

**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 provided 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