STATE OF NORTH CAROLINA

FOLLOW-UP OF THE AUDIT FINDINGS FROM THE 2004

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

OF THE

NORTH CAROLINA COMMUNITY COLLEGE SYSTEM

RALEIGH, NORTH CAROLINA

JUNE 2005

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

FOLLOW-UP OF THE AUDIT FINDINGS FROM THE 2004

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

OF THE

NORTH CAROLINA COMMUNITY COLLEGE SYSTEMS

RALEIGH, NORTH CAROLINA

JUNE 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
Dr. R. Scott Ralls, President Craven Community College
Dr. Donald L. Reichard, President Johnston Community College
Dr. Brantley Briley, President Lenoir Community College
Dr. Marvin Joyner, President Nash Community College
Dr. F. Marion Altman, Jr., President Pamlico Community College
Dr. William C. Aiken, President Sampson Community College
Dr. Kathleen Matlock, President Southeastern Community College
Dr. Michael R. Taylor, President Stanly Community College
Dr. Randy Parker, President Vance-Granville Community College
Dr. Stephen Scott, President Wake Technical Community College

Ladies and Gentlemen:

We have completed our follow-up review of the audit findings from the June 2004 information system (IS) audit of Craven, Johnston, Lenoir, Nash, Pamlico, Sampson, Southeastern, Stanly, Vance-Granville, and Wake Technical Community Colleges. This review was conducted during the period of March 4, 2005 – May 12, 2005. The review was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

Our follow-up review included determining the status of the findings identified in the five general controls areas: general security, access controls, systems software, physical security, and disaster recovery areas. The overall status of these findings is addressed in the attached report.

This report represents a summary of the general results of our follow-up review. A separate management letter containing the conditions found and recommended corrective action was provided to each individual college at the conclusion of our fieldwork.

We wish to express our appreciation to the staff of the 10 colleges we reviewed for the courtesy, cooperation, and assistance provided to us during this follow-up review.

Respectfully submitted,

Leslie W. Merritt, Jr.

Leslie W. Merritt, Jr., CPA, CFP
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted a follow-up review of the audit findings from the June 2004 information system (IS) audit of Craven, Johnston, Lenoir, Nash, Pamlico, Sampson, Southeastern, Stanly, Vance-Granville, and Wake Technical Community Colleges from March 4, 2005 through May 12, 2005. The primary objective of this follow-up review was to determine the status of the findings found in the June 2004 information system (IS) audit. Our follow-up review focused on the following five areas of general controls: general security, access controls, systems software, physical security, and disaster recovery. This report represents a summary of the general results of our follow-up review. A separate management letter containing the status of the findings were provided to each individual entity at the conclusion of our fieldwork.

General security involves the establishment of a reasonable security program that addresses the general security of information resources. We found that five of 10 Community Colleges reviewed had not resolved all general security findings identified from the June 2004 audit. The other five colleges either made substantial progress or have completely resolved their findings in this area. The absence of good general security policies and management procedures contribute to weaknesses in other general control areas.

Access Control involves the implementation of controls to restrict access to computer resources to only those users who have an authorized need to use or know critical information. The access control environment consists of access control software, operating system and network configurations, and the implementation of information security policies and procedures. We reviewed the access controls to the networks and sensitive student and financial information residing on the critical operating systems for the 10 Community Colleges selected for the follow-up review. We found unresolved access control weaknesses for six out of 10 Community Colleges under review. The other four colleges either made substantial progress or have completely resolved their findings in this area. Due to the sensitive nature of the conditions found, we have conveyed the details of these findings to management in a separate letter pursuant to the provision of *North Carolina General Statute* 147-64.6(c)(18).

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 and appropriately updated. All 10 Community Colleges resolved their system software findings.

Physical security primarily involves the inspection of a 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. Three of 10 colleges selected for review had physical security findings identified in the June 2004 audit. Two of the community colleges reviewed had resolved the findings in this area, and one community college had an unresolved minor finding in this area.

Disaster Recovery involves the creation of a plan to enable the recovery from an extended business interruption due to the destruction of the computer center or other assets. A complete disaster recovery plan that is tested periodically is necessary to ensure prompt resumption of computer systems. Eight of 10 community colleges had findings in disaster recovery during the June 2004 audits. All eight community colleges reviewed had either resolved, or made significant progress in resolving the June 2004 findings in this area.

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 follow-up review was designed to ascertain the effectiveness of general controls at the 10 community colleges selected for review.

SCOPE

General controls govern the operation and management of computer processing activities. The scope of our IS general controls follow-up review was to determine if findings were appropriately resolved for the following five areas: general security issues, access controls, systems software, physical security, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

We reviewed policies and procedures, used questionnaires to interview key administrators and other personnel, developed a program to generate information from the critical operating systems to examine 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 follow-up review of controls. We performed the following tasks.

PHASE 1 – Follow-Up on previous audit findings

In Phase 1, we sent questionnaires to the 10 colleges. We asked them to provide specific information regarding their critical operating systems, their security policies and procedures, their access and network infrastructure, and their disaster recovery plans. This information was reviewed to determine if the college had made substantial progress or whether findings were appropriately resolved.

PHASE 2 – Onsite Review

We then visited the 10 colleges to perform tests that could not be performed offsite to assess whether the previously identified weaknesses were resolved. During this examination, we identified conditions that could allow physical security breaches into the computer centers and evaluated environmental concerns of the computing center.

PHASE 3 – Review of Audit Scripts
In Phase 3, we internally developed a program to review the server configurations of the operating systems and the configuration of critical and sensitive files. We ran this program on each critical system of the community colleges to determine if the server and files were configured to restrict unauthorized access to critical student and financial information.

PHASE 4 – Vulnerability assessment
In Phase 4, we tested for known vulnerabilities, specific to the critical operating system under review, and also tested to see if unauthorized access could be obtained into the critical operating systems. We accomplished this task by using services that come standard with all computers. The overall goal of this phase was to determine if vulnerabilities still existed that would allow user level access to the critical operating systems via the internet or internally.

We conducted our follow-up review 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.

BACKGROUND INFORMATION

The 10 Community Colleges selected for this follow-up review are a part of the North Carolina Community College System (NCCCS), which is comprised of the North Carolina Community College Systems Office located in Raleigh and 58 community colleges located across North Carolina. The mission of the North Carolina Community College System is to open the door to high-quality, accessible educational opportunities that minimize barriers to post-secondary education, maximize student success, and improve the lives and well being of individuals within North Carolina.

The colleges within NCCCS share responsibility for information technology. Each entity has a division that is responsible for information technology for their respective entity. The mission of the information technology divisions is to ensure that information technology is utilized and delivered to the students, faculty, and staff to aid them in accomplishing the overall mission of the North Carolina Community College System.

[This Page Left Blank Intentionally]

AUDIT RESULTS

The following results reflect the areas where the 10 community colleges have either made substantial progress in resolving the findings from the June 2004 Information Systems audit or 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. Our follow-up review identified five community colleges that had unresolved findings from the June 2004 audit. Their policies lacked one or more of the following critical policies and procedures.

- Organization wide security policies;
- User security policies;
- Group assignment and re-assignment policies;
- New accounts and termination policies;
- Monitoring of the critical operating systems and servers;
- How to respond to security threats and incidents;
- How users should securely use the networks;
- Baseline configuration for securing the critical operating system; and
- Risk assessment.

The other five colleges either made substantial progress or have completely resolved their findings in this area.

ACCESS CONTROLS

Access Control involves the implementation of controls to restrict access to computer resources to only those users who have an authorized need to use or know critical information. The access control environment consists of access control software and operating system and network configurations, and the implementation of 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 reviewed the access controls to the critical operating systems. We found several significant weaknesses unresolved from the June 2004 audit in access controls. At the time of our follow-up review, six out of 10 colleges had unresolved weaknesses in this area. The other four colleges either made substantial progress or have completely resolved their findings in this area. Due to the sensitive nature of the conditions found, we have conveyed the details of these findings to management in a separate letter pursuant to the provision of *North Carolina General Statute* 147-64.6(c)(18).

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. At the time of our follow-up review, all 10 colleges had resolved the previous findings identified in this area from the June 2004 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. Three of the 10 colleges selected for review this year were colleges that had findings in physical security. Of the three community colleges which had findings in this area, our follow-up review identified that two of the community colleges reviewed had resolved the findings in this area, and one community college had an unresolved minor finding from the June 2004 audit.

DISASTER RECOVERY

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, many college 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. Two of the 10 community colleges selected did not have findings in the disaster recovery area during the June 2004 IS audits. Of the eight community colleges, which had findings in this area, our follow-up review identified that all eight community colleges reviewed had either resolved , or made significant progress in resolving these findings since the June 2004 audit.

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
Mr. Martin Lancaster	President, North Carolina Community College System

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

President Pro Tempore	Speaker of the House
Senator Marc Basnight, Co-Chair	Representative James B. Black, Co-Chair
Senator Charles W. Albertson	Representative Richard T. Morgan
Senator Patrick J. Ballantine	Representative Martha B. Alexander
Senator Daniel G. Clodfelter	Representative Rex L. Baker
Senator Walter H. Dalton	Representative Bobby H. Barbee, Sr.
Senator Charlie S. Dannelly	Representative Harold J. Brubaker
Senator James Forrester	Representative Debbie A. Clary
Senator Linda Garrou	Representative E. Nelson Cole
Senator Wilbur P. Gulley	Representative James W. Crawford, Jr.
Senator Fletcher L. Hartsell, Jr.	Representative William T. Culpepper, III
Senator David W. Hoyle	Representative W. Pete Cunningham
Senator Ellie Kinnaird	Representative W. Robert Grady
Senator Jeanne H. Lucas	Representative Joe Hackney
Senator Stephen M. Metcalf	Representative Julia C. Howard
Senator Anthony E. Rand	Representative Joe L. Kiser
Senator Eric M. Reeves	Representative Edd Nye
Senator Robert A. Rucho	Representative William C. Owens, Jr.
Senator R. C. Soles, Jr.	Representative Wilma M. Sherrill
Senator Scott Thomas	Representative Thomas E. Wright

Other Legislative Officials

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

Internet: http://www.ncauditor.net

Telephone: 919/807-7500

Facsimile: 919/807-7647