STATE OF NORTH CAROLINA

INFORMATION SYSTEMS AUDIT

PEOPLESOFT ACCOUNTS PAYABLE APPLICATION

NORTH CAROLINA STATE UNIVERSITY

FEBRUARY 2001

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

INFORMATION SYSTEMS AUDIT

PEOPLESOFT ACCOUNTS PAYABLE APPLICATION

NORTH CAROLINA STATE UNIVERSITY

FEBRUARY 2001

STATE OF NORTH CAROLINA
Office of the State Auditor

Ralph Campbell, Jr.
State Auditor

2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601
Telephone: (919) 807-7500
Fax: (919) 807-7647
Internet http://www.osa.state.nc.us

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Dr. Marye Anne Fox, Chancellor

Ladies and Gentlemen:

We have completed our audit of the PeopleSoft Accounts Payable application at North Carolina State University (the University). The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards* and was conducted during the period from September 19, 2000 through October 24, 2000. We present this report for your consideration.

The primary objective of this audit was to ensure that as data passes through the application, it is complete, accurate, timely and protected from unauthorized change. The scope of our audit included an assessment of the security architecture of the PeopleSoft Accounts Payable application and an assessment of the application and operating system configuration, specifically reviewing the access controls, data security, and network security over the application and the technical operating environment.

This report contains an executive summary and audit results which detail the areas where improvements should be made to strengthen controls over data passing through the PeopleSoft Accounts Payable application and operating environment.

We wish to express our appreciation to the staff of the North Carolina State University Administrative Computing Services for the courtesy, cooperation and assistance provided to us during this audit.

North Carolina General Statues require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Ralph Campbell, Jr.

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

[This Page Left Blank Intentionally]

EXECUTIVE SUMMARY

We conducted an audit of the PeopleSoft Accounts Payable application at North Carolina State University (the University) between September 19, 2000 and October 24, 2000. The primary objective of this audit was to ensure that as data passes through the application, it is complete, accurate, timely and protected from unauthorized change. Our conclusions are organized into three categories: those related to the PeopleSoft Accounts Payable Application Software, those related to the System Administration of the PeopleSoft Accounts Payable application by the University, and those related to Management Control issues.

PEOPLESOFT ACCOUNTS PAYABLE APPLICATION SOFTWARE

We noted the following weaknesses related to the PeopleSoft Accounts Payable application.

- The PeopleSoft Accounts Payable application software does not provide sufficient security features in the areas of user ID management, password management, and security violation and audit trail logging. See Audit Finding 1, *Security Functionality* and Audit Finding 2, *Security Violation Reporting and Audit Trails* for further information.

- A subsystem of the PeopleSoft application software which transmits financial data to the legacy Financial Accounting System (FAS) could provide unauthorized access to the legacy system. See Audit Finding 3, *Legacy System* for further information.

SYSTEM ADMINISTRATION

We identified several conditions related to the system administration of the PeopleSoft Accounts Payable application which should be addressed to improve controls.

- We noted that multiple system users share the PeopleSoft database account on the UNIX operating system that hosts the PeopleSoft Accounts Payable application. This usage is not effectively tracked. See Audit Finding 4, *Shared Identification* for further information.

- The PeopleSoft Accounts Payable application permits a user to have an unlimited number of sign-ons at multiple work-stations. See Audit Finding 5, *Concurrent Sessions* for further information.

- Controls over changes made to the PeopleSoft Accounts Payable application do not ensure that each change has been tested, reviewed and approved. See Audit Finding 6, *Application System Changes* for further information.

- Project data including system specifications, processing narratives, test plans and requirements documentation has not been protected from unauthorized change or deletion. See Audit Finding 7, *Project Data* for further information.

MANAGEMENT CONTROLS

Following are the findings we noted related to the Management Controls.

- NC State does not have an adequate segregation of duties between the employees who support, administer and use the PeopleSoft Accounts Payable application system. See Audit Finding 8, *Separation of Duties* for further information.

- NC State has not maintained security standards and procedures appropriate for the current client/server processing environment. See Audit Finding 9, *Security Standards and Procedures* for further information.

- NC State does not have an adequate business continuity plan for the user community in the event of a serious disruption of operations. See Audit Finding 10, *University Business Continuity Plan* for further information.

SUMMARY

The control environment over the PeopleSoft Accounts Payable application running at North Carolina State University requires improvement for the application to be considered a well-controlled, mission critical application. It should be noted that North Carolina State University Administrative Computing Services personnel have been very receptive to our suggestions during the audit. North Carolina State University Administrative Computing Services personnel addressed some findings we noted related to system administration and management controls while we were on site.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the North Carolina General Statutes Chapter 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. This IS audit was designed to ensure that as data passes through the PeopleSoft Accounts Payable application, the data is complete, accurate, timely and protected from unauthorized change.

SCOPE

The scope of our audit included an assessment of the security architecture of the PeopleSoft Accounts Payable application and an assessment of the application and operating system configuration, specifically reviewing the access controls, data security, and network security over the application and the technical operating environment.

METHODOLOGY

This IS audit was performed in accordance with Government Auditing Standards issued by the Comptroller General of the United States and Information Systems Audit Standards issued by the Information Systems Audit and Control Association. To accomplish our audit objective we reviewed:

- The application security architecture of the PeopleSoft Accounts Payable application, a vendor supplied software product, to ensure that the application offers effective data security controls.
- The segregation of the business functions performed within the PeopleSoft Accounts Payable application, to ensure that each transaction is properly authorized, reviewed and approved.
- Procedures for the initiation, review, approval and testing of changes made to the PeopleSoft Accounts Payable application.
- Standards and procedures for security in the client/server environment in which the PeopleSoft Accounts Payable application functions.
- Plans for the continuity of the Accounts Payable business function in the event of a serious disruption at the University.
- The completeness of the audit trail which identifies vendor and voucher transactions.
- The accuracy and completeness of transaction codes used in voucher processing.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

In 1997, North Carolina State University identified the need to enhance and standardize the University's financial and personnel systems, and also to better ensure compliance with Y2K. To satisfy these needs, the University selected the PeopleSoft suite of applications as an enterprise solution to replace the aging financial and personnel systems. The scope of the project included both PeopleSoft Financials and PeopleSoft Human Resources (HR). However, to accommodate legacy systems and to provide even greater functionality, the project also includes an interface with the legacy Financial Accounting System (FAS) running on the mainframe. In addition to the PeopleSoft applications, the University implemented the Web Travel System (which accepted input for travel expense reimbursement requests entered through the Internet), a workflow system, a voucher imaging system, an organizational security system, and an EDI system to streamline payments through Wachovia bank.

In October, 1998, the first PeopleSoft modules – General Ledger and Accounts Receivable were installed into production. Then in May, 1999 the University installed PeopleSoft Purchasing and in July, 1999 installed the Accounts Payable system. The University staff largely completed the installation, development work and user support using very few PeopleSoft or other consultants. The project team consisted of University staff from various organizations working together towards a common objective. This team included staff from the Controller's Office, Purchasing, the Budget Office, Administrative Computing Services (ACS) and representatives from the user community.

Work on the project is on-going. Changes are made as the University identifies opportunities to "fine tune" the system and correct or revise processing. This project has led to other initiatives such as the development, adoption, and implementation of the Configuration Management Standards and Procedures.

As part of the University's effort to support the PeopleSoft implementations, the Enterprise Information Systems (EIS) department was created. The EIS department serves as a liaison between the professional IT staff in the Administrative Computing Services department, the campus community, and the functional central and administrative offices. The EIS department has the lead responsibility for determining the fit, value, and cost/benefit of all future releases/modifications to the PeopleSoft suite of administrative software and for developing all functional specifications to be used by the technical staff for development and deployment. EIS also has primary responsibility for developing all QA test plans and assuring that all QA testing is performed correctly and in a manner that ensures system stability.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit findings identify the areas in the PeopleSoft Accounts Payable Application where recommendations have been made for improvement.

PEOPLESOFT ACCOUNTS PAYABLE APPLICATION SOFTWARE

The following findings are associated with the PeopleSoft Accounts Payable application software, a packaged product purchased from PeopleSoft, Inc.

AUDIT FINDING 1: SECURITY FUNCTIONALITY

The PeopleSoft Accounts Payable application does not provide the following basic security features:

- Ability to set a minimum password length and password composition rules.
- Ability to set Password expiration/change requirements.
- Ability to lock logon IDs after an excessive number of failed login attempts has occurred.
- Ability to suspend logon IDs after long periods of inactivity.

Because of the lack of these basic security features, the PeopleSoft Accounts Payable is vulnerable to the following problems:

- Hackers may be able to more easily guess passwords because users are not forced to use passwords that meet minimum requirements.
- Hackers may be able to more easily steal passwords because of the lack of expiration/change requirements.
- Hackers will have more potential accounts to attack because old accounts have not been locked due to inactivity.

If an unauthorized user gains access to the PeopleSoft Accounts Payable application, (s)he may gain the ability to add vendors, enter and approve vouchers, and process invoice payments.

Recommendation: The University should assess software products to provide these basic security features. Once the assessment has been completed and the product acquired and installed, the University should be sure they are implemented on the production server running the application at the University.

Auditee's Response: The University has assessed 3rd party software packages that will provide additional security features for the PeopleSoft Human Resources and Financials Systems. A software product from PentaSafe Security Technologies, Inc. (formerly Braintree Security Software) called IntraSECURE was selected and purchased by the University. IntraSECURE was selected because it was the only security product that supported the Sybase database environment used by the PeopleSoft systems at NC State.

The implementation of IntraSECURE has been completed. The following is an overview of the security features that are now in effect with the implementation of IntraSECURE:

Enforcing password change policy:

- Users are able to synchronize passwords across the reporting and production environments of both the HR and Financial systems.
- Users are required to change their password every 30 days
- Passwrods must be between six and eight characters long
- Different passwords must be used for 10 consecutive days
- Passwords are validated against "simple" passwords (e.g., key sequences, same as user ID, etc.) and password history
- Users may voluntarily change their own password at any time
- Users requiring administrative assistance to reset/change their password must be validated by User Identification and Authentication/UIA (web-based private question/answer) system or physical proof of identification
- UIA has been implemented in conjunction with IntraSECURE. Upon initial signon to IntraSECURE, users were directed to the website for UIA and encouraged to enter 3 unique questions and answers that can only be answered by the user. Users will have until January 31, 2001 to complete questions and answers using the UIA application. Beginning February 1, 2001 the ACS Help Desk Staff will require users who forget their passwords to answer a question from UIA. Users who do not complete the questions/answers in UIA by January 31, 2001 will be required to present proof of identification to the ACS Help Desk staff in room 307 of the Hillsborough Building.

AUDIT FINDING 2: SECURITY VIOLATION REPORTING AND AUDIT TRAILS

The PeopleSoft Accounts Payable application currently does not offer security violation logs or readily accessible audit trails to track user access to the system. Certain vendors may be able to supplement the security reporting and audit trails provided by PeopleSoft, Inc.

Security violation reports are detective controls used to identify potentially unauthorized access attempts and to detect suspicious usage activity such as access during non-business hours or access patterns that may indicate impropriety. Without these reports, it is much more difficult to identify and take action on suspicious login or usage activities.

Recommendation: The University should assess vendor product offerings to improve security violation reporting and audit trail features. Once the products are installed, the University should be sure they are effective on the production server running the application at the University.

Auditee's Response: As noted in the response to Recommendation #1 the University has purchased a software product from PentaSafe Security Technologies, Inc. called IntraSECURE which provides improved security to the applications. IntraSECURE's network intrusion reporting capabilities include:

- User ID will be considered "stale" after 90 days of disuse and automatically locked out
- User ID will be automatically disabled after 3 consecutive failed login attempts and designated a break-in victim
- Each failed login attempt and automatic disablement (due to break-in threshold) is logged

AUDIT FINDING 3: LEGACY SYSTEM

The PeopleSoft Accounts Payable application feeds accounting transactions to the PeopleSoft General Ledger. The PeopleSoft General Ledger system, in turn, feeds these transactions to the Financial Accounting System (FAS) which runs on the University's mainframe computer.

During our review of the interface program which feeds the accounting transactions from PeopleSoft to FAS, we noted that the password for an ID which could be used to access the legacy IBM mainframe system is "hard-coded" within the interface program. A disgruntled employee with this knowledge could disrupt processing within the FAS system and unauthorized activity could be difficult to trace.

Recommendation: Administrative Computing Services should minimize the access that this ID could provide to reduce the exposure of the FAS system to attacks.

Auditee's Response: An assessment of the authorization for this ID has been completed. The mainframe security for this ID has been changed to only allow transmittal access to the appropriate files to reduce exposure should this ID be used for an attack.

SYSTEM ADMINISTRATION

The following findings are associated with the administration of the PeopleSoft Accounts Payable application.

AUDIT FINDING 4: SHARED IDENTIFICATIONS

Employees within the Administrative Computing Services section use a shared ID to access the PeopleSoft database where the Accounts Payable system resides. There is currently no

process to track the use of this ID. Access to the database is normally required only in unusual circumstances, such as when data is corrupted or when other errors occur which can not be repaired using the PeopleSoft Application interface. Employees can not access the PeopleSoft database using the identification assigned to them individually.

A shared IDs eliminates the individual accountability for the actions taken using that ID.

Recommendation: The University should consider either assigning access to the database directly to those employees who require it to perform their authorized job functions, or should implement a system to track the usage of shared IDs. Which ever method is chosen, all actions taken while using any ID should be traceable to the individual using the ID.

Auditee's Response: Effective October 30, the manager of the development staff requests that the Financials Security Administrator change the passwords for the shared IDs each time the on-call responsibility rotates to another staff member. The manager only divulges the new passwords to the new on-call person, logging the name of the on-call staff member and the date on which he/she was given the passwords. (The Configuration Manager serves as the backup for the Development Manager for this function.) Additionally, effective January 31, all activity performed using these shared IDs will be logged at the database level for detailed tracking purposes. In this manner, we are able to tightly control those having access to the passwords for these shared IDs, closely track those having access at any given point in time, and closely monitor all operations performed using these IDs.

AUDIT FINDING 5: CONCURRENT SESSIONS

The PeopleSoft application system permits an unlimited number of concurrent sessions (log-ins) by the same user. Also, the network operating system is configured to allow each user to have concurrent sessions at an unlimited number of work-stations.

An owner of the ID may share his/her logon ID and password with another user, allowing that user to process transactions under the owner's identification. This reduces individual accountability for activities performed using this ID.

Recommendation: Administrative Computing Services and Enterprise Information Systems should determine if a user can be limited to a fixed number of work-stations, e.g. three, and implement a policy limiting the number of concurrent sessions through the network operating system and/or through supplemental application security software.

Auditee's Response: Network and Client Services has implemented a limit of three concurrent sessions at the network operating system level for its 1,700 administrative customers.

AUDIT FINDING 6: APPLICATION SYSTEM CHANGES

There is no effective system to ensure that all changes to the PeopleSoft Application System have been reviewed, tested and approved. This situation could result in unauthorized or untested changes to the PeopleSoft application being migrated into production, leading to application processing that is inconsistent with management's intentions.

However, we did note that ACS is in the process of developing and implementing Configuration Management Standards and Procedures to address these (and other) changes to the computer operating environment.

Recommendation: Incorporate within the Configuration Management Standards and Procedures, controls which will provide reasonable assurance that all changes to the PeopleSoft Accounts Payable application have been reviewed, tested and approved. Implement the standards and procedures in the production environment.

Auditee's Response: All changes to the Financials modules must now have appropriate testing with documented approvals from the primary customer(s), the EIS Systems Accountant, the ACS Technical Representative(s), and the Financials Management Team. The necessary approvals are outlined in the Configuration Management Standards and Procedures document and are enforced by the Financials Configuration Manager (i.e. modifications are not implemented in production without the appropriate documentation).

AUDIT FINDING 7: PROJECT DATA

We noted that a number of PeopleSoft Accounts Payable project files which include program narratives, test plans, system specifications and requirements, have not been protected from unauthorized update or deletion. These files are critical to the maintenance and support of the application.

We were informed that a project is underway to address (among other areas) the safeguarding and administration of project data as part of the Configuration Management Standards and Procedures.

Recommendation: Incorporate within the Configuration Management Standards and Procedures, controls which will provide reasonable assurance that all critical project data is adequately safeguarded and properly maintained. Implement the standards and procedures in the production environment.

Auditee's Response: We are incorporating into our Configuration Management Standards and Procedures the process for storing all project data in a consolidated and tightly controlled file space on a network file server. We have begun implementing this process and will have all project data consolidated to one network directory with security access for only designated staff members no later than January 31, 2001.

MANAGEMENT CONTROLS

The following findings are associated with management controls over the Information Technology environment at North Carolina State University.

AUDIT FINDING 8: SEPARATION OF DUTIES

We reviewed the design of controls over the separation of duties and found certain instances where an employee could perform functions which would be better controlled if the transaction authorities were assigned to separate employees.

The PeopleSoft Accounts Payable system allows for the control of accounts payable functions performed by employees. These controls are referred to as "operator classes" as they restrict which functions an operator (employee) may perform. These controls are then further refined through "work flow" which has been in use at NC State preceding PeopleSoft. The University then extended these controls through a PeopleSoft "add on" system referred to as "organizational security". Organizational security is PeopleSoft's terminology for limiting the organizational scope of an employee's transactions.

During our review, the University performed an informal assessment of assigned authorities and revoked those authorities determined to be incompatible.

Recommendation: The University should identify incompatible functions assigned on a regular basis, through the use of computer queries or other means. Also, the University should limit PeopleSoft Accounts Payable authorities to the minimum feasible. If there remain employees assigned incompatible functions, then mitigating controls, such as after the fact reporting, should be designed and implemented.

Auditee's Response: We have removed all capability to add vendors from all Accounts Payable staff with the exception of the two staff members responsible for this function. These two individuals have inquire-only access to vouchers and thus can no longer create payment vouchers.

AUDIT FINDING 9: SECURITY STANDARDS AND PROCEDURES

NC State does not have security standards which address the requirements of operating in a client/server environment. Security administration procedures for the PeopleSoft Accounts Payable application have not been formalized.

Until recent years, all NC State application systems ran on a central IBM mainframe computer. NC State has limited policies that define some security standards over IBM mainframe application systems. However, the transfer of applications outside the IBM platform standard has left the University without comprehensive security standards applicable to the entire University computing environment.

The lack of comprehensive security standards could lead to inconsistent and inadequate implementation of security controls over University applications.

Recommendation: The University should enhance their security standards for the legacy environment to include standards applicable to all University computing platforms.

Auditee's Response: The Vice Chancellor for Finance and Business has charged a campus committee to review, revise, and update the University's Data Management Procedures in a memorandum dated September 25, 2000. The committee will complete their assessment by February 15, 2001 and submit a recommendation to the Vice Chancellor who will forward it to the Chancellor for final approval. Upon approval the revised Data Management Procedures will be posted on the University's web site.

AUDIT FINDING 10: UNIVERSITY BUSINESS CONTINUITY PLAN

The University does not have a comprehensive business continuity plan that would direct the critical operating areas in the event of serious disruptions to their computing capabilities. The University does have a disaster recovery plan for their mainframe data center but does not have one for the client/server environment processing the PeopleSoft applications. The University has begun the development of a continuity plan, however it is not fully developed or functional at this time.

Until recent years, all NC State application systems ran on a central IBM mainframe computer. A contract was signed with ComDisco, Inc. to provide IBM mainframe processing facilities to the University in the event the Universities IBM mainframe was unavailable. We were informed that the University is currently evaluating bids for services for both their client/server environment and their legacy systems. It should be noted that a business continuity plan differs from a disaster recovery plan, as it is focused on how the user community continues their operations under various scenarios, including the loss of a data center.

The lack of a business continuity plan could lead to delays or inadequate reactions to a major disruption of the University's operations.

Recommendation: The University should continue to develop a business continuity plan that addresses the University's needs and develop a disaster recovery plan for the client/server environment. At a minimum the plan should address the following:

- Objective of the plan (for example, continue normal operations, continue in a degraded mode, abort the function as quickly and as safely as possible, and so on)
- Criteria for invoking the plan (for example, missing a renovation milestone, reaching the projected failure date, experiencing serious system failures, and so on)
- Expected life of the plan (how long operations can continue in contingency operating mode)

- Roles, responsibilities and authority

- Plan creation and consideration of resource constraints to plan for each contingency and objective
- Testing of the plan and training on its implementation
- Procedures for operating under the business continuity plan
- Resource plan for operating under the business continuity plan (for example, staffing, scheduling, materials, supplies, facilities, temporary hardware and software, communications, and so on)
- Criteria for returning to normal operations
- Procedures for returning to normal operations
- Procedures for recovering lost or damaged data

Auditee's Response: We will develop business continuity plans for the central offices which depend on the PeopleSoft administrative systems on the Sun E10000 computer to conduct their daily business. These central office business continuity plans will be focused on sustaining the university's administrative business functions in the event of a major failure or unavailability of the client server environment used by the new PeopleSoft administrative systems.

Following completion of business continuity plans for the central offices, specific plans for the continuation of the University's information technology functions will be developed by each campus department for its operation.

DISTRIBUTION OF AUDIT REPORT

In accordance with G.S. § 147-64.5 and G.S. § 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable Michael F. Easley	Governor of North Carolina
The Honorable Beverly M. Perdue	Lieutenant Governor of North Carolina
The Honorable Richard H. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. David T. McCoy	State Budget Officer
Mr. Edward Renfrow	State Controller

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman	Representative James B. Black, Co-Chairman
Senator Frank W. Ballance, Jr.	Representative Martha B. Alexander
Senator Patrick J. Ballantine	Representative E. Nelson Cole
Senator James Forrester	Representative James W. Crawford, Jr.
Senator Wilbur P. Gulley	Representative W. Pete Cunningham
Senator David W. Hoyle	Representative Ruth M. Easterling
Senator Howard N. Lee	Representative Joe Hackney
Senator Fountain Odom	Representative Martin L. Nesbitt
Senator Aaron W. Plyler	Representative Edd Nye
Senator Anthony E. Rand	Representative William C. Owens, Jr.
Senator R. C. Soles	Representative E. David Redwine
Senator Robert G. Shaw	Representative Eugene Rogers
Senator Ed N. Warren	Representative Stephen W. Wood
Senator Allen H. Wellons	Representative Thomas E. Wright

Appointees to the Joint Select Committee on Information Technology

Senator Austin M. Allran	Representative Joe P. Tolson
Senator Charles Carter	Representative Russell Edwin Tucker
Senator Daniel G. Clodfelter	Representative William L. Wainwright
Senator Eric Miller Reeves	Representative Trudi Walend
Mr. Dwight Allen	Mr. Rufus Edmisten
Mr. Curtis Clark	Ms. Diana Oblinger
Ms. Darleen Johns	Ms. Janet Smith

Other Legislative Officials

Representative Phillip A. Baddour, Jr.	Majority Leader of the N.C. House of Representatives
Representative N. Leo Daughtry	Minority Leader of the N.C. House of Representatives
Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

ORDERING INFORMATION

Copies of this report may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Telephone: 919/807-7500

Facsimile: 919/807-7647

E-Mail: reports@ncauditor.net

A complete listing of other reports issued by the Office of the North Carolina State Auditor is available for viewing and ordering on our Internet Home Page. To access our information simply enter our URL into the appropriate field in your browser: http://www.osa.state.nc.us.