



# **STATE OF NORTH CAROLINA**

## **SPECIAL REVIEW**

**NORTH CAROLINA STATE UNIVERSITY  
OFFICE OF INFORMATION TECHNOLOGY  
RALEIGH, NORTH CAROLINA**

**JUNE 2008**

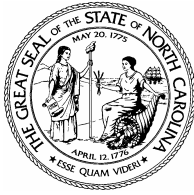
**OFFICE OF THE STATE AUDITOR  
LESLIE W. MERRITT, JR., CPA, CFP  
STATE AUDITOR**

**SPECIAL REVIEW**

**NORTH CAROLINA STATE UNIVERSITY  
OFFICE OF INFORMATION TECHNOLOGY**

**RALEIGH, NORTH CAROLINA**

**JUNE 2008**



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

STATE OF NORTH CAROLINA  
Office of the 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  
Dr. James L. Oblinger, Chancellor, North Carolina State University  
Mr. Jim W. Phillips, Jr., Chair, Board of Governors, The University of North Carolina  
Mr. Erskine Bowles, President, The University of North Carolina  
Mr. D. McQueen Campbell, III, Chair, Board of Trustees, North Carolina State  
University  
Members of the North Carolina General Assembly

Ladies and Gentlemen:

Pursuant to North Carolina General Statute § 147-64.6(c)(16), we have completed our special review of North Carolina State University. The results of our review, along with recommendations for corrective action, are contained in this report.

Copies of this report have been provided to the Governor, the Attorney General, and other appropriate officials in accordance with North Carolina General Statute § 147-64.6(c)(12) which requires the State Auditor to provide written notice of apparent instances of violations of penal statutes or apparent instances of malfeasance, misfeasance, or nonfeasance by an officer or employee.

Respectfully submitted,

*Leslie W. Merritt, Jr.*

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

June 17, 2008

## TABLE OF CONTENTS

---

	PAGE
INTRODUCTION.....	1
BACKGROUND.....	3
FINDINGS AND RECOMMENDATIONS.....	5
RESPONSE FROM NORTH CAROLINA STATE UNIVERSITY.....	11
DISTRIBUTION OF AUDIT REPORT.....	17

## INTRODUCTION

---

The Office of the State Auditor began an investigation into allegations regarding inappropriate use of computers at North Carolina Central University. During the course of that review, auditors became aware of a connection between an information technology employee at North Carolina State University and the employees at North Carolina Central University. Allegedly, the North Carolina State University (University) employee allowed individuals external to the organization to access the university computer network to share music files. In addition, we received allegations that the employee was involved in illegal downloading and distribution of copyrighted materials.

Our special review of these allegations included the following procedures:

- Interviews with current and former employees of North Carolina State University as well as individuals external to the University.
- Examination of relevant documents and records including forensic analysis of computer data storage devices and network drives.
- Review of policies and procedures and federal and State regulations including the North Carolina General Statutes and North Carolina Administrative Code.

This report presents the results of our special review. The review was conducted pursuant to North Carolina General Statute §147-64.6(c)(16) rather than a financial statement audit or review. The Office of the State Auditor also performs a financial statement audit of the University on an annual basis.

[ This Page Left Blank Intentionally ]

## **BACKGROUND**

---

North Carolina State University (University) was established as a land-grant institution in 1887. The University is the largest four-year institution in North Carolina with enrollment exceeding 31,000 students. The University is one of 16 constituent institutions in the University of North Carolina system. The University offers degrees in over 100 fields in both undergraduate and graduate programs of study. A Board of Trustees oversees its operations at the institutional level. The University's Chancellor and other senior administrators manage the day-to-day operations.

In November 2007, the University consolidated its information technology functions by combining the Resource Management and Information Systems and Information Technology Division to create the Office of Information Technology (OIT). The OIT provides central administrative and academic information technology services to students, faculty, staff, and administrators.

While the consolidation was in transition, the Office of Information Technology was led jointly by an Associate Vice Chancellor and an Assistant Provost. In May 2008, the University hired a Chief Information Officer to lead the organization. The Chief Information Officer will officially begin duties on September 1, 2008 and will report directly to the Chancellor. The OIT is divided into seven functional areas with a director overseeing each section.

[ This Page Left Blank Intentionally ]



## FINDINGS AND RECOMMENDATIONS

---

### **1. THE OPERATIONS AND SYSTEMS ANALYST MISUSED THE UNIVERSITY NETWORK AND COMPUTERS BY DOWNLOADING MOVIES, MUSIC, GAMES, SOFTWARE, AND PORNOGRAPHY.**

Our review of computers and disk drives assigned to the Operations and Systems Analyst indicated inappropriate use of University networks and computers. We found numerous files of inappropriate material including “ripped”<sup>1</sup> versions of films, music, software, and video games. In addition, our analysis discovered pornographic and violent materials. Some of these files were buried deep within sub-folders indicating an apparent attempt to conceal the content from detection.

The Operations and Systems Analyst admitted inappropriate use of University-issued computers. At first, he acknowledged downloading movies, music, and software for personal use but denied accessing pornography. The Operations and Systems Analyst told us he accessed these copyrighted materials through newsgroups such as “Merlin’s Portal” on the Internet. He said users pay a monthly fee to join the group and members offer items for download for free. Upon further questioning, the Operations and Systems Analyst admitted to downloading pornography to his laptop. (See Finding #3)

We obtained an e-mail indicating the Operations and Systems Analyst maintained a “stockpile” of movies. When asked about this e-mail, he estimated downloading as many as “two to four per week.” The Operations and Systems Analyst told us he sometimes accessed this data after 5:00PM and at other times would start his computer each morning and download materials while he performed other duties. He said his downloading activities began in 2005 while employed at North Carolina Central University and continued when he became a North Carolina State University employee in March 2006. Using estimates he provided, the Operations and Systems Analyst may have downloaded 400 movies since becoming an NC State employee.

The Operations and Systems Analyst said he used the University network because the larger bandwidth provided faster downloads as compared to the dial-up connection at his home. Using the University network, he would download the items to a University computer, transfer them to a personally-owned external hard drive, and then transfer the files to compact discs (CD’s) or digital video discs (DVD’s) at home. The Operations and Systems Analyst said these items were for personal use and stressed that he did not sell any of these items.

The Operations and Systems Analyst conceded that the downloaded materials were “unauthorized,” “illegal,” and “inappropriate” use of state computers. In addition, he admitted a risk existed that these files could have viruses attached to them. He attempted to minimize that risk saying that the sites are “self-policing” to remove users who offer contaminated files.

---

<sup>1</sup> A “ripped” file is one in which encryption that prevents duplication has been removed by a software program.

## **FINDINGS AND RECOMMENDATIONS (CONTINUED)**

---

The Operations and Systems Analyst is responsible for maintaining several servers for the University including the “All Campus Card Service” server and other servers dedicated to specific departments such as Transportation and Facilities. His duties included server administration and support. As such, the Operations and Systems Analyst has an even higher responsibility to protect the University network from unauthorized use. Further, his inappropriate use of the University network and computers violated University computer use policies which can be classified as “unacceptable personal conduct.”

### **RECOMMENDATION**

The University should take strong disciplinary action against the Operations and Systems Analyst. In addition, the University should review all items for which he had access to determine the extent of his inappropriate use. Further, this review should seek to determine whether the University’s computer system and network security was harmed.

## **2. THE OPERATIONS AND SYSTEMS ANALYST MAY HAVE VIOLATED FEDERAL COPYRIGHT LAWS BY DISTRIBUTING COPYRIGHTED MATERIALS.**

The Operations and Systems Analyst told us he downloaded movies, music, games, and software for personal use. In addition, he admitted that he provided copies of these items to friends and business associates. Further, he acknowledged using software programs to break encryption files used to protect copyrights.

The Operations and Systems Analyst said he had given copies of movies and music to individuals within the Office of Information Technology at NC State University and the Information Technology Services Department at NC Central University. He denied selling any of these materials but instead said they were given as free copies. The Operations and Systems Analyst acknowledged that it was “illegal” to obtain and distribute these items.

Federal copyright laws contained in Title 17 of the United States Code prohibit infringement of copyrights and distribution of copyrighted materials. Violators of these copyright laws may be subject to both civil and criminal penalties.

In addition, the University’s Copyright Infringement Policy states “*copying, distributing, downloading, and uploading information on the Internet may infringe the copyright for that information....Violations of copyright law that occur on, or over the university’s networks or other computer resources may create liability for the university as well as the computer user.*”

Note: This finding will be referred to the U.S. Attorney’s Office, Eastern District, the District Attorney for North Carolina Judicial District 10, and the North Carolina State Bureau of Investigation.

### RECOMMENDATION

The University should take strong disciplinary action against the Operations and Systems Analyst. The University's copyright administrators should work in conjunction with law enforcement personnel to determine whether federal copyright laws were violated. Further, the University should perform periodic forensic reviews of its data networks to determine whether unauthorized copyrighted materials are being accessed and distributed.

### **3. THE OPERATIONS AND SYSTEMS ANALYST INTENTIONALLY DELETED ALL INFORMATION FROM HIS UNIVERSITY-OWNED LAPTOP COMPUTER TO CONCEAL INAPPROPRIATE USE.**

When performing our forensic analysis of multiple computers assigned to the Operations and Systems Analyst, we were unable to obtain any data from a laptop computer. The hard drive was unreadable which appeared to indicate the entire hard drive to the laptop was erased.

The Operations and Systems Analyst was placed on investigatory leave on March 28, 2008. The laptop in question was in his possession at his home until he provided it to the University two days later. When returning it to the University, he said the laptop was damaged and unusable.

The Operations and Systems Analyst told us the laptop was damaged when his daughter accidentally knocked it off the bed. At first, he claimed that damage rendered the laptop inoperable. After we told him we did not see any damage to the laptop, he admitted the only damage was to the power supply. Then, the Operations and Systems Analyst admitted the laptop continued to work until the battery expired. Further, we told him the inability to obtain any data from the laptop was inconsistent with damage resulting from a dropped laptop. He admitted he used "KillDisk," a software program that removes all data from a hard drive and prevents the recovery of deleted files, to delete data from the laptop. The Operations and Systems Analyst said he destroyed the data because he did not know what might be contained on the computer. After further inquiry, he admitted the laptop contained downloaded movies, music, software, and "some pornography."

In addition, we discovered an e-mail the Operations and Systems Analyst sent to other employees within the Office of Information Technology on March 6, 2008 alerting them to our review. The e-mail states:

*"Just in case you might have any questionable files on your PC's HD or on a share, I heard from a VERY reliable source that the state is running some scanning software with forensic capabilities for discoveries. So, delete it well..."*

## FINDINGS AND RECOMMENDATIONS (CONTINUED)

---

The Operations and Systems Analyst told us he was given “a heads up” by an individual under investigation at another university and wanted to extend that notification to his co-workers.

North Carolina General Statute § 14-455 states “*it is unlawful to willfully and without authorization alter, damage, or destroy a government computer. A violation of this subsection is a Class F felony.*” Further, North Carolina General Statute § 147-64.7A details that anyone who attempts to “*hinder or obstruct the State Auditor or the State Auditor’s designated representative in the performance of their duties, shall be guilty of a Class 2 misdemeanor.*” Intentionally erasing all contents of the laptop hard drive may violate these statutes.

Note: This finding will be referred to the U.S. Attorney’s Office, Eastern District, the District Attorney for North Carolina Judicial District 10, and the North Carolina State Bureau of Investigation.

### RECOMMENDATION

The University should take strong disciplinary action against the Operations and Systems Analyst. In addition, the University should reiterate to its employees the importance of protecting all government data. Finally, University management should determine whether other employees deleted any information in an effort to conceal their misuse of computers.

#### **4. THE OPERATIONS AND SYSTEMS ANALYST PROVIDED ACCESS TO A UNIVERSITY SERVER TO ALLOW A FRIEND TO DOWNLOAD MUSIC FILES.**

We obtained an e-mail dated February 6, 2008 indicating that the Operations and Systems Analyst “set up a share” that allowed a former associate, who works in the Information Technology Services Department at North Carolina Central University, to access the NC State network. In a February 20, 2008 e-mail, the Operations and Systems Analyst told the NC Central employee that “the vendor came in yesterday morning to install the app [application] on the server you were using and I had to drop the share.” In response, the NC Central employee asked the Operations and Systems Analyst to “setup another share” and the Operations and System Analyst agreed.

The Operations and Systems Analyst told us the NC Central employee was vacationing in Atlanta and wanted to download karaoke files to entertain his children. The Operations and Systems Analyst reasoned that he had an unutilized server available and that he believed he could trust his former associate. The Operations and Systems Analyst transferred files to the server and provided his username and password to his former associate to enable the access. The NC Central employee confirmed he accessed the NC State network through the share.

## **FINDINGS AND RECOMMENDATIONS (CONCLUDED)**

---

The Operations and Systems Analyst admitted it was “very poor judgment on my part.” Since the user was a friend, he did not consider it a security risk. However, the Operations and Systems Analyst said providing access and his password were violations of the University’s Computer Use Policy.

In addition, North Carolina General Statute § 14-454.1 outlines unlawful access to government computers as follows:

*“Any person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any government computer for any purpose other than those set forth in subsection (a) of this section is guilty of a Class H felony.”*

Note: This finding will be referred to the U.S. Attorney’s Office, Eastern District, the District Attorney for North Carolina Judicial District 10, and the North Carolina State Bureau of Investigation.

### **RECOMMENDATION**

The University should take strong disciplinary action against the Operations and Systems Analyst. In addition, the University should provide additional training to all Office of Information Technology employees that stresses the need to ensure network security.

[ This Page Left Blank Intentionally ]

# RESPONSE FROM NORTH CAROLINA STATE UNIVERSITY

North Carolina State University is a land-grant university and a constituent institution of The University of North Carolina

**Office of the Chancellor**  
Box 7001 / A Holladay Hall  
Raleigh, North Carolina 27695-7001

**NC STATE UNIVERSITY**

919.515.2191 (phone)  
919.831.3545 (fax)

June 11, 2008

Leslie W. Merritt, Jr., CPA, CFE  
State Auditor  
2 So. Salisbury Street  
20601 Mail Service Center  
Raleigh, NC 27699-0601

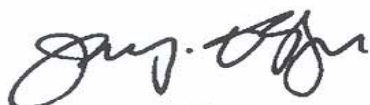
Dear Mr. Merritt:

Thank you for the May 28, 2008 draft report on your special review of allegations concerning inappropriate use of computers by an employee at North Carolina State University (NC State). The NC State Office of Information Technology, Legal Affairs, Human Resources, and Internal Audit have reviewed the report and recommendations. Internal Audit worked closely with your investigators and IT forensic staff throughout this investigation and ensured that corrective actions began immediately on all issues as they were uncovered. Please find our responses to your recommendations attached to this letter.

We would like to express our appreciation of the professionalism with which your auditors conducted this investigation and their very collaborative and productive approach.

Please contact Cecile Hinson, Director of Internal Audit, at (919) 515-8862 if you have any questions or require additional information.

Sincerely,



James L. Oblinger  
Chancellor

Enclosure: NC State Response to May 28, 2008 Special Review Draft Report

cc: Mr. Samuel Averitt, Vice Provost for Information Technology  
Ms. Barbara Carroll, Associate Vice Chancellor for Human Resources  
Ms. Cecile Hinson, Director of Internal Audit  
Mr. Steve Keto, Associate Vice Chancellor for Resource and Information Systems  
Ms. Mary Elizabeth Kurz, Vice Chancellor and General Counsel  
Mr. Charles Leffler, Vice Chancellor for Finance and Business  
Dr. Larry Nielsen, Provost and Executive Vice Chancellor

**North Carolina State University  
Response to May 28, 2008 Special Review Draft Report  
of the North Carolina Office of the State Auditor**

**State Auditor Finding #1**

**Issue:**

The Operations and Systems Analyst misused the [NC] State [University] network and computers by downloading movies, music, games, software, and pornography.

**Recommendation:**

The University should take strong disciplinary action against the Operations and Systems Analyst. In addition, the University should review all items for which he had access to determine the extent of his inappropriate use. Further, this review should seek to determine whether the University's computer system and network security was harmed.

**NC State University Response to Finding #1**

NC State management placed the Operations and Systems Analyst on Investigative Leave when supporting evidence for the allegations was presented to Internal Audit by UNC General Administration and the Office of the State Auditor. The employee has since terminated employment with the University.

Upon receipt of the allegations, the employee's access to all University systems was disabled. Internal Audit and the Office of Information Technology (OIT) Security and Compliance Unit (OIT Security) secured and inventoried the employee's office and equipment. All equipment was turned over to the State Auditors for forensic review. Additional servers that the employee had access to are currently being reviewed by OIT Security for potentially illegal data. To date, no further evidence of potentially illegal data has been identified.

In addition, OIT Security immediately began investigating the potential impact of the employee's activities to the NC State IT environment. This investigation is currently in the final stages. No negative impacts in the form of threats, vulnerabilities, or weaknesses to our environment have been uncovered to date. Internal Audit has consulted with OIT Security during their investigation and will be provided with a final report upon its completion. In addition, Internal Audit will follow-up on the results and conclusions of that report to ensure any necessary corrective actions have been fully and successfully implemented.



## **State Auditor Finding #2**

### **Issue:**

The Operations and Systems Analyst may have violated Federal copyright laws by distributing copyrighted materials.

### **Recommendation:**

The University should take strong disciplinary action against the Operations and Systems Analyst. The University's copyright administrators should work in conjunctions with law enforcement personnel to determine whether federal copyright laws were violated. Further, the University should perform periodic forensic reviews of its data networks to determine whether unauthorized copyrighted materials are being accessed and distributed.

## **NC State University Response to Finding #2**

NC State management placed the Operations and Systems Analyst on Investigative Leave when supporting evidence for the allegations was presented to Internal Audit by UNC General Administration and the Office of the State Auditor. The employee has since terminated employment with the University.

NC State has and will continue to preserve evidence about this matter pending a determination by the US Attorney's Office that there were criminal copyright violations. We will respond to information requests and cooperate fully with any law enforcement investigations.

Performance of "periodic forensic reviews of the University's data networks" is not feasible due to the size and complexity of the IT environment. There is no practical way to distinguish copyright and non-copyright material stored on every server, computer, or traveling across the network. Similarly, there is no practical way to distinguish between copyrighted material downloaded or stored for legal academic or administrative purposes from potentially illegal material. Finally, downloading activities similar to those performed by the Operations and System Analyst would not be easily distinguishable from legitimate downloads since there was no evidence uncovered by the State Auditors or OIT Security that the employee utilized Peer-to-Peer file-sharing software.

However, OIT Security is examining the set of systems supported by Hosted Systems Department employees to ensure that none of them have been or are engaging in similar downloading or sharing of copyrighted materials. In addition, Internal Audit interviewed each employee in the Hosted Systems Department as to their potential involvement in this matter and reiterated to them their responsibility to abide by University Policies, Rules, and Regulations and comply with Federal and State laws.

NC State has Policies, Rules, and Regulations in place that prohibit illegally downloading copyrighted material. Furthermore, when copyright holders notify the University's copyright administrators of a violation coming from a campus system, the activity is disabled and/or the system is disconnected from the network and appropriate disciplinary action is taken against the offender, if identifiable. The University also reserves the right to turn off any network port evidencing abnormally large spikes in bandwidth usage.

### **State Auditor Finding #3**

**Issue:**

The Operations and Systems Analyst intentionally deleted all information from his University-owned laptop computer to conceal inappropriate use.

**Recommendation:**

The University should take strong disciplinary action against the Operations and Systems Analyst. In addition, the University should reiterate to its employees the importance of protecting all government data. Finally, University management should determine whether other employees deleted any information in an effort to conceal their misuse of computers.

### **NC State University Response to Finding #3**

NC State management placed the Operations and Systems Analyst on Investigative Leave when supporting evidence for the allegations was presented to Internal Audit by UNC General Administration and the Office of the State Auditor. The employee has since terminated employment with the University.

OIT management is in the process of developing a training procedure for its staff that will review pertinent policies and ethical obligations on a regular basis. Additionally, Internal Audit interviewed each employee in the Hosted Systems Department as to their potential involvement in this matter and reiterated to them their responsibility to abide by University Policies, Rules, and Regulations and comply with Federal and State laws.

OIT Security is analyzing the University computers assigned to the staff that received the March 6, 2008 email message warning of the OSA investigation for evidence of deletion of information to conceal misuse. Results of those analyses will be included in the OIT Security report to be submitted to Internal Audit. Internal Audit will follow-up on the results and conclusions of that report to ensure any necessary corrective actions have been fully and successfully implemented.

#### **State Auditor Finding #4**

**Issue:**

The Operations and Systems Analyst provided access to a University server to allow a friend to download music files.

**Recommendation:**

The University should take strong disciplinary action against the Operations and Systems Analyst. In addition, the University should provide additional training to all Office of Information Technology employees that stresses the need to ensure network security.

#### **NC State University Response to Finding #4**

NC State management placed the Operations and Systems Analyst on Investigative Leave when supporting evidence for the allegations was presented to Internal Audit by UNC General Administration and the Office of the State Auditor. The employee has since terminated employment with the University.

OIT management is in the process of developing a training procedure for its staff that will review pertinent policies and ethical obligations on a regular basis.

OIT is also in the process of updating the NC State Computer Use Policy. When completed and approved, this updated policy and the NC State Human Resources' illegal file-sharing disciplinary policy will be shared with the campus at large via:

- targeted email
- presentations by the NC State Digital Millennium Copyright Act Copyright Agent at appropriate University committees such as the University Information Technology Committee and the OIT Management Team
- University-wide publications such as new student/employee orientation material, University Bulletin

[ This Page Left Blank Intentionally ]

## 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