STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

NORTH CAROLINA DEPARTMENT OF REVENUE

AUGUST 2008

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

NORTH CAROLINA DEPARTMENT OF REVENUE

AUGUST 2008

STATE OF NORTH CAROLINA
Office of the State Auditor

Leslie Merritt, Jr.,
CPA, CFP
State Auditor

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

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Mr. Reginald S. Hinton, Secretary,
North Carolina Department of Revenue

Ladies and Gentlemen:

We have completed our information systems (IS) general controls audit at the North Carolina Department of Revenue (DOR). The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate Information Systems (IS) general controls at DOR. The scope of our IS general controls audit included general security, access controls, program maintenance, physical security, and disaster recovery. We specifically reviewed access controls to the Revenue Cash Administration (RCA), Electronic Filing for Individual Income (ELF), Data Capture, Electronic Funds Transfer (EFT), Integrated Tax Administration System (ITAS) and Online Filing and Payments (OFP) applications. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary and audit results which detail the areas where DOR has performed satisfactorily relevant to our audit scope, where improvements should be made, and where further study is necessary.

We wish to express our appreciation to the staff of DOR for the courtesy, cooperation and assistance provided to us during this audit.

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

Respectfully submitted,

Leslie W. Merritt, Jr.

Leslie Merritt, Jr., CPA, CFP
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an information system (IS) audit of the North Carolina Department of Revenue (DOR) from January 22, 2008, through April 18, 2008. The primary objective of this audit was to evaluate the IS general controls in place during that period. Based on our objective, we report the following conclusions.

General security involves the establishment of a reasonable security program that addresses the general security of information resources. DOR has established a reasonable security program that addresses the general security of information resources. *Our audit identified two significant weaknesses in general security. See Audit Finding 1: No Written Procedures For The ELF Application, and Audit Finding 2: Improved Record-Keeping And Filing System Needed For Critical Security Documents.*

The **access control** environment consists of access control software and information security policies and procedures. DOR has established controls to govern access to its critical systems, however, the controls in place are not working as intended. *Our audit identified several significant weaknesses in access controls. See Audit Finding 3: Failure To Generate Users Access Capability List, and Audit Finding 4: Poor Management and Record-Keeping of Systems Access To Critical Applications. DOR has employees with access to an Integrated Tax Administration System application function who do not require this access to perform their job duties. This detailed finding has been reported in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18). The other weaknesses that are sensitive in nature have also been conveyed to management in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18).*

Program maintenance primarily involves enhancements or changes needed to existing systems. DOR has established controls to govern maintenance of their critical programs; however, DOR was missing two key controls that would ensure the integrity of programs. *Our audit identified significant weaknesses in program maintenance. See Audit Finding 5: Application Procedures Manual Not Updated and Audit Finding 6: Lack of Source Code Comparison and Retention of Prior Source Code Versions.*

Physical security primarily involves the inspection of the agency's computer center for the controls that should reasonably secure the operations of the computer center from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. DOR has implemented controls to reasonably secure the computer center from fire, water, electrical, and vandalism. *However, our audit identified a significant weakness in environment control of the computer center.* See *Audit Finding 7: Inadequate Environmental Controls In The Server Room.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable DOR to recover from an extended business interruption due to the destruction of the computer center or other DOR assets. DOR has a complete disaster recovery plan, and periodically tests the plan. *However, our audit identified a significant weakness in disaster recovery. See Audit Finding 8: Inadequate Retention Of Disaster Recovery Plan Test Results.*

[This Page Left Blank Intentionally]

OBJECTIVES

Under the *North Carolina General Statutes* 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. IS general control audits are examinations of controls which effect the overall organization and operation of the IS function. This IS audit was designed to ascertain the effectiveness of general controls at DOR.

SCOPE

General controls govern the operation and management of computer processing activities. The scope of our IS general controls audit was to review general security issues, access controls, program maintenance, systems software, systems development, physical security, and disaster recovery which directly affect DOR's computing operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

We audited policies and procedures, interviewed key administrators and other personnel, examined system configurations, toured the computer facility, tested on-line system controls, reviewed appropriate technical literature, reviewed computer generated reports, and used security evaluation software in our audit of application controls. We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

The North Carolina Department of Revenue was created by the General Assembly in 1921. The Department's mission is to administer the state tax laws and to collect the taxes due in an impartial, uniform, and efficient manner. The Department of Revenue is led by the Secretary, Deputy Secretary, and three Assistant Secretaries. The Assistant Secretary for Information Technology is responsible for the Applications Development and Support Division, the Database Administration Division, the Customer Support and Analysis Division, and the Technology Services Division.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where DOR has performed satisfactorily and where recommendations have been made for improvement.

GENERAL SECURITY ISSUES

General security issues involve the maintenance of a sound security management structure. A sound security management structure should include a method of classifying and establishing ownership of resources, proper segregation of duties, a security organization and resources, policies regarding access to the computer systems and a security education program. DOR has established a reasonable security program that addresses the general security of information resources. *Our audit identified two significant weaknesses in general security*.

AUDIT FINDING 1*: NO WRITTEN PROCEDURES FOR THE ELF APPLICATION*

DOR does not have or maintain user or operation manuals for the Electronic Filing for Individual Income (ELF) application. DOR has identified this as a critical application. Users are relying upon other users and processes already in place to operate this application. The absence of user/operation manuals for a critical application at DOR creates a situation in which mistakes are more likely to occur. Also, employees may not follow management's intentions in regards to this application. Mistakes made within a critical application at DOR can have a tremendous impact on the integrity, accuracy, and reliability of the data.

Controls should be in place to ensure that the organization has established adequate policies and procedures and that they are reviewed and updated regularly.

Recommendation: DOR's management should obtain or create the end-user and technical operation manuals for all critical applications. These manuals should be provided to those employees whose job requires access to the ELF application.

Auditee's Response: The ELF system is modified annually for adherence to IRS requirements and North Carolina Individual Income Tax statutes. The DOR technical and functional staff is involved, in detail, with this process. We agree having more thorough end-user and technical operations manuals for the ELF application would be preferable.

AUDIT FINDING 2: IMPROVED RECORD-KEEPING AND FILING SYSTEM NEEDED FOR CRITCAL SECURITY DOCUMENTS

The Department of Revenue's (DOR) current method of filing signed acknowledgment forms for security policies makes it difficult for DOR to locate the forms for employees. DOR could not easily locate the forms we requested for our audit. DOR was still locating forms near the end of our audit. They did finally locate forms for all staff in our sample except for one person.

When investigating the cause for so many missing forms, DOR stated that its current record-keeping practices allowed for the discarding of these signed documents. However, we could not substantiate this claim through their current policies.

According to the Department of Cultural Resources and the Department of Revenue's own policies, DOR must improve its recordkeeping standards for the aforementioned forms:

1. Cultural Resources Records Retention Policy (ITEM G32 Policies, Procedures, and Regulations File) states that management should retain reference copies of all its policies, procedures, and regulations. The disposition instructions for these documents states that they may only be destroyed, in office, when they are superseded or obsolete.

2. DOR's policies, relating to the aforementioned forms states that:

    - Employees are required to attend the Policy Awareness Communication Experience in Security (PACES) security awareness training program annually and sign related acknowledgement forms.
    - Employees are required to read DOR's Internet Usage Policy and sign a "read and understood" statement.
    - Employees must acknowledge reading the Internal Security Policy by signing a "read and understood" statement.
    - Employees are required to sign an acknowledgment form indicating that they have read and understood the policies pertaining to the Confidentiality of Tax Information and the Security Access Card.

Recommendation: Management at DOR should instruct staff in the use of existing policies that require these forms to be retained. Management should investigate the implementation of another means of filing these forms to ensure ease of retrieval.

Auditee's Response: DOR takes the protection of taxpayer information extremely seriously and continually strives to ensure adherence to all State and Federal guidelines with regard to security policies and record keeping. DOR staff located the forms referenced as missing with minimal difficulty, once a list of the missing forms was provided. Due to organizational changes, policy changes and filing procedures, some of these forms were not all in the same location. DOR does have a record-keeping and filing system for retaining security related documents requiring signature and this system is used for all forms that have been signed since the system was implemented. Efforts are ongoing to ensure that all historical

documents are included in the system as well. All employees, including management, are reminded of the requirements for obtaining and retaining the required security forms on an annual basis. The agency has a documented supervisor's checklist, which includes these requirements. This process also extends to contractors and other non-employee personnel that may require access to the DOR facility and information systems. A database for recording and storing the images of these forms has been under development and is being used in a pilot-mode to determine what additional requirements need to be included.

DOR does agrees that the adherence to the records retention policy regarding security related forms is critical and that it is appropriate that we continually instruct staff in the use of existing policies regarding security forms.

ACCESS CONTROLS

The most important information security safeguard that DOR has is its access controls. The access controls environment consists of DOR access control software and information security policies and procedures. An individual or a group with responsibility for security administration should develop information security policies, perform account administration functions and establish procedures to monitor and report any security violations. *Our audit identified several significant weaknesses in access controls. DOR has employees with access to an Integrated Tax Administration System application function who do not require this access to perform their job duties. This detailed finding has been reported in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18). The other weaknesses that are sensitive in nature have also been conveyed to management in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18).*

AUDIT FINDING 3: FAILURE TO GENERATE USER ACCESS CAPABILITY LIST

The Department of Revenue could not generate a list to show user's access capabilities to the RCA, ELF, and OFP applications. Without this list, DOR cannot determine a user's true access. This makes it difficult to determine if a user has more access to the application than intended.

According to Control Objectives for IT (COBIT) DS5 (Ensure Systems Security) section 5.9 (Central Identification and Access Rights Management), controls should be in place to ensure that users identification and access rights are appropriately established and managed in a unique and central manner to obtain consistency and efficiency of global access control.

Recommendation: DOR should explore options within the applications that will allow them to generate an access rights report for each user, and use this report to ensure users have appropriate access to the application.

Auditee's Response: DOR does not currently have the ability to generate a single list. However, we are able to determine who has what access. DOR agrees that having an easier methodology would be ideal.

AUDIT FINDING 4: POOR MANAGEMENT AND RECORD-KEEPING OF SYSTEM ACCESS TO CRITICAL APPLICATIONS

DOR developed a process to centralize authorization of access to its critical system. As a part of this process, DOR uses a form to authorize and document DOR user access at various security levels. This form is also used to document the supervisor's approval of access and any future changes to a user's access because of changes in job duties or terminations. We found several weaknesses in the form and in this process. More specifically, we found the following:

- The access rights forms do not sufficiently define the level or access a user actually needs to a particular system for some applications.
- Some forms could not be found and as a result we could not verify whether the user should have actually received access to a system.
- Supervisors often use email to show approval of access. These emails were lost or discarded. Many users' forms show no supervisor approval of access.
- The recordkeeping practice for user access forms was not in accordance with the Department of Cultural Resources retention policy, and some user's forms were not appropriately retained
- User forms are not being recertified when a change occurs to the user's job functions or at least annually for all users. This increases the risk that users have excessive access to system resources.

We tested this process for access to the following critical applications, OFP, RCA, Data Capture, ITAS, EFT and ELF applications, and found these weaknesses existed for access to all of these applications.

Control Objectives for IT (COBIT) DS5 (Ensure Systems Security) section 5.5 (Management Review of User Accounts) states that management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risks of errors, fraud, misuse, or unauthorized alteration.

Recommendation: DOR Management should re-vamp this process to ensure that centralized management of access is controlled, monitored, and well-documented to prevent unauthorized or excessive access to DOR critical systems.

Auditee's Response: DOR has strong access control policies in place and additionally has supporting confidentiality and disclosure agreements with all employees that further serve to protect the confidentiality of taxpayer information. Because of the criticality of the public trust, DOR agrees that it is appropriate to always look for improvements in these processes and agrees that a review of the current system access and record-keeping process is appropriate and will be done.

PROGRAM MAINTENANCE

Program maintenance consists of making changes to existing application systems. Programmers should follow program change procedures to ensure that changes are authorized, made according to specifications, properly tested, and thoroughly documented. Application programmers should be restricted to a test environment to ensure that all changes to production resources are tested and approved before moving the changes into production. Changes to application system production programs should be logged and monitored by management. *Our audit identified significant weaknesses in program maintenance.*

AUDIT FINDING 5: APPLICATION PROCEDURES MANUAL NOT UPDATED

DOR's Application Development Procedures manual has not been updated since July 2004. Failure to keep procedures manuals updated for the maintenance of a critical application increase the risk of errors in maintenance.

The National Institute of Standards and Technology (NIST), indicates organizations should develop, disseminate, and periodically review all policies that address the purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities. This includes procedures manuals.

Recommendation: Management should update the Application Development Procedures manual, as well as, any other critical manuals to ensure that information contained within the manuals remain relevant and accurately reflect the processes at the Department of Revenue.

Auditee's Response: DOR agrees that the Application Procedures Manual should be reviewed and periodically updated.

AUDIT FINDING 6: LACK OF SOURCE CODE COMPARISON AND RETENTION OF PRIOR SOURCE CODE VERSIONS

DOR programmers for the OFP, RCA, and ELF applications do not routinely compare current source codes to previous versions of the source code to ensure that no unauthorized changes have been made. In addition, DOR programmers do not retain prior versions of the ITAS and EFT source codes, making it impossible to perform comparison checks with a revised version to identify any unauthorized changes.

The National Institute of Standards and Technology indicates organizations should monitor changes to information systems to determine the effects of changes made to applications. Also the organization should employ integrity verification on applications to look for evidence of information tampering, errors, and omissions. The organization should employ good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, and cryptographic hashes) and use tools to automatically monitor the integrity of the information system and the applications it hosts.

Recommendation: Management should review the current program source code with the original version of the source code to identify any unauthorized changes made. In addition, management should begin using a version control system, such as Endeavor, for ITAS and EFT to ensure that all versions of these applications are retained, thereby promoting both integrity and auditability of the application.

Auditee's Response: DOR agrees that the Department does not do source code comparisons for the mainframe applications. DOR has the ability to perform source code comparisons for its distributed environment applications. The tool provided by ITS, ENDEVOR, to manage source code for the mainframe environment will not support the ITAS source code due to the metacobol objects and other constraints. As additional information, the ITAS application was a transfer system and is more than 20 years old. The ITAS system is anticipated to be replaced over the next 3-4 years and it is the intent of the Department to ensure that a tool is available to provide for source code comparison.

PHYSICAL SECURITY

Controls over physical security are designed to protect a computer center from service interruptions resulting from fire, water, electrical problems, vandalism, and other causes. DOR's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. *Our audit identified a significant weakness in physical security during our audit.*

AUDIT FINDING 7: SERVER ROOM IS BEING USED AS A STORAGE ROOM

The Department of Revenue's (DOR) server room is being used as a storage warehouse facility for pallets of computer equipment. Because of the sensitive nature of information contained on servers within this room, DOR should only use this room as it was originally intended. The equipment that is stacked on palettes' in this room is moved around and shifted to different locations using a pallet jack by DOR employees who would not normally need access to the server room. This increases the risk that existing computer equipment could be damaged by the pallets of equipment or the pallet jack needed to move the pallets of equipment around the computer room. The pallets are wrapped in flammable materials, such as cardboard and plastic. This introduces an unnecessary fire hazard into this secure server room.

Control Objective for IT (COBIT) states that management should have controls in place to ensure that the organization has established adequate security over the physical environment that houses its critical servers and infrastructure.

Recommendation: DOR's management should find an alternate location in which to store computer equipment. This type of equipment could be stored in a separate storage room or warehouse.

Auditee's Response: The storage of computer equipment in the DOR computer room is due to the need to provide a climate controlled environment. The bulk order process of ITS necessitates the purchase of a large quantity of hardware at several intervals throughout the year. DOR does not have sufficient climate controlled space to store this equipment that has sufficient security and round-the-clock staffing, other than the computer room. It should be stated that the area referenced is not just a server room, but a full scale, raised-floor, specially equipped floor space specifically for computer operations. Manual fork-lifts are used on this floor to move heavy equipment on a normal basis. While the storage of PCs in their original shipping boxes is not ideal, it has not posed a security or physical risk to the computing operations. Only authorized personnel have access to the computer room and no one has access to the room for purposes of accessing the stored equipment that would not have access otherwise. DOR would very much like to have the luxury of separate storage areas or to have on-demand delivery of PC equipment, but neither of these options are available at this time.

DISASTER RECOVERY

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, DOR's daily operations would be interrupted. To reduce this risk, computer service centers develop business continuity plans. Business continuity procedures should be tested periodically to ensure the recoverability of the data center. *Our audit identified a significant weakness in disaster recovery.*

AUDIT FINDING 8: INADEQUATE RETENTION OF DISASTER RECOVERY PLAN TEST RESULTS

Although DOR conducts bi-annual tests of its disaster recovery plan, DOR was unable to provide documentation to show the results of such tests. DOR stated that Information Technology Services, their third party provides a check list which documents the jobs run during the disaster recovery test, and their successful completion. However, DOR disposed of this check list once the restoration tests were completed and the disaster recovery exercise was finished. As such, DOR did not follow the retention policy set forth by the Department of Cultural Resources for Disaster Recovery documentation.

In its guidance the Cultural Resources Records Retention Policy (ITEM G14), requires an agency to retain Emergency Management files until they are superseded or obsolete. It defines Emergency Management Files as records concerning evacuations, preparations for disasters, and operations in the event of disasters. This includes disaster recovery test results.

Recommendation: DOR's management should obtain and retain test results of its Disaster Recovery Plans until another test supersedes the need to keep the prior test.

Auditee's Response: DOR has routinely executed disaster recovery tests of the technical ITAS environment at least semi-annually for the past 10 years. The processes used for these test are largely automated and reports have not typically been printed. Rather, results are verified through hands-on verification. DOR will, in the future, generate sufficient reports to record the successful completion of the tests and will retain these reports per state policy.

ORDERING INFORMATION

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

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

Telephone: 919/807-7500

Facsimile: 919/807-7647