STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS

NC A&T STATE UNIVERSITY

GREENSBORO, NORTH CAROLINA

APRIL 2005

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

NC A&T STATE UNIVERSITY

GREENSBORO, 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.ncauditor.net

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
The Board of Directors of NC A&T State University
Dr. James C. Renick, Chancellor

Ladies and Gentlemen:

We have completed our information systems (IS) audit of North Carolina Agricultural and Technical State University (NC A&T). This audit was conducted from October 26, 2004, through December 23, 2004. 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 NC A&T. 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. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary and audit results which detail the areas where NC A&T 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 NC A&T 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

PAGE

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at North Carolina Agricultural and Technical State University (NC A&T) from October 26, 2004, through December 23, 2004. 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 found the existing security policies and procedures are not located in a central place and not combined into a single document. These policies and procedures are not complete. *See Audit Finding 1, Existing Security Policies are not Complete and They are in Several Locations.* Also, password policies are not adequate. *See Audit Finding 2, Incomplete and Inconsistent Password Policies.*

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 *North Carolina General Statutes* 147-64.6(c)(18).

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

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 program maintenance during our audit.

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. 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 NC A&T to recover from an extended business interruption due to the destruction of the computer center or other university assets. We did not note any significant weaknesses in disaster recovery during our audit.

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 affect the overall organization and operation of the IS function. This IS audit was designed to ascertain the effectiveness of general controls at NC A&T.

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 NC A&T's computing operations. Other IS general control topics were reviewed as considered necessary.

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 security 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

North Carolina Agricultural and Technical State University (NC A&T) was established in 1891 as Agricultural and Mechanical College for Negroes. The university was temporarily located in Raleigh until it moved to Greensboro in 1893. In 1915, the university's name was changed to Agricultural and Technical College of North Carolina. The Master's program began in 1939. In 1967, the university was designated a regional university and in 1972 it was merged into the University of North Carolina. The Doctoral program began in 1993.

The Division of Information Technology and Telecommunications (ITT) is under the leadership of the CIO who reports to the Chancellor. ITT is responsible for all central computing, and is responsible for both academic and administrative networking for the campus. The following audit results reflect the areas where NC A&T has performed satisfactorily and where recommendations have been made for improvement.

[This Page Left Blank Intentionally]

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. NC A&T State University has established a reasonable security program that addresses the general security of information resources. However, we identified three significant weaknesses in general security during our audit.

AUDIT FINDING 1: EXISTING SECURITY POLICIES ARE NOT COMPLETE AND THEY ARE IN SEVERAL LOCATIONS.

The existing security policies and procedures were located in several places on the university's Intranet. A user is required to look several places for the policies and procedures and one could easily assume a policy and/or procedure does not exist. Security policies and procedures should be located in one central document.

Also, written network security policies and procedures were not located for firewall rules, emergency response to intrusion, review of system intrusion logs, and switch and router configurations. In addition, there are no written policies and procedures governing consultants and contractors. Without written policies and procedures for guidance, management's security intentions may not be conveyed to or followed by employees. Written policies and procedures should be complete.

Recommendation: Although informal policies and procedures seem to exist in practice, the university should formalize the practices by putting them in writing. Management should also consolidate and centralize all security policies and procedures.

Auditee's Response: IT security policies are centralized on the Division of Information Technology and Telecommunications' website. Network security procedures are being revised. The Computing and Networking Usage policy is currently being reviewed for applicable changes as well.

AUDIT FINDING 2: INCOMPLETE AND INCONSISTENT PASSWORD POLICIES

Two written policies and procedures were located for passwords and they recommend different password lengths and expirations. The policy from IT Security and Audits recommends a six-character password length and does not address expiration. The second policy, from AIS, recommends a seven-character password length and refers to a six-month expiration as the time to change a password. Differing policies are confusing, making it difficult for users to know what to follow. The university password composition, length, and expiration policy should be uniform across various platforms and university departments.

Recommendation: The University should consolidate and standardize the password policies, regardless of platform. The university should also change expiration dates to a maximum of 90 days for normal users and 30 days for users with special system privileges.

Auditee's Response: The password policies are consolidated. The password expiration for accounts with high level privileges is 30 days. Otherwise, the password expiration is 45 days. The University is currently deploying enterprise level management tools that allow University resources to be centrally managed which reinforce password management.

ACCESS CONTROLS

The most important information security safeguard that NC A&T 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.

We noted several weaknesses in access controls that if corrected would further enhance network security. 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 did not identify 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. We did not note any significant weaknesses during our review of 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.

NC A&T no longer performs any significant in-house systems development. New application systems are purchased from software vendors and the purchases are guided by procedures and standards for the procurement of software products. 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. NC A&T's 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, many 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.

We did not note any significant weakness in disaster recovery planning during our review.

[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 14, 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