

Minutes of the September 11, 2008 Meeting
of the Board of Governors' Audit Committee

The Audit Committee met in the Executive Conference Room of the UNC General Administration-Spangler Center in Chapel Hill, North Carolina on Thursday, June 11, 2008, at 4:30 p.m.

Members in attendance were Mr. Brent Barringer, Mr. Frank Daniels, Jr., Mr. Charles Hayes, Mr. G. Leroy Lail, Mr. Charles H. Mercer, Jr., and Dr. Gladys Ashe Robinson. Necessarily absent were Mrs. Clarice Cato Goodyear and Mr. Jim Phillips. Other Board of Governors members attending the meeting were Mr. Ray S. Farris, Mr. Marshall B. Pitts, Jr., and Mr. William Smith. President Erskine B. Bowles; Chief of Staff Jeffrey R. Davies; Vice Presidents Laura Luger, Dr. Harold Martin, Robert O. Nelson, and Joni Worthington; Associate Vice Presidents David King and James O. Smith; Chancellor Stanley Battle (NCA&T), Chancellor Charlie Nelms (NCCU), Chancellor Kenneth Peacock (ASU); Dr. Alan Robertson, Vice Chancellor for Financial Affairs (NCCU), Ms. Yolanda Banks-Deaver, Assistant Vice Chancellor for Administration and Finance (NCCU), Chief of Staff Ms. Susan Hester (NCCU); Ms. AJ Desai and Mr. Keith Fuez (Ernst & Young), and Ms. Gwen Canady were also in attendance.

Chair Daniels welcomed everyone to the meeting and recognized the new members of the Audit Committee.

President Bowles reported on the status of the steps to resolve the unapproved North Carolina Central University's New Birth College Program at New Birth Missionary Baptist Church in Lithonia, GA. He also gave appreciation to Chancellor Nelms for his eagerness to resolve this issue.

The New Birth Program was not approved by North Carolina Central University's Board of Trustees, UNC General Administration, or the Southern Association of Colleges and Schools (SACS). Both NCCU and UNCGA were in the process of examining the creation and operations of the program. There were four basic areas being reviewed:

1. Students
 - 125 affected students
 - 25 degrees awarded
 - 38 students registered for Fall 2008
2. SACS Follow-up
 - Proposal submitted by September 19, 2008
3. Federal Financial Aid
 - Discussions with the U.S. Department of Education concerning eligibility for funding and the potential repayment of funds

4. Examine all programs and take measures to prevent similar incidents from happening again

On the motion of Chair Daniels, seconded by Mr. Barringer, the Committee went into Closed Session to prevent the disclosure of privileged information under N.C.G.S. 147-64.6(c)(18) and N.C.G.S. 116-40.7(c) of the North Carolina General Statutes or regulations.

CLOSED SESSION

The Chair then recognized President Bowles and he discussed Standardization and Consolidation of campus finance functions. For the 2007 fiscal year, there were 55 audit findings on 11 different campuses. Part of the solution to these problems involved standardization and centralization of financial operations. The University had been working with Ernst & Young to develop a plan to resolve these problems.

The Ernst & Young team (AJ Desai and Keith Feuz) presented a strategic plan, short term improvements (6-8 months) and shared service development and roll out (2+ years) for improving and transforming fiscal operations. (Attachment 1) Questions were answered throughout the presentation.

Chair Daniels mentioned that the Board notebooks held the audit reports and findings released since the last meeting and asked if there were any questions; no questions were received. (Attachment 2)

Mr. King reported on the ongoing UNC Internal Audit initiatives, including the use of Hotlines and analytical software to improve the effectiveness of internal audit activity. There will be a meeting of all UNC Internal Auditors in October.

Mr. King briefly discussed an auditing software program, Audit Command Language (ACL), to analyze data. The State Auditor has offered its ACL training resources to UNC Internal Auditors.

Lastly, Mr. Nelson reported on the administration of a multi-year federal grant known as GEAR UP at Appalachian State University. Both ASU and the U.S. Department of Education were conducting reviews of the GEAR UP grant activity. A team from UNC General Administration and the Internal Auditors at ASU were reviewing. Fayetteville State University and UNC General Administration also had GEAR UP programs.

There being no further business, the meeting was adjourned.

Mr. Frank Daniels, Jr.
Chair of the Audit Committee

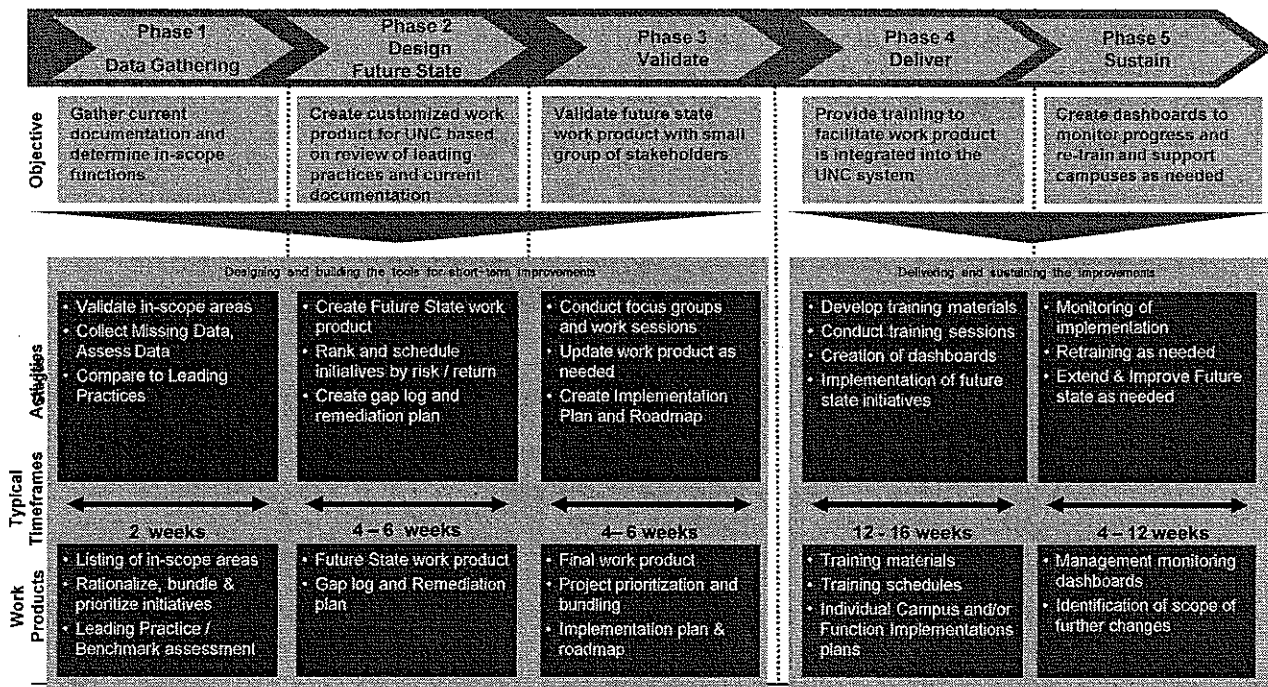
Mr. Charles Hayes
Secretary of the Audit Committee

Finance Function Transformation Implementation Plan

- ▶ An implementation plan will be created to execute the approach outlined in the following two slides (3-4 weeks)
- ▶ The plan will be broken out into two phases: short-term improvements (6-8 months) and shared service development and roll-out (2+ years)
- ▶ Short-term improvements will address the following areas:
 - ▶ policies and procedures
 - ▶ standardized closing calendar, checklists and templates
 - ▶ formalized review and approval procedures
 - ▶ timely monitoring and reporting procedures
 - ▶ standardized reporting
 - ▶ creation of key performance indices and management dashboards
- ▶ Shared service approach will consider such things as:
 - ▶ Change management and program management considerations
 - ▶ Lift and shift vs. standardization and centralizing
 - ▶ Consideration of different implementation approaches: single process, single location, new site, existing site, etc.
- ▶ Both phases will run concurrently, with interdependencies managed by the PMO
- ▶ The deliverables of the implementation plan include:
 - ▶ Project plan for each phase, with timelines
 - ▶ Detailed project plan for each phase of the approach with work steps, timelines and resource needs
 - ▶ Standardized reporting tools, templates and documents which will be leveraged in the implementation

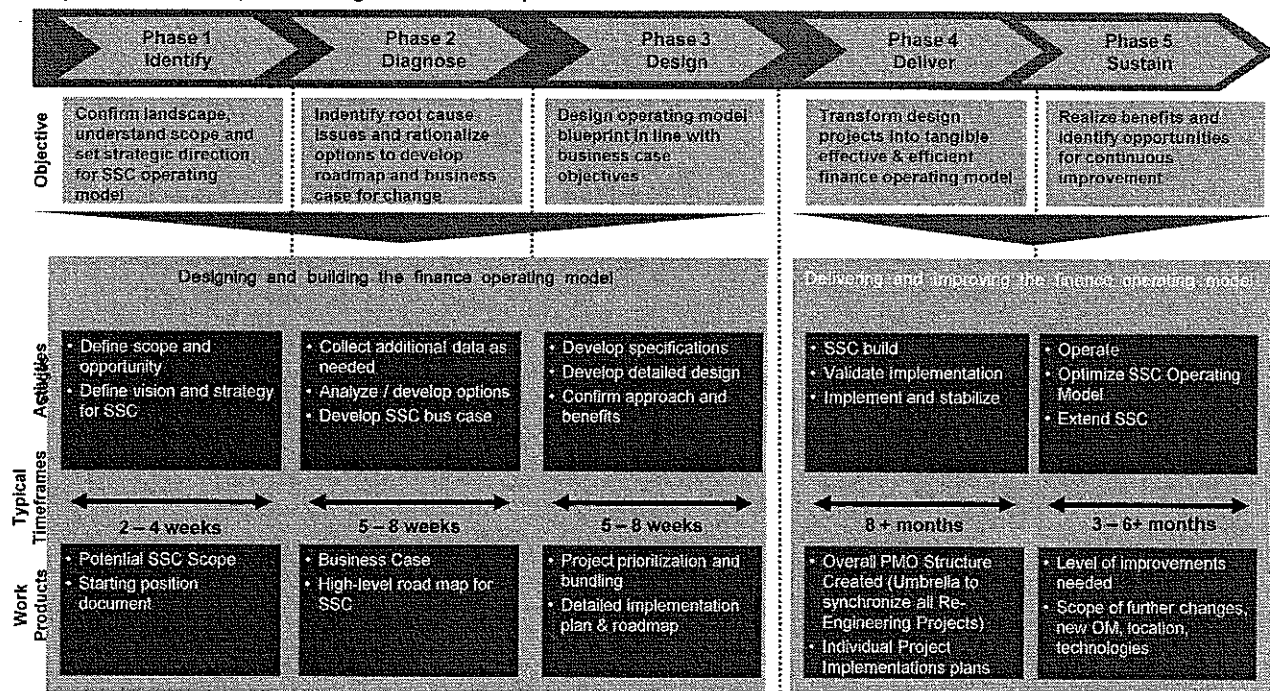
Short-term Improvements Approach

We will use this approach for each of the six areas identified in our future state document. The development of the implementation plans will run concurrently for all the areas.



Finance Transformation Redesign Approach

To create shared service operations, we assess and re-define the overall strategy, understand current operational needs, and design the future operations.



2007 Financial, Investigative, and Strategic Audit Reports Released Since Last Meeting by the North Carolina Office of the State Auditor:

1. North Carolina State University: – (Strategic Audit Review):

Report URL:

<http://www.ncauditor.net/EpsWeb/Reports/StrategicAudit/SAR-2008-6030.pdf>

See attachment.

2. North Carolina Central University: – (Investigative Audit): Six Audit Findings

Report URL:

<http://www.ncauditor.net/EpsWeb/Reports/Investigative/INV-2008-0337.pdf>

Matters Related to Financial Reporting or Federal Compliance Objectives

1. UNIVERSITY INFORMATION TECHNOLOGY SERVICES EMPLOYEES MISUSED THE UNIVERSITY NETWORK AND COMPUTERS BY DOWNLOADING MOVIES, MUSIC, GAMES, SOFTWARE, AND PORNOGRAPHY.

Data Base Administrator

Our review of computers and disk drives assigned to and under the control of the Data Base Administrator in the University's Information Technology Services (ITS) Department indicated inappropriate use of University networks and computers. We found numerous files of inappropriate material including "ripped"¹ versions of films, music, software, and video games. In addition, our analysis discovered pornographic materials.

During our interview, the Data Base Administrator admitted inappropriate use of University-issued computers by downloading files from various internet sites. He said that it was strictly for personal use and that he never sold or distributed any of the material except to a few friends.

The Data Base Administrator said he used the University networks because the larger bandwidth provided faster downloads. 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 to his personal computer at home.

During our review, we discovered two volumes² present on the University network server under the control of the Data Base Administrator. These volumes contained a number of files containing movies, music and pictures, some of which were pornographic. Also, various types of application software were in the volumes. The Data Base Administrator indicated that these volumes were where he would store data on a temporary basis until he transferred it to his external hard drive. downloaded because he did not keep count. He estimated that he had downloaded approximately

¹ A "ripped" file is one in which encryption that prevents duplication has been removed by a software program.

² A "volume" is a fixed amount of storage on a disk or tape, often used interchangeably with "drive."

The Data Base Administrator could not quantify the exact number of movies he had 100.

When asked, the Data Base Administrator acknowledged that downloading copyrighted material was illegal. He also said that he downloaded pornographic material on a "semi-regular" basis but knew of no university policy prohibiting that. However, he said that he knew that the State had a policy prohibiting that activity.

The Data Base Administrator said that he learned about the downloading method from a former University ITS employee, who is now employed at another university, who had the reputation while at the University as the "movie guy."

Information Technology Manager

We also reviewed the computers and disk drives assigned to and under the control of the Information Technology (IT) Manager. This review also indicated inappropriate use of University networks and computers. We found numerous files of inappropriate material including movies, music, software, and video games. In addition, some pornographic images were present on the IT Manager's computer.

In addition, we found decrypting software called AnyDVD³ on the IT Manager's computer. When we questioned the IT Manager as to why this type of software was needed, he said that he made movies for the Chancellor of events such as inauguration and graduation using a digital camera. After further prodding, the IT Manager admitted that the software was not needed as he had indicated but was used to override copy protection on retail DVD's and to produce "ripped" copies of movies.

We asked the IT Manager if he had knowledge of the Data Base Administrator downloading movies using the University's equipment. He said that he once spoke to the Data Base Administrator about it and told him not to do it. The IT Manager said that he believed that the Data Base Administrator had stopped.

We discussed with the IT Manager the meaning of an e-mail we located on his computer stating that the Data Base Administrator was making downloaded movies available to him. The IT Manager stated that he had only accepted two or three of these type movies one time when he had to spend an evening working and he wanted a movie to watch while there. However, the Data Base Administrator said that he had provided the IT Manager with movies on approximately 20 occasions.

We asked the IT Manager why there were pornographic images on his assigned University laptop computer. The IT Manager answered that if there were any such images it was because he gets items sent to him by individuals who were "spammed" and he has to open the attachment to verify its content. We asked if he visited any pornographic sites while at work and he indicated that he did not. We then asked why we were able to locate 68 hits to a site called "Nudetube.com" originating under his user name. He denied any knowledge of that without giving a plausible explanation.

The Data Base Administrator and IT Manager are responsible for accessing and maintaining various computer networks for the University, including all campus network servers dedicated to specific departments. Their duties include network security and informing other users about inappropriate use. As such, they have an even higher responsibility to protect the University network from unauthorized use.

³ AnyDVD is a driver allowing decryption of DVD's, as well as targeted removal of copy preventions. AnyDVD is also able to remove copy-prevention from audio CD's.

Recommendation:

The University should take strong disciplinary action against the Data Base Administrator and IT Manager. In addition, the University should review all items for which they had access to determine the extent of their inappropriate use. Further, this review should seek to determine whether the University's computer system and network security were harmed.

2. UNIVERSITY INFORMATION TECHNOLOGY SERVICES EMPLOYEES DISTRIBUTED COPYRIGHTED MATERIALS.

The Data Base Administrator 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 Data Base Administrator said he had given copies of movies and music to individuals within the Information Technology Services Department at NC Central University. He denied selling any of these materials, instead claiming they were given as free copies. The Data Base Administrator 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.

Note: This finding will be referred to the U.S. Attorney's Office, Middle District, the District Attorney for North Carolina Judicial District 14, and the North Carolina State Bureau of Investigation.

Recommendation:

The University should take strong disciplinary action against the Data Base Administrator. 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 INFORMATION TECHNOLOGY MANAGER WAS GRANTED UNAUTHORIZED ACCESS TO ANOTHER UNIVERSITY'S SERVER IN ORDER TO DOWNLOAD MUSIC FILES.

While reviewing e-mail messages located on the IT Manager's computer, we located an e-mail dated February 6, 2008 indicating that an employee at North Carolina State University (NC State) "set up a share" that allowed the IT Manager access to the NC State computer network. In a February 20, 2008 e-mail, the NC State employee told the IT Manager "the vendor came in yesterday to install the app on the server you were using and I had to drop the share." In response, the IT Manager asked the NC State employee to "setup another share" and the NC State employee agreed.

The IT Manager told us that he was vacationing in Atlanta during that time and wanted to download some karaoke files to entertain his children. He said the NC State employee who previously worked at NC Central agreed to grant access to the IT Manager. He said that this access was granted "only that one time."

The IT manager, whose responsibility at NC Central is to oversee network security, admitted that is was wrong for the NC State employee to grant him access to the NC State network. The IT Manager also said that he had never given similar access to the NC State employee to the NC Central network.

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, Middle District, the District Attorney for North Carolina Judicial District 14, and the North Carolina State Bureau of Investigation.

Recommendation:

The University should take strong disciplinary action against the IT Manager. In addition, the University should provide additional training to all Information Technology Services Department employees that stress the need to ensure network security.

4. THERE EXISTS A LACK OF ADEQUATE CONTROLS OVER ASSETS.

During the course of our review, we became aware that the Information Technology Services Department lacks an adequate system of controls over the purchase and accountability of their assets.

The procedures in place are that any item purchased with a price of greater than \$1,000 is tagged by the Fixed Asset Office and that office is required to log where the item is assigned. However, according to the Chief Information Officer (CIO), tracking inventory "is a gap for us."

The CIO said that an annual inventory is required to be conducted and that the ITS Department receives a list of missing items in order to locate them. The CIO said that they have been able to locate most items in the past. He said that a transfer asset form is required to be completed when an asset is transferred to another user.

Because there were allegations raised as to questionable purchases being made, a complete inventory audit was performed and provided to the Fixed Asset Office. During that audit, equipment costing less than \$1,000 was discovered that had been purchased and never authorized. For example, a digital camera and Global Positioning System (GPS) device was located that the CIO indicated that he had not approved. The CIO stated that four large screen HDTV monitors were purchased for the ITS department by his predecessor. These monitors are supposedly used by the managers to "monitor trouble tickets." However, when we reviewed the asset lists that were produced by the Fixed Asset Office, we did not see any TV monitors.

Both the CIO and IT manager said that the CIO signs off on all purchases of small items as well as large items. However, during our interview with the IT Manager, he indicated that he had purchased a camera and GPS device when a vendor contacted him stating that they had "extra money" on a purchase order and asked what was to be done with the money. The IT manager said that he ordered the camera and GPS device with that money. The IT Manager also said that the HDTV monitors had been purchased using "end of the year money."

The IT Manager said that he used the camera to take pictures around campus, broadcast football games, and record the Chancellor's inauguration, all of which are broadcast over the campus networks. The IT manager said that he ordered the GPS device "because he likes toys." The IT manager said that he only used the GPS device once on a trip to Asheville (or Ashevilleboro) in December 2007.

During our interviews with other employees, we learned that there have been a number of smaller equipment purchases made such as Ipods and Blackberry devices with no tracking system in place to determine their current use. Also, we were told that some Macintosh laptop computers were purchased and that Ipod devices were included with the purchase. Four employees of the ITS department received those Ipod devices with no records being kept of their receipt.

During our review, we observed a significant amount of unused equipment present in the server room. These items included Blade servers, switches, laptops and monitors. We were unable to determine the exact purpose or need of this equipment.

Recommendation:

University management should implement policies and procedures to ensure that all equipment purchases are properly approved and tracked as to where the equipment is being used. ITS personnel should work with the Fixed Asset Office to implement procedures to ensure that equipment is properly accounted for.

5. EMPLOYEES ARE NOT REQUIRED TO COMPLETE SECONDARY EMPLOYMENT FORMS.

During the course of our review, we discovered that the IT Manager was part-owner of a business providing network services. The IT Manager said that the business was no longer active but they were continuing to file tax returns in hopes of reviving the business in the future.

We reviewed the personnel file for the IT Manager and there was no indication that a secondary employment disclosure was completed by the IT Manager. During our questioning of the IT Manager, he indicated that he had not completed a secondary employment form related to his secondary business. Also, when we interviewed the CIO, he said that he was unaware of the IT Manager's secondary employment.

The North Carolina State Personnel Manual states:

"The employment responsibilities to the State are primary for any employee working full-time; any other employment in which that person chooses to engage is secondary. An employee shall have approval from the agency head before engaging in any secondary employment. The purpose of this approval procedure is to determine that the secondary employment does not have an adverse effect on the primary employment and does not create a conflict of interest. "

It is the responsibility of the employee:

- *To complete a Secondary Employment Form for all employment that is not covered by Dual Employment, and*
- *To update the form annually, as well as to document changes as they occur. "*

According to the University Human Resource officials, the University follows the State Personnel policy related to secondary employment and the policy has always been in place but "only in the past couple of years" have the Human Resource division attempted to encourage compliance. The official said that it is the responsibility of each employee to submit and update a secondary employment form and for each department to keep employees informed of the need to do so.

Recommendation:

University management should ensure that all employees have completed a secondary employment form in accordance with State Personnel policies and should annually remind employees of the need to complete the form if there have been any changes.

6. UNIVERSITY OFFICIALS DID NOT PROPERLY VERIFY DEGREES, PRIOR EMPLOYMENT, AND CREDENTIALS WHEN HIRING AND PROMOTING EMPLOYEES.

During our review, we noted that the Data Base Administrator indicated on his initial employment application for the position of Computer Consulting II, that he had obtained a degree in computer science with 108 semester hours of credit from an out of state university. However, during the verification of reference and education process, it was confirmed that the Data Base Administrator had completed only 52 semester hours and did not obtain a degree as he had indicated on his employment application.

During our interview with the Data Base Administrator, he confirmed that he had not completed the degree requirements and was still attending the school online.

Training and Experience requirements for the position stated that: "Graduation from a two-year college or technical school with a degree in data processing and eighteen months of experience in data processing; or graduation from a four-year college or university and eighteen months of experience in data processing; or equivalent combination of training and experience," were required for the position.

We reviewed the personnel file of the Data Base Administrator and noted that no action appeared to have been taken with regard to the discrepancy. Human Resource officials indicated that the Data Base Administrator's employment qualifications were based upon a combination of work experience as well as educational achievement.

Also, according to University Human Resource officials, subsequent promotions that the Data Base Administrator received were done so under the new "Career Banding" initiative that emphasizes job skills and experience rather than educational attainment.

However, we believe that the inclusion of incorrect or false information on an employment application should have raised concerns about the applicant. We saw no evidence that the issue was ever addressed.

Recommendation:

University management should ensure that any discrepancies that are discovered related to a new employee's employment history and educational achievements are noted and addressed. Any actions taken related to the discrepancies (up to and including rescinding the employment offer) should be noted in the employee's personnel file for review in future promotions and/or hiring decisions.

Please see attachment 2 for University responses to the findings.

3. North Carolina State University: – (Investigative Audit): Four Audit Findings

Report URL:

<http://www.ncauditor.net/EpsWeb/Reports/Investigative/INV-2008-0336.pdf>

Matters Related to Financial Reporting or Federal Compliance Objectives

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"⁴ 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.

⁴ A "ripped" file is one in which encryption that prevents duplication has been removed by a software program.

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 IDS 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 ..."

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.

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 stress the need to ensure network security.

Please see attachment 3 for University responses to the findings.

4. Elizabeth City State University: – (Financial Audit): Six Audit Findings

Report URL:

<http://www.ncauditor.net/EpsWeb/Reports/Financial/FIN-2007-6086.pdf>

Matters Related to Financial Reporting or Federal Compliance Objectives

The following audit findings were identified during the current audit and describe conditions that represent significant deficiencies in internal control or noncompliance with laws, regulations, contracts, grant agreements or other matters.

1. INADEQUATE BANK RECONCILIATIONS

The University did not perform bank reconciliations for the Short-term Investment Fund, the State Disbursing account and Capital Improvement account for any month in our audit period. A majority of the University's transactions are processed through these three accounts. The University was unable to completely reconcile the accounts until April 2008. As a result, there was an increased risk of error and misappropriation of assets.

Recommendation:

The University should improve internal control to ensure that all its bank accounts are reconciled completely, accurately, and timely.

University's Response:

We concur with the recommendation.

The following steps have been accomplished:

- We have reconciled the bank statement balances to the Banner bank fund balances for all three Banks.
- We are finalizing procedures and plan to have all reconciliations current at June 30, 2008.

2. FINANCIAL STATEMENTS AND NOTES REQUIRED SIGNIFICANT CORRECTIONS

The financial statements and notes prepared by Elizabeth City State University presented for audit contained significant errors. Without our audit adjustments, users of the financial statements could have been misled about the University's financial condition and results of operations.

During our audit of the 2007 financial statements, the following errors were found:

- a. The University posted two erroneous journal entries resulting in the overstatement of Unearned Revenue by \$1,012,318.
- b. The University had capital assets totaling \$2,285,813 recorded as General Infrastructure that was not being depreciated. The assets were in the subsidiary ledger but depreciation expense for the assets had not been recorded in prior years. This resulted in Depreciable Capital Assets being overstated by \$1,021,009.

- c. The University had projects recorded as Construction in Progress that had been completed and placed in service during prior years or the current year. As a result, No depreciable Capital Assets was overstated by \$5,300,070.
- d. Amounts totaling \$256,031 due from the Primary Government or State of North Carolina Component Units were recorded as Accounts Receivable.
- e. There were numerous errors related to the Net Pledges Receivable balance including a prior period adjustment.
- f. The Allowance for Uncollectible Noncapital Gifts in the amount of \$1,120,146 was erroneously netted against the operating revenue account Sales and Services, resulting in a negative balance in the note to the financial statements.
- g. Various other errors were noted in the financial statements, notes to the financial statements and management's discussion and analysis.

There were other problems and a lack of controls related to the financial reporting process as well. Specifically:

- Journal entries posted by the University did not have adequate explanations or supporting documentation.
- There was limited, if any, review for many journal entries posted to the general ledger throughout the year.
- There was also limited management review of the financial statements and the notes to the financial statements prior to submission to the Office of the State Controller and the Office of the State Auditor. This review was not adequate to identify misstatements on the financial statements and notes.

Recommendation:

The University should place greater emphasis on the year-end financial reporting process and implement effective internal control procedures to ensure the completeness and accuracy of the financial statements. The University should perform an adequate review of the journal entries posted to the general ledger to ensure the entries are appropriate and adequately supported.

University's Response:

We concur with the recommendation. Since June 30, 2007, we have hired additional staff. Procedures for adequate preparation and review will be in place by June 30, 2008 to ensure accuracy and timeliness for management approval.

The Banner accrual system for June 30, 2008, was made available in May 2008. For June 30, 2007, the system became available near the end of August 2007. The additional time for processing accrual transactions and additional staff will provide for greater accuracy in preparing and reviewing financial statements.

3. INFORMATION SYSTEM ACCESS RIGHTS INCONSISTENT WITH JOB DUTIES

The University did not have adequate procedures in place to ensure that employees only had information systems access rights necessary to perform their job duties. This could result in unauthorized or inappropriate transactions.

Appropriate University personnel did not periodically review access rights to determine if the correct access was granted to an employee consistent with their job duties. As a result, we noted

117 user id's with maintenance/update access to post journal entries to the general ledger. Maintenance access indicates that a user can update information in the system. Of these 117 user id's, only 20 had been approved by the Module Security Administrator to have maintenance access. Journal entries are posted without any electronic approval necessary, which also increases the risk that inaccurate and/or inappropriate entries will be included in the financial records.

Adequately designed internal controls require transactions and other significant events to be authorized and executed only by persons acting within the scope of their authority. Therefore, system access rights should be reviewed on a regular basis.

Recommendation:

Management should implement policies and procedures to ensure that users are assigned access levels consistent with their job duties. Such policies and procedures should include allowing the Module Security Administrator to perform review of access to determine if it is appropriate.

University's Response:

We concur with the recommendation and have corrected the inappropriate system access. The following steps will be taken by June 30, 2008 to prevent inappropriate information system access.

- ECSU Banner Security System Guidelines will be updated to provide reconciliation between user roles and actual access.
- The Banner Security Administrator (Information Technology) will provide the Module Security Administrator (Accounting) with a monthly report on user system access. This task will be included in Accounting's monthly close-out schedule.
- The Module Security Administrator along with the Banner Security Administrator will review user system access (BANSECR) every ninety (90) days.
- A review process has been added to monthly close-out matrix.

4. DEFICIENCIES IN INTERNAL CONTROLS OVER CAPITAL ASSETS

During our audit period the University failed to reconcile the capital asset subsidiary system to the general ledger and amounts ultimately reported in the financial statements. As a result, there was an increased risk of error in the financial statements.

The University policy manual states that "Fixed Assets should be reconciled monthly by the Fixed Asset Office Officer and the Accounting Department. The Capitalized assets recorded on the fixed asset system should be balanced to the assets recorded on the general ledger. Any differences must be researched and resolved. The reconciliation must be documented and remain on file in accordance with record retention policies."

Recommendation:

The University should adhere to its policies and procedures to ensure the fixed asset subsidiary system is reconciled to the general ledger.

University's Response:

We concur with the recommendation and will ensure the fixed asset subsidiary system is reconciled to the general ledger.

5. STUDENT ACCOUNTS SYSTEM NOT RECONCILED TO THE FINANCIAL STATEMENTS

The University failed to reconcile the subsidiary ledger (Student Information System) that supports the student accounts to the general ledger and amounts ultimately reported in the financial statements. If the subsidiary ledger is not reconciled to the general ledger there is a risk that the amounts reported in the financial statements are incorrect.

During our audit, we identified numerous misstatements in the financial statements and notes related to student accounts including:

- Student Accounts Receivable was overstated by \$1,167,063.49
- Amounts disclosed with the components of the Sales and Services revenue account were misstated.

Recommendation:

The University should implement proper policies and procedures to ensure subsidiary systems are reconciled to the general ledger.

University's Response:

We concur with the recommendation and will ensure that all subsidiary systems are reconciled to the general ledger.

6. NONCOMPLIANCE WITH BOND COVENANTS

The University has not complied with certain debt service covenants for the Elizabeth City State University Housing Foundation Series A bonds. As a result, the bond trustee could require immediate repayment of the debt, though only from its dormitory system net revenues.

The "Use Agreement" between the University and Elizabeth City State University Housing Foundation, LLC requires the University to operate the foundation-owned apartments Viking Village such that it shall maintain a certain debt service coverage ratio. In addition the use agreement also requires University and the Board of Governors of the University of North Carolina System to revise fees, rents, and charges for the use of and for services furnished by the Viking Village so that the University will meet the covenant stated above.

Recommendation:

The University should revise fees, rents, and charges for the use of and for their services furnished by Viking Village so that the debt service bond covenants are met.

University's Response:

In concurrence with this recommendation the University has executed the following steps to ensure compliance with bond covenants.

- In 2007, a responsibility matrix was created detailing the staff assignments related to bond covenants.
- The Elizabeth City State University Board of Trustees approved a rate increase of \$200 per resident per year for Viking Village.
- Revenues and expenditures are being closely monitored.

5. North Carolina Central University: – (Financial Audit): Four Audit Findings

Report URL:

<http://www.ncauditor.net/EpsWeb/Reports/Financial/FIN-2007-6090.pdf>

Matters Related to Financial Reporting or Federal Compliance Objectives

The following audit findings were identified during the current audit and describe conditions that represent significant deficiencies in internal control or noncompliance with laws, regulations, contracts, grant agreements or other matters.

1. DEFICIENCIES IN FINANCIAL REPORTING

The financial statements prepared by the University contained misstatements that were corrected as a result of our audit. Without these corrections, the financial statements could have been misleading to readers. We also noted that audited information from component units was not available on a timely basis. Misstatements included:

- a. There were misclassifications in the net asset account balances totaling \$5.9 million.
- b. Current unrestricted cash was overstated by \$7.4 million, current restricted cash was understated by \$5.3 million, and noncurrent restricted cash was understated by \$2.1 million.
- c. The University has not periodically evaluated the appropriateness of the estimated useful lives of its capital assets. A review of capital assets identified an estimated overstatement of accumulated depreciation of approximately \$3.26 million.
- d. The Statement of Cash Flows contained several errors. Ten months after the year-end, University personnel prepared a revised statement.
- e. The investment note required significant revisions. For example, the University failed to report disclosures about material investments held by the discretely presented component unit. These investments had a market value of \$10.9 million.
- f. The table in the changes in long-term liabilities note did not balance by \$5.3 million. Several amounts were entered in the table as negatives and should not have been. In addition, the note included a table from the prior fiscal year that was not updated for fiscal year 2007.
- g. Various other misstatements were made in the financial statements and notes to the financial statements.

The audit reports for the North Carolina Central University Foundation, Inc. and the NCCU Real Estate Foundation, Inc. (Real Estate Foundation) were not received until May 2008. The University did not hire an auditor for the Real Estate Foundation until we raised the issue at least six months after year end. The audits of these component units are needed prior to issuance of the University's audit report.

Recommendation:

The University should place greater emphasis on and devote more resources to the year-end financial reporting process and implement effective internal controls to ensure complete and accurate financial statements. Furthermore, the University should ensure that foundation audits are performed timely.

University Response:

The University concurs. During the fiscal year, the University filled key vacancies, conducted additional staff training, and consulted with various technical experts in an effort to eliminate financial reporting deficiencies.

The NCCU Foundation and the Real Estate Foundation have engaged their respective auditors for fiscal year 2008. Those audits will be completed within the prescribed time frames outlined in the Memorandum of Understanding.

2. DEFICIENCIES IN BANK RECONCILIATIONS

The University did not prepare bank reconciliations accurately or timely during our audit year. This increases the risk that an error or misappropriation could occur and not be detected in a timely manner.

Our review of the monthly bank reconciliations for the State disbursing and Institutional Trust Fund (ITF) accounts disclosed the following weaknesses:

- The University did not complete reconciliations for the ITF account in a timely manner. Ten of the 12 monthly reconciliations examined were prepared from four to 80 days late, with an average of 39 days late. Consequently, the University has not complied with the State Treasurer's Internal Control Policies Manual, which requires that bank accounts be reconciled promptly after the end of each month. University policies require reconciliation within 15 days of receipt of the monthly State Treasurer's bank statement.
- The University had unreconciled differences between the bank balance and the book balance in both the State disbursing and the ITF accounts. The State disbursing account had six months with unreconciled differences up to \$158,165 at June 30, 2007. The ITF account had unreconciled differences for the entire fiscal year up to \$5,900,227 with an unreconciled balance of \$374,919 at June 30, 2007. In addition, the ITF book balance per the bank reconciliation reflects \$1,638.95 more than the general ledger at June 30, 2007.
- The State disbursing reconciliation contains old outstanding checks dating back to June 1996 that have not been cleared or escheated.

Recommendation:

The University should improve internal control to ensure that all its bank accounts are reconciled completely, accurately and timely. Any variance with the general ledger should be investigated and reconciled. Outstanding items should be cleared or escheated in a timely manner.

University Response:

The University concurs. Prior to the implementation of Banner, the University reconciled all its bank accounts. During the year, the University created several webfocus reporting tools to assist with the reconciliations, enlisted the services of an external CPA firm, cleared reconciling items on the state disbursing account, and escheated old outstanding checks. The University will continue to review and refine the reconciliation process.

3. INFORMATION SYSTEM ACCESS AND SECURITY NEEDS TO BE STRENGTHENED

The University has weaknesses in assigning information system access rights and security classes, as well as the monitoring of information technology activity. These deficiencies could result in unauthorized or inappropriate transactions.

Weaknesses include the following:

- There are multiple employees in the Information Technology Systems unit who can login to the information system under a single user name. This single user name accesses the security form that creates/modifies user accounts, grants access to security classes, sets up passwords, and locks/unlocks user accounts. With multiple users having the ability to login using a single user name, there is no way to trace activity to the responsible employee.
- There are several individuals who have unnecessary access to forms and security classes. The individuals have no job responsibilities that require them to have access to some of the forms and/or classes to which they have been given access.
- One of the security classes in purchasing and receiving includes forms and responsibilities inconsistent with appropriate segregation of duties. Individuals assigned to this security class may create a requisition, process a purchase order, and verify the receipt of goods.
- The Information Technology Manager has unlimited access to all forms and security classes and the activity of this account is not monitored. The lack of monitoring decreases the ability to detect inappropriate activity at this security level.

Recommendation:

The University should limit system access rights to ensure that employees are assigned the least amount of system access necessary to perform their job. Adequate segregation of duties should be maintained. System access rights should be reviewed on a regular basis and the Information Technology Manager's activity should be monitored.

University Response:

The University concurs. The University has implemented a process whereby monthly security reports of user access are provided to the functional areas for review. Additionally, the University underwent a security assessment by an external technology firm to identify areas for improvement. The University is also monitoring all Banner activity of the IT staff, including the Database Administrators via logs, which is accessible only to the IT Security Officer and the Chief Information Officer. The activity of the Information Technology Manager is being monitored.

4. UNTIMELY NOTICE TO LENDERS OF CHANGES IN STUDENTS' STATUS

The University did not provide student financial aid lenders with timely notice when students withdrew from the University. Title 34CFR, Part 635.309(b)(2) requires the University to notify the National Student Clearinghouse within 30 days of its discovery that a recipient of a Federal Direct Loan has ceased to be enrolled on at least a half-time basis, failed to enroll, or changed his or her permanent address.

The University failed to provide timely notice for all 25 of the student withdrawals we reviewed. Six were reported outside of the required timeframe. The remaining 19 were not reported until it was brought to the University's attention by the auditors. These were reported approximately two to 10 months late. The University had not adopted written procedures for providing the notice.

Recommendation:

The University should develop written policies and procedures and implement controls to provide for timely notification of changes in student status.

(Award # P007A063097 - Award year 7/1/2006 - 6/30/2007)

University Response:

The University is in agreement with the audit finding and recognizes the urgent need to strengthen checks and balances when reporting withdrawn students to the National Student Clearinghouse. In this regard, a committee has been formed to review the current process. The committee has already identified ways to strengthen the process to eliminate further findings of this nature. For example, a withdrawal report will be submitted twice monthly to the Registrar's Office from the Dean of Students Office, and a complete review will be done by the Registrar's Office to make sure that withdrawn students have been reported accurately in Banner and the National Student Clearinghouse. Every effort will be made going forward to make absolutely sure that each student institutional withdrawal will be reported accurately to the National Student Clearinghouse to ensure that lenders are notified in a timely manner when a student status changes. It should also be noted that the Banner system is processing the withdrawals that are submitted to the National Student Clearinghouse file. The corrective action has been completed and the implementation date was February 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>

May 30, 2008

Dr. James L. Oblinger, Chancellor
North Carolina State University
Campus Box 7001
Raleigh, North Carolina 27695

Dear Dr. Oblinger:

We have completed a strategic review to identify improper use of procurement cards (P-Cards) by North Carolina State University employees. The statewide rules for P-Card use falls under the Department of Administration's Purchase and Contract Division. All state agencies operate under the Bank of America Card Contract with the Division of Purchase and Contract. The results of our review are contained in this management letter. The review was conducted pursuant to North Carolina General Statute §147-64.6(c)(16) rather than as a financial audit.

North Carolina General Statutes require the State Auditor to make audit reports available to the public. Management letters and responses receive the same distribution as audit reports.

Please contact me if you have any questions about these audit findings and recommendations. We express our sincere appreciation to you and your staff for the cooperation extended to us during our strategic review.

Sincerely,

LESLIE W. MERRITT, JR., CPA, CFP
STATE AUDITOR

A handwritten signature in cursive script that reads "Charles T. Williford".

Charles T. Williford, CPA, CITP, CISA, CFE, CPM
Director of Information Systems Audits

LMjr/CTW/TG:mfd

BACKGROUND

The Office of the State Auditor has implemented a strategic review initiative. This initiative is an effort to analyze state agency/university data on a proactive basis and help identify unusual trends and potential problems in this data.

The P-Card program is designed to enable organizations to make small purchases more quickly and efficiently, thereby reducing the volume of requisitions, purchase orders, invoices and checks processed by those organizations. Similar to the VISA and MasterCard formats, procurement cards can be processed by vendors just like personal charge cards. Rather than making multiple small payments to many vendors, the using organization writes one check to the procurement card provider. Vendors receive payments from the procurement card processor within few days without extra paperwork.

In July 2006 the Division of Purchase and Contract entered into a contract with the Bank of America to administer the VISA P-Card program for the state of North Carolina. This contract is set to expire in December 2012. Under this contract, there is no charge for issuance or maintenance of the cards. Each agency that uses these cards receives a rebate on the total amount charged to the P-Cards.

The Division of Purchase and Contract has general guidelines for the participant organizations to follow but has left control of the P-Card program with the chief fiscal officer of the organizations.

The procurement card program administrator at the Department of Administration, Division of Purchase and Contract, in consultation with the individual agency's chief fiscal officer, determines the appropriate limits by transaction amount, billing cycle, and merchant categories.

REVIEW RESULTS

We obtained the P-Card electronic file from the Bank of America that covered the period of December 2006 through December 2007. During that period NCSU had a total of 85,263 individual transactions that totaled \$23,196,973.48.

To conduct our strategic review, we performed the following procedures:

- Obtained and reviewed NCSU P-Card program policy.
- Selected a judgmental sample of 73 P-Card transactions from the Bank of America electronic file to review their supporting documentation. Sample selection focused on transactions that appeared inappropriate based on such factors as merchant name, merchant category description and/or item description.
- Matched the names of NCSU P-Card holders with the names on the "felony" file we received from the NC Department of Correction. The objective here was to determine whether any of the card holders was convicted of a felony that we deemed it "incompatible" with holding a P-Card (for example, identity theft or credit card fraud).
- Extracted all purchases where the limit by per-transaction amount was exceeded.
- Interviewed appropriate agency P-Card program staff.

The results of our review are as follows:

- 1) NCSU's P-Card program policy appears to be adequate.
- 2) From our review of P-Card transactions we identified two employees who used their P-Card for personal use. One employee repaid his personal charge by check and the other employee had her last paycheck reduced for all personal charges.
- 3) We did not identify any P-Card holders that matched the NC Department of Correction felony file.
- 4) We identified seven purchases that exceeded the single transaction limit. All of these transactions were properly approved by the Division of Purchase and Contract.

Based on the results of our review it is our opinion that the P-Card internal controls in place at NCSU either helped deter or prevent most improper charges from taking place. The questioned personal charges mentioned in item 2) above were identified early and either repaid or deducted from employee pay. The university has dismissed one the two employees identified in item 2) above.

REVIEW RESULTS (CONCLUDED)

Agency Response:

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

919.515.2151 (phone)
919.831.3545 (fax)

May 22, 2008

The Honorable Leslie W. Merritt, Jr., State Auditor
Office of the State Auditor
2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601

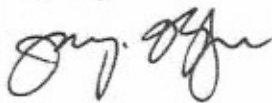
Dear Mr. Merritt:

Thank you for the draft of your strategic review to identify improper use of procurement cards. We are pleased at the verification that our internal controls are working and that our staff had previously identified the items noted in the audit and taken appropriate actions.

We would like to express our appreciation for the auditors' professionalism while working with our staff.

If you have any questions, please contact Ernest G. Murphrey, Associate Vice Chancellor for Financial Services, at (919) 513-0410.

Sincerely,



James L. Oblinger
Chancellor

cc: Cecile M. Hinson
Charles D. Leffler
Ernest G. Murphrey
Charles T. Williford

JLO/EGM:lbo

RESPONSE FROM NORTH CAROLINA CENTRAL UNIVERSITY



James E. Shepard, Founder

Office of the Chancellor

June 11, 2008

Mr. Leslie W. Merritt, Jr., CPA, CFP
State Auditor
2 S. Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Dear Mr. Merritt:

Thank you for the opportunity to review and comment on the draft report, dated May 27, 2008, regarding the special review of the Information Technology Service (ITS) Department at North Carolina Central University. I am in agreement with your recommendations. The ITS management and our Interim Internal Audit Director have reviewed the report and its recommendations.

Issues that are identified in the report have been addressed. We have hired UNISYS to complete an assessment of the ITS general controls for FY 2008. In addition, the Internal Audit Office is conducting further review of this matter and will issue a separate audit report upon completion.

Please feel free to contact me should you have questions regarding our responses.

Sincerely,

Charlie Nelms
Chancellor

Enclosure: University Management Response

Copy to: Dr. Alan Robertson, Vice Chancellor of Administration & Finance
Mr. David King, Associate Vice President of Finance
Mr. Greg Marrow, Chief Information Officer
Ms. Loretta Hayes, Interim Director of Internal Audit



NORTH CAROLINA CENTRAL UNIVERSITY
OSA ITS Special Review
AUDIT FINDINGS AND RECOMMENDATIONS
For Fiscal Year 2008

Finding #1:

University Information Technology Services (ITS) employees misused the state network and computers by downloading movies, music, games, software, and pornography.

Recommendation:

The University should take strong disciplinary action against the Database Administrator and the IT Manager. In addition, the University should review all items for which they had access to determine the extent of their inappropriate use. Further, this review should seek to determine whether the University's computer system and network security were harmed.

University Response:

We concur with the recommendation. The University has taken immediate disciplinary action by releasing the two employees in question from the University. Furthermore, the following steps have been taken:

1. *The University brought in a company that specializes in the assessment of security threats or violation of security systems, Unisys Corporation, to do a complete NCCU security threat assessment. The threat assessment has been completed. No direct threats or intentional damage/harm to University computer systems or network security by the individuals in question was found. ITS is proactively working with Unisys to address their recommendations on how to better secure our networking equipment and computer systems.*

Finding #2:

University Information Technology Services (ITS) employees distributed copyright materials.

Recommendation:

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

University Response:

We concur with the recommendation. The University has taken immediate disciplinary action by releasing the two employees in question from the University. Furthermore, the following steps have been taken:



NORTH CAROLINA CENTRAL UNIVERSITY
OSA ITS Special Review
AUDIT FINDINGS AND RECOMMENDATIONS
For Fiscal Year 2008

1. *Information Technology Services (ITS) has taken proactive steps to ensure all ITS employees are familiar with University policies regarding Copyright Materials and Federal copyright laws contained in Title 17 of the United States Code. All ITS employees will be given copies of this Federal code and attend an annual training session on Copyright laws.*
2. *ITS will state clearly in its employee guide that any such violation of this law will result in strong disciplinary action being taken by the University up to and including dismissal.*
3. *ITS will deploy software during the summer of 2008 as recommended by an external Security Consultant that can monitor the illegal downloading of movies, music, and games by all University personnel.*

Finding #3:

The Information Technology Manager was granted unauthorized access to another University's Server in order to download music files.

Recommendation:

The University should take strong disciplinary action against the IT Manager. In addition, the University should provide additional training to all ITS department employees that stress the need to ensure network security.

University Response:

We concur with the recommendation. The University has taken immediate disciplinary action by releasing the two employees in question from the University. Furthermore, the following steps have been taken:

1. *ITS is currently setting up a series of educational classes that will occur annually during the summer months with all ITS employees that will address network security, privacy laws, copyright infringement, and other topics related to responsible use of University computing resources.*

Finding #4:

There is a lack of adequate controls over assets.

Recommendation:

University management should implement policies and procedures to ensure that all equipment purchases are properly approved and tracked as to where the equipment is being used. ITS personnel should work with the Fixed Asset Office to implement procedures to ensure that equipment is properly accounted for.



NORTH CAROLINA CENTRAL UNIVERSITY
OSA ITS Special Review
AUDIT FINDINGS AND RECOMMENDATIONS
For Fiscal Year 2008

University Response:

We concur with the recommendation. The University has taken steps to educate all employees within the ITS division about the Policies and Procedures in place by the University Fixed Asset Office. Furthermore, the following steps have been taken:

- 1. All ITS employees have completed and turned in fixed asset forms referencing any assets within their belongings. This process will be conducted annually to ensure all forms are up-to-date.*
- 2. ITS has met with both Purchasing and the Fixed Asset office to discuss existing University policies and procedures and the steps that need to be taken to ensure that employees are adhering to these policies and procedures.*
- 3. ITS has purchased and deployed an Asset Management System that will be used to track all assets purchased or maintained by the ITS division. By July 15, 2008, all ITS managed assets will be tracked and managed by the new ITS asset management tool.*

Finding #5:

Employees are not required to complete secondary employment forms.

Recommendation:

University Management should ensure that all employees have completed a secondary employment form in accordance with State Personnel policies and should annually remind employees of the need to complete the form if there have been any changes.

University Response:

We concur with the recommendation. The University has taken steps to educate all employees within the ITS division about the Policies and Procedures in place regarding the completion of secondary employment forms. Furthermore, the following mandate has been put in place:

- 1. ITS Managers will be held accountable for ensuring these forms are updated on an annual basis.*



NORTH CAROLINA CENTRAL UNIVERSITY
OSA ITS Special Review
AUDIT FINDINGS AND RECOMMENDATIONS
For Fiscal Year 2008

Finding #6:

University officials did not properly verify degrees, prior employment, and credentials when hiring and promoting employees.

Recommendation:

University management should ensure that any discrepancies that are discovered related to a new employee's employment history and educational achievements are noted and addressed. Any actions taken related to the discrepancies (up to and including rescinding the employment offer) should be noted in the employee's personnel file for review in future promotions and/or hiring decisions.

University Response:

The University agrees with the recommendation. During the period in question, there were many vacancies in the employment area, which contributed to the lack of proper verifications. Currently, the Department of Human Resources has procedures in place for verifying credentials and/or degrees. This issue has been corrected.

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