built-in security features of the mainframe operating system and applications, the university uses a separate software package to control access. 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 did not identify any significant telecommunications control weaknesses during our audit.

A complete **disaster recovery** plan that is tested periodically is necessary to enable the University to recover from an extended business interruption due to the destruction of the computer center or other University assets. The University has disaster recovery plans for the computer center and major user departments. However, we noted some deficiencies in the plans. See Audit Finding 1, *Disaster Recovery Planning,* for further 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. This IS audit was designed to ascertain the effectiveness of general controls at North Carolina Agricultural and Technical 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 computer 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

North Carolina Agricultural and Technical State University (N.C. A&T) is a public, comprehensive, land-grant university located in Greensboro, North Carolina. Founded in 1891, N.C. A&T became part of the University of North Carolina (UNC) system of higher education in 1972. It is the largest historically black college/university within the UNC system.

The Computing and Information Technology department is tasked with providing computing and networking services to the N.C. A&T community – students, faculty, and staff. The department, led by the Associate Vice Chancellor for Academic Affairs, is divided into five areas, each with its own unique mission: Administrative Information Systems, Client Services, Systems and Software, Network and Telecommunications, and Instructional and Research Computing.

- The Administrative Information Systems (AIS) area is responsible for central administrative computing related information management activities for the University. AIS provides technical support for the campus financial, human resources, and student records systems as well as appropriate computing for other administrative functions in academic and administrative units.

- The Client Services area is responsible for determining standards for computer hardware, software, and related equipment. It ensures that such equipment is appropriate for University computing environment. Client Services provides assistance in information delivery, problem management, and technical troubleshooting for recommended hardware and supported software packages for the University and is responsible for managing and supporting classroom and public access computing labs. Additionally, Client Services consults distributed information technology professionals on campus regarding setting up and administering local area networks in their respective departments.

- The System and Software area is responsible for the day-to-day management of the academic computers and software systems. This includes monitoring, ensuring that the equipment is fully functional and responds to a user's needs. This area helps keep the working environment safe, secure and suitable for computing equipment.

- The Network and Telecommunications area supports education and research goals of the University by promoting and providing effective and reliable data, video, and voice connectivity for students, faculty, and staff.

- The Instructional and Research Computing (IRC) area supports a variety of services aimed at improving the quality of instruction and research through the application of technology. These services consist of instructional support, research support, web services, and documentation.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where North Carolina Agricultural and Technical 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.

The University has established a reasonable security program that addresses the general security of information resources. Our audit did not identify any significant weaknesses in general security.

ACCESS CONTROLS

The access control environment consists of access control software and information security policies and procedures. A security administrator 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. In addition, the University has installed a separate software package to monitor system activity of selected users. Appropriate security policies and procedures were in place. 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.

The University has adopted adequate program change procedures. 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 note 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.

The operations procedures at the University are adequate to ensure that computer processing is orderly and well controlled. We did not detect 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.

The systems software at the University is properly approved and maintained by the computer service center. 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 physical 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 1: DISASTER RECOVERY PLANNING

Administrative Information Systems (AIS) has developed a disaster recovery plan for the computer center. Various user departments have developed business continuity plans to provide for continued operations in the event of a disaster affecting the computer center. Our audit found that there is no central administration for the AIS and department plans. There is no documentation that that the user department plans have been reviewed to ensure they are consistent with the AIS plan in their recovery strategies. Without central administration and review of the AIS disaster recovery plan and user department's business continuity plans there is a risk that the plans are not consistent.

There is no documentation that the Chancellor has approved the AIS disaster recovery plan. In addition, most user department's business continuity plans do not have documentation of management approval. Of the six departmental plans we reviewed only one had the signature of senior management indicating that they approved the plan. Without management approval there is no assurance that the plans meet the expectation of management.

We also found that the disaster recovery and business continuity plans are not adequately tested. There have been limited tests performed for the AIS disaster recovery plan. However, these tests have not sufficiently tested the plan's provisions for recovering from a disaster. Also, there is no documentation that the user department's plans have been tested either independently or in conjunction with the AIS plan. Without adequate testing of the disaster recovery and business continuity plans there is no assurance that the plans will provide effective recovery from a disaster.

Recommendation: There should be centralized administration of the AIS disaster recovery and user department's business continuity plans. The University should designate someone with the responsibility to administer the AIS and user department plans. This position should review the plans to ensure that the plans are consistent in their recovery strategies and the University's business continuity objectives. In addition, the AIS and department plans should be compiled into the overall University business continuity plan.

The user department's business continuity plan should be approved by senior management to indicate that the plan is consistent with the University continuity plan objectives. As such, the AIS disaster recovery plan and overall University continuity plan should be signed by the Chancellor to indicate that the plans meets the expectations of management. The user

department plan should be signed by the department head and approved by the appropriate vice-chancellor for the department.

To have an effective disaster recovery and continuity plan, management needs to assess their adequacy on a regular basis. Plans need to be adequately tested to ensure that the plans cover all items needed to restore the business functions as designed. Disaster recovery and business continuity plans should be tested at least annually or when a major change to the environment occurs. The University should also test the department plans in conjunction with the AIS disaster recovery plan to ensure that the plans can effectively restore computer resources and business functions.

Auditee's Response: We concur with the recommendation and have started taking the appropriate steps to review, refine, ensure consistency and test the plans. We will compile all departmental plans into divisional plans, ultimately compiling an overall university business continuity plan that is approved by the appropriate Vice Chancellors and Chancellor.

A testing schedule is being established and observed that will ensure that testing occurs in conjunction with the AIS Disaster Recovery plan.

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 L. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. Marvin K. Dorman, Jr.	State Budget Officer
Mr. Edward Renfrow	State Controller
Ms. Molly C. Broad	President, The University of North Carolina
Dr. James C. Renick	Chancellor, North Carolina A & T 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 Frank W. Ballance, Jr.	Representative Martha B. Alexander
Senator Patrick J. Ballantine	Representative E. Nelson Cole
Senator James Forrester	Representative James W. Crawford, Jr.
Senator Wilbur P. Gulley	Representative W. Pete Cunningham
Senator David W. Hoyle	Representative Ruth M. Easterling
Senator Howard N. Lee	Representative Joe Hackney
Senator Fountain Odom	Representative Martin L. Nesbitt
Senator Aaron W. Plyler	Representative Edd Nye
Senator Anthony E. Rand	Representative William C. Owens, Jr.
Senator Robert G. Shaw	Representative Liston B. Ramsey
Senator Ed N. Warren	Representative E. David Redwine
Senator Allen H. Wellons	Representative Stephen W. Wood
	Representative Thomas E. Wright

Appointees to the Joint Select Committee on Information Technology

Senator Austin M. Allran	Representative Joe P. Tolson
Senator Charles Carter	Representative Russell Edwin Tucker
Senator Daniel G. Clodfelter	Representative William L. Wainwright
Senator Eric Miller Reeves	Representative Trudi Walend
Mr. Dwight Allen	Mr. Rufus Edmisten
Mr. Curtis Clark	Ms. Diana Oblinger
Ms. Darleen Johns	Ms. Janet Smith

Other Legislative Officials

Representative Phillip A. Baddour, Jr.	Majority Leader of the N.C. House of Representatives
Representative N. Leo Daughtry	Minority Leader of the 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**