STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

NORTH CAROLINA COMMUNITY COLLEGE SYSTEMS OFFICE

RALEIGH, NORTH CAROLINA

JUNE 2004

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

NORTH CAROLINA COMMUNITY COLLEGE SYSTEM OFFICE

RALEIGH, NORTH CAROLINA

JUNE 2004

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
The Board of Directors of the North Carolina Community College System
Mr. Martin Lancaster, President

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the North Carolina Community College Systems Office. 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 North Carolina Community College Systems Office. The scope of our IS general controls audit included general security, access controls, systems development, program maintenance, systems software, physical security, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary that highlights the areas where the North Carolina Community College Systems Office has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at the North Carolina Community College Systems Office 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

EXECUTIVE SUMMARY

We conducted an information system (IS) audit at the North Carolina Community College Systems Office (NCCCS) from April 4, 2003 - April 30, 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 that the North Carolina Community College Systems Office should adopt formal standards for information technology (IT) to improve the IT Security Policies and Procedures and perform a risk assessment. *See Audit Finding 1, IT Security Policies and Procedures.* We also found that the North Carolina Community College Systems Office has not provided the community college systems administrators with the necessary training needed to properly manage and secure the critical operating systems. *See Audit Finding 2, Security and Maintenance Training.* Furthermore, NCCCS has not developed an overall security program for itself and the 59 community colleges. *See Audit Finding 3, Centralized Security Program.*

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for the North Carolina Community College Systems Office's critical operating systems. We found several weaknesses in access controls. Due to the sensitive nature of the conditions found, 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).

Systems development includes the creation of new application systems or significant changes to existing systems. We found that the NCCCS had used and adopted a formal system development life cycle (SDLC). However, they did not include security specifications for the critical operating system in the requirement definitions phase of the SDLC. *See Audit Finding 4, Security Specification or Baseline for the Critical Operating System.*

Program maintenance primarily involves enhancements or changes needed to existing systems. Because the same procedures are used to patch and upgrade the critical application and the operating system, we indirectly tested program changes to the critical application in our test of system software maintenance.

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 found a significant weakness in systems software maintenance. Due to the sensitive nature of the condition found, we have conveyed this finding to management in a separate letter pursuant to the provision of *North Carolina General Statute* 147-64.6(c)(18).

Physical security primarily involves the inspection of the 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. The North Carolina Community College Systems Office computer center is secure from foreseeable and preventable security and environmental threats. *We did not detect a significant weakness in physical security.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable an agency or college to recover from an extended business interruption due to the destruction of the computer center or other agency's assets. The North Carolina Community College Systems Office has a disaster recovery plan, however, the disaster recovery plan has not been tested. In addition, NCCCS provides the primary backup server for the majority of the 59 community colleges. However, this server is not equipped to handle simultaneous disruptions in service occurring at more than one community college. Furthermore, none of the community colleges relying on this server has performed tests to determine if remote processing can occur from this server. *See Audit Finding 5, Resumption of Computer Systems*.

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 the North Carolina Community College Systems Office.

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, physical security, operations procedures, and disaster recovery which directly affect the North Carolina Community College Systems Office computing operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

We audited 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 audit of 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 North Carolina Community College Systems Office, located in Raleigh, North Carolina, was founded in May 1963. 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 by providing:

- Education, training and retraining for the workforce, including basic skills and literacy education, occupational and pre-baccalaureate programs,
- Support for economic development through services to and in partnership with business and industry, and
- Services to communities and individuals, which improve the quality of life.

Information Services is a section of the Information Resources and Technology division. This section is headed by the Director of Information Services and this position reports to the Associate Vice President for Information Resources and Technology. This section is responsible for administering the computer operations of NCCCS and providing information services to the 59 community colleges. This includes systems for student data, FTE data, staff, equipment, and financial data. This section's responsibilities include:

- Systems development and integration services,
- Computing hardware/software operating systems support,
- Office automation support and training,
- Planning and implementation of a data communications network, and
- Data collection and analysis service.

The mission of Information Resources and Technology is to lead and enable NCCCS to better utilize information technology to deliver service to the students, faculty, and staff.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where the North Carolina Community College Systems Office 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.

AUDIT FINDING 1: IT SECURITY POLICIES AND PROCEDURES

The North Carolina Community College Systems Office (NCCCS) management has not adopted formal information technology (IT) standards to help them address all critical areas of their IT security environment. The following critical policies and procedures were not addressed in their security program:

- NCCCS has no written standards or policies and procedures regarding super user access, the monitoring of critical operating systems and servers, how to respond to security threats, and how users should securely use the networks. Without adding these critical components to a security program, management has not appropriately communicated to the NCCCS staff its overall approach to security and internal control in these aforementioned critical areas.
- NCCCS has not performed a risk assessment of their critical operations. Without a risk assessment, management has not determined which areas are deemed critical and how to prioritize resources and time to ensure that the critical areas remain effective.

NCCCS management should assume full responsibility for developing a framework policy, which establishes the organization's overall approach to security and internal control. The policy should comply with overall business objectives and be aimed at decreasing risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration. In addition, management should ensure that this policy specifies the purpose and objectives, the management structure, the scope within the organization, the assignment of responsibilities for implementation and the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies.

Recommendation: Management at NCCCS needs to develop and adopt a set of formal standards to ensure that all critical general security issues are addressed in their policies and procedures. Also, they should have a mechanism in place to periodically review standards for any new critical areas that should be addressed and include policies and procedures regarding these areas in NCCCS' security policies.

Auditee's Response: We concur with the recommendations and will work to implement them.

AUDIT FINDING 2: SECURITY AND MAINTENANCE TRAINING

NCCCS management has not provided the community college systems administrators with the necessary training needed to properly manage and secure the critical operating systems. Without adequate training, the systems administrators cannot properly maintain and secure the critical operating system, thus allowing for unauthorized access to the critical operating system. Management should identify the training needs of staff and ensure that they are in line with the long-range plan. Management should also establish and maintain procedures for identifying and documenting the training needs of all personnel using the information services. A training curriculum for each group of employees should be established. Based on the identified needs, management should define the target groups, identify and appoint trainers, and organize timely training sessions. Training alternatives should also be investigated (internal or external location, in-house trainers or third-party trainers, etc.). Additionally, all personnel should be trained and educated in system security principles. Senior management should provide an education and training program that includes: ethical conduct of the information services function, security practices to protect against failures affecting availability, confidentiality, integrity, and performance of duties.

Recommendation: NCCCS management should be responsible for coordinating and providing the community college system administrators with the necessary training to enable them to perform effective management and security of the community college's sensitive and critical operating systems.

Auditee's Response: We concur with the recommendation and will work to implement it. NCCCS will be responsible for coordinating community college system administrators with necessary management and security training.

AUDIT FINDING 3: CENTRALIZED SECURITY PROGRAM

NCCCS has not developed an overall security program for its own operations and the 59 community colleges. The lack of a centralized security program to govern NCCCS and the 59 community colleges could potentially lead to lack of consistency and standardization in security configurations and security training for IT personnel across the entire community college system. Based on the technological infrastructure plan, management should define technology norms in order to foster standardization. In addition, senior management should assume full responsibility for developing a framework policy, which establishes the organization's overall approach to security and internal control. The policy should comply with overall business objectives and be aimed at minimization of risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration. Measures should be based on cost-benefit analyses and should be prioritized. In addition senior management should ensure that this high-level security and internal control

policy specifies the purpose and objectives, the management structure, the scope within the organization, the assignment of responsibilities for implementation and the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies.

Recommendation: The NCCCS Information Services division and a committee selected from the 59 community colleges should be given the responsibility for creating a centralized security program. This program will provide specific guidelines and instruction regarding the security of all technology platforms and networks and ensure that maintenance of such platforms is kept current to reduce the risk of preventable vulnerabilities. Furthermore, the communication of such policies should be posted on an intranet or in hard-copy form and should only be accessible by affected IT staff and security personnel from the 59 community colleges and NCCCS.

Auditee's Response: The NCCCS will work collaboratively with the College Institution Information Processing Systems (IIPS) Organization to address this finding.

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. We reviewed the access controls for the North Carolina Community College Systems Office's critical operating systems. We found several significant weaknesses in access controls. Due to the sensitive nature of the conditions found, 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).

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 comprehensive documentation so that the users, operators and programmers each have the information they need to do their jobs. We reviewed the phases of system development/acquisition cycles for NCCCS and found that although a systems development life cycle (SDLC) was used and is in place, no security requirements were defined for the critical operating system in the requirements definition phase of the SDLC.

AUDIT FINDING 4: BASELINE FOR THE CRITICAL OPERATING SYSTEM

NCCCS is responsible for providing hardware and software specifications for all equipment required to run system wide applications. Specifications and baselines are normally submitted in the requirements definition phase of the systems development life cycle (SDLC). We found that NCCCS did not include in its requirements definition for new critical applications security specifications or a baseline for the operating system used to host the critical application. As a result, NCCCS and the majority of the 59 community colleges may be running the new critical applications on operating systems that are not secure. The SDLC methodology should require that the solution's functional and operational requirements be specified including performance, safety, reliability, compatibility, security and legislation.

Recommendation: NCCCS should ensure that security specifications are included in the requirement definitions phase for the applications, operating systems and any other equipment supporting the new proposed application.

Auditee's Response: We concur with the recommendation and will work to implement it. NCCCS will ensure that the security specifications are included in the requirement definitions phase for all applications.

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. Because the same procedures are used to patch and upgrade the critical application and the operating system, we indirectly tested program changes to the critical application in our test of system software 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. We found a significant weakness in systems software maintenance. Due to the sensitive nature of the condition found, we have conveyed this finding to management in a separate letter pursuant to the provision of *North Carolina General Statute* 147-64.6(c)(18).

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 North Carolina Community College Systems Office computer center is secure from foreseeable and preventable security and environmental threats. *We did not detect a significant weakness in physical security.*

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 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. Our audit identified one significant weakness in disaster recovery.

AUDIT FINDING 5: RESUMPTION OF COMPUTER SYSTEMS

NCCCS has not performed annual testing of its disaster recovery plan as required by disaster recovery best practice standards. In addition, NCCCS purchased a server to act as the primary disaster recovery back-up server for the majority of the 59 community colleges. However, this NCCCS server is not equipped to handle simultaneous disruptions in service occurring at more than one community college. None of the community colleges have tested this server to determine if it can handle remote processing of their critical operations until computer services are restored. Only one community college has tested this server to determine that the back-up tapes would load successfully on the server. In the event of simultaneous disruptions in service at the community colleges, NCCCS' current disaster recovery server would not be able to support the prompt recovery of the community colleges critical systems. Procedures should require that the disaster recovery plans and servers be maintained and tested periodically to ensure that they are operable and they can handle the workload if a disaster occurs.

Recommendation: NCCCS should test its disaster recovery plan on a yearly basis. In addition, NCCCS should encourage and inform the community colleges to only rely on the NCCCS disaster recovery server as a secondary option to recovery from a disruption because the one disaster recovery server may not be equipped to handle the workload of simultaneous disruptions occurring at more than one college. In addition, NCCCS should ensure that each College test remote processing capabilities from this server to their respective campuses to ensure that the server will operate as intended if ever used in any disaster recovery efforts.

Auditee's Response: We concur with the recommendation and will work to implement it.

[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
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, Co-Chair
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