STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

UNIVERSITY OF NORTH CAROLINA AT PEMBROKE

APRIL 2007

OFFICE OF THE STATE AUDITOR

LESLIE MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

UNIVERSITY OF NORTH CAROLINA AT PEMBROKE

APRIL 2007

STATE OF NORTH CAROLINA

Office of the State Auditor

Leslie 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.osa.state.nc.us

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Allen C. Meadors, Ph.D., FACHE, Chancellor

Ladies and Gentlemen:

We have completed our audit of University of North Carolina at Pembroke (UNCP). This audit was conducted during the period from November 6, 2006, through December 6, 2006. 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 UNCP. The scope of our IS general controls audit included general security, access controls, program maintenance, systems software, systems development, physical security, 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 UNCP 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 UNCP 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 Merritt, Jr., CPA, CFP
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an Information Systems (IS) audit at the University of North Carolina at Pembroke (UNCP) from November 6, 2006, through December 6, 2006. 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. UNCP has established a reasonable security program that addresses the general security of information resources. However, we identified some deficiencies in its security program that address all critical areas of its IT security environment. See Audit Finding 1, *Security Program Weaknesses*.

The **access control** environment consists of access control software and information security policies and procedures. We found 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 G.S. 147-64.6(c)(18).

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

Systems Development includes the creation of new application systems or significant changes to existing systems. We did not identify any significant weaknesses in systems development during our audit.

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 identify any significant weaknesses in the physical security.

A complete **disaster recovery** plan that is tested periodically is necessary to enable UNCP to recover from an extended business interruption due to the destruction of the computer center or other UNCP assets. Our audit did not note any significant weaknesses in disaster recovery.

[This Page Left Blank Intentionally]

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the *North Carolina General Statutes* 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 effect the overall organization and operation of the IS function. This IS audit was designed to ascertain the effectiveness of general controls at UNCP.

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, and disaster recovery which directly affect UNCP'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 application 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

The University of North Carolina at Pembroke is a comprehensive University committed to academic excellence in a balanced program of teaching, research, and service. It offers a broad range of degrees and nationally accredited professional programs at the bachelor's and master's levels. Combining the opportunities available in a large university with the personal attention characteristic of a small college, the University provides an intellectually challenging environment created by a faculty dedicated to effective teaching, interaction with students, and scholarship. Graduates are academically and personally prepared for rewarding careers, postgraduate education, and community leadership.

Founded in 1887 to educate American Indians, the University now serves a student body reflective of the rich cultural diversity of American society. As it stimulates interaction within and among its cultural groups, the University enables its students to become informed, principled, and tolerant citizens with a global perspective.

The central information technology unit at UNCP is University Computing and Information Services (UCIS). The primary function of the office is to handle all aspects of computing and telecommunications for the University and provide the technical infrastructure and support needed to meet the mission of the University. It is composed of three support service units. These are Network and System Administration, Client Services, and Applications Development. Each of these units is led by a Director that reports to the Executive Director of University Computing and Chief Technology Officer. The Executive Director also manages the Enterprise System Database Administrator and is also the Manager of the Interactive Video Facility. Together, these units provide support and maintain the technology infrastructure at UNCP.

- The Network and System Administration (NSA) unit is responsible for managing the campus network and most central servers. NSA staff also manages Banner security under the direction of the Executive Director and may support the Enterprise System/Database Administrator.

- The Client Services unit is responsible for desktop support, lab support, training for general desktop applications, and limited academic support. The Enterprise System/Database Administrator is responsible for managing server operating systems and the server-level aspects of Oracle.

- The Applications Development (AD) unit is responsible for supporting administrative applications such as Banner and Plus. AD staff also manages academic applications such as the Blackboard Course Management System.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where UNCP 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. UNCP has established a reasonable security program that addresses the general security of information resources. *However, we noted one significant weakness in general security during our audit.*

Audit Finding 1: SECURITY PROGRAM WEAKNESSES

UNCP has established a reasonable security program that addresses the general security of information resources. However, the following security issues were not addressed in its security program:

- The University's Security Policies are currently in draft format. As a result, management's security intentions may not be followed and security may be implemented in an inconsistent manner.
- There is no formally written baseline configuration for securing the University's critical operating system. As a result, security may be implemented in an inconsistent and insecure manner.
- No risk assessment has been performed for the University's critical operations. As a result, critical risks may not be identified and addressed.

Recommendation: Management should develop and adopt a set of formal standards to ensure that all critical security issues are addressed in its policies and procedures. Also, it should have a mechanism in place to periodically review these standards for any new critical areas that should be addressed and include policies and procedures regarding these areas in its security policies. Management should also develop a baseline configuration for securing the University's network and computer devices. The University should also perform a risk assessment.

Auditee's Response: We agree with the finding. Corrective action is underway.

ACCESS CONTROLS

The most important information security safeguard that UNCP has is its access controls. The access controls environment consists of UNCP's 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 a number of weaknesses in access controls. 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 G.S. 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. *We did not note 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. *Our audit did not identify any significant weaknesses in system 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.

UNCP 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. *UNCP's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity.*

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, UNCP would grind to a halt. To reduce this risk, computer service centers develop business continuity plans. Business continuity procedures should be tested periodically to ensure the recoverability of the data center. *Our audit did not identify any significant weakness in disaster recovery planning.*

[This Page Left Blank Intentionally]

ORDERING INFORMATION

Audit reports issued by the Office of the State Auditor can be obtained from the web site at www.ncauditor.net. Also, parties may register on the web site to receive automatic email notification whenever reports of interest are issued. Otherwise, copies of audit reports 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