STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

EMPLOYMENT SECURITY COMMISSION

NOVEMBER 2008

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEMS

GENERAL CONTROLS

EMPLOYMENT SECURITY COMMISSION

NOVEMBER 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. Harry E. Payne, Jr., Chairman
North Carolina Employment Security Commission

Ladies and Gentlemen:

We have completed our information systems (IS) general controls audit of the Employment Security Commission (ESC). 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 ESC. 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 UI Benefits and UI Tax 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 ESC 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 ESC 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

PAGE

EXECUTIVE SUMMARY

We conducted an information systems (IS) audit of the Employment Security Commission (ESC) from April 15, 2008, through July 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. ESC has established a reasonable security program that addresses the general security of information resources. Our audit identified three significant weaknesses in general security. *See Audit Finding 1: Unauthorized Software Monitoring, Audit Finding 2: Naming Convention Standards Not Adopted, and Audit Finding 3: Employee Security Forms Not Signed.*

The **access control** environment consists of access control software and information security policies and procedures. ESC has established controls to govern access to its critical systems however, the controls in place are not working as intended. Our audit identified one significant weakness in access control. *See Audit Finding 4: System Access Record-keeping Needs Improvement.*

Program maintenance primarily involves enhancements or changes needed to existing systems. Our audit identified several significant weaknesses in program maintenance. *See Audit Finding 5: Programmers Have ALTER Access to Critical/Sensitive Production Back-up Files, Audit Finding 6: Program Change Testing Results Not Retained, and Audit Finding 7: Inadequate Change Control Policies and Procedures .*

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. ESC has implemented controls to reasonably secure the computer center from fire, water, electrical, and vandalism. However, our audit identified a significant weakness in environmental control of the computer center. See *Audit Finding 8: Data Backup Equipment is Subject to Water Damage.*

A complete **disaster recovery** plan that is tested periodically is necessary to enable ESC to recover from an extended business interruption due to the destruction of the computer center or other ESC assets. ESC has a complete disaster recovery plan, and periodically tests the plan. However, our audit identified a significant weakness in disaster recovery. *See Audit Finding 9: Disaster Recovery Test Results Not Adequately Documented.*

[This Page Left Blank Intentionally]

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

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 ESC.

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, physical security, and disaster recovery which directly affect ESC'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 Employment Security Commission was created as the Unemployment Compensation Commission by the General Assembly in a special session on December 16, 1936. The name was changed by law to Employment Security Commission effective April 1, 1947. Originally established as a three-member body, it was changed to a seven-member commission effective July 1, 1941.

The Commission's mission is to promote and sustain the economic well being of North Carolinians in the world marketplace by providing high quality and accessible workforce-related services.

The Employment Security Commission is led by the chairman, two deputy chairmen, two deputy commissioners and three directors.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where ESC 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. ESC has established a reasonable security program that addresses the general security of information resources. *Our audit identified three significant weaknesses in general security*.

AUDIT FINDING 1: UNAUTHORIZED SOFTWARE MONITORING

Although ESC has addressed the unauthorized installation of copyright software in its policy, ESC does not have a monitoring mechanism for detecting a breach of this policy. Upper level management decided to allow departmental managers to authorize software installation on agency computers.

Unauthorized software installed on agency computers increases the risk that agency personnel can introduce malicious code, malware, or viruses in the ESC environment, and violate copyright laws and license agreements. By not restricting and monitoring software installations on agency computers, the integrity of information maintained on these computers could become vulnerable, thus causing a Personal Identification Information (PII) exposure or subjecting ESC to a potential lawsuit because of copyright or license agreement violations.

Management should review and verify on a regular basis that only authorized software is present on agency computers. Errors and deviations should be reported, acted on and corrected.

Recommendation: ESC should establish a monitoring mechanism for detecting the unauthorized installation of copyrighted or personal software.

Auditee's Response: As stated in Audit Finding 1, ESC upper level management decided to allow departmental managers to authorize software installation on agency computers. Thus, such installations are authorized.

The audit finding goes on to say, "Unauthorized software installed on agency computers increases the risk that agency personnel can introduce malicious code, malware, or viruses in the ESC environment, and violate copyright laws and license agreements." ESC has the State mandated standard antivirus software, Trend Micro, installed on every PC to detect, quarantine and eradicate malware, viruses, and other forms of malicious code.

ESC will investigate the availability, cost and effectiveness of software monitoring tools.

AUDIT FINDING 2: NAMING CONVENTION STANDARDS NOT ADOPTED

Although ESC uses naming conventions within its organization, ESC has not adopted a standard for naming conventions because the policy for naming conventions is still in draft form.

This could cause inconsistent application of naming critical data throughout the organization. Inconsistent application of naming conventions makes it harder to implement data classification and implement appropriate assignments to the data. For example, data files containing social security numbers should be properly identified using a consistent naming convention so that only appropriate and authorized access is assigned to the data.

Naming conventions should be formally adopted and approved by agency management. These standards should be a part of the application development standards of the organization. These standards should include software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing.

Recommendation: ESC should reprioritize its completion of Chapter 9 of the Technical Manuals Guide to provide consistent use of a naming convention throughout the organization. This would allow quick detection of breaches to sensitive data, appropriate access to data, and consistency throughout the organization.

Auditee's Response: The IS Director has met with the Deputy Chairman to request the resources necessary to complete Chapter 9 of the Technical Guide and establish a plan for prioritizing changes in accordance with the availability of funds and staff resources. The request has been approved.

AUDIT FINDING 3: EMPLOYEE SECURITY FORMS NOT SIGNED

ESC requires employees to sign form NCSA-01 "Certification for Completion of Security Training" to show that employees read and understood ESC's internal security policies, and to provide evidence that employees acknowledge this understanding annually. However, ESC has not been enforcing this policy. We found that several employees in our sample had not recently signed the form as of the date of our audit request.

By obtaining employee's signatures on the NCSA-01 form, ESC reduces its liability if an employee violates any items covered by this certification. The items covered by this one certification are as follows:

- Acknowledgement that ESC employees have read and understood the ESC security policy,

- Alcohol- and drug-free workplace policy and,
- Emergency evacuations plans.

According to the Employment Internal Security handbook, each employee must sign this form to evidence and acknowledge that they have read and understood critical security policies, procedures, and training. Also, this form should be signed annually.

Recommendation: ESC should enforce its policy by ensuring that all employees have completed the security training and have signed the NCSA-01 form.

Auditee's Response: ESC does require employees to sign form NCSA-01 "Certification of Completion of Security Training" as a component of the PMP process. All of the required certification forms, including the NCSA-01, are required to be forwarded to the HR Department along with the PMPs. Since 2001, every year ESC issues an HR Bulletin stating that the security form is required.

HR has the responsibility for logging in the PMPs and all associated forms on, or before, June 30 of the given year. If the "forms package" for an employee is incomplete, it is the responsibility of the HR Department to follow up with the appropriate manager(s) to secure the necessary documents.

At the time of the audit, HR was in the process of working through these submittals. Several forms requested by the auditors were signed on the date of the request. It is normal, and expected, that HR requests signature and submittal of any missing forms as such forms are identified.

ACCESS CONTROLS

The most important information security safeguard that ESC has is its access controls. The access controls environment consists of ESC's 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 a significant weaknesses in access controls.*

AUDIT FINDING 4: SYSTEM ACCESS RECORD-KEEPING NEEDS IMPROVEMENT

ESC developed a process to centralize authorization of access to its critical systems. As a part of this process, ESC uses a form to authorize and document ESC 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 this process:

- No evidence of supervisor approval. We found one employee granted herself access to the system.

- The user's access form did not support the actual access granted to the system. Thus, in some cases users may have been granted access to information that they do not need for their current job responsibilities.

A user's access to computer systems should be approved by someone at a higher level in the organization than the employee requesting the access. 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: ESC 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 ESC critical systems.

Auditee's Response: Records of the request for access to ESC systems, Network User Requests (NURs), the supervisory approval for access and the response to the request for access are kept for ESC employees. NURs are not used for employees of external entities. Depending on the date of the request, the supporting documentation for requests by such entities may be in either electronic or hardcopy format.

The supporting evidence for AUDIT FINDING 4 cited a specific case:

1. Employee – NUR submitted by individual for herself

The request was sent via e-mail on March 17, 2003. The ESC Help Desk responded on March 18, 2003, "CANNOT SUBMIT FOR SELF – PLEASE HAVE MANAGER RESUBMIT".

As an additional measure to eliminate the potential for "access carryover" in instances where employees move from one job to another job within the Agency, ESC implemented Executive Bulletin 05 (08) on July 15, 2008. This bulletin states: **"**Staff Separation**:** Managers must immediately revoke the password for any employee leaving their cost center by entering an erroneous password five (5) times. This should be done for mainframe, network and e-mail accounts. Within 8 business hours of occurrence, managers must submit NUR's for all personnel (this includes Intermittents, Partners and Contractors) who leave a cost center and are not expected back within a 90-day period."

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 several significant weaknesses in program maintenance.*

AUDIT FINDING 5: PROGRAMMERS HAVE ALTER ACCESS TO CRITICAL/SENSITIVE PRODUCTION BACK-UP FILES

During our test of Access Controls, we found several programmers had access to the overpayments back-up production files. According to the ESC technical guidance manual, no programmer should have access to modify, delete, or alter production data, except for emergency changes. Because programmers have sufficient knowledge regarding the programs that produce the data, industry best practices dictate that good separation of duties in the IT area would restrict a programmer's access to the production data.

Recommendation: ESC Management should limit programmer access to production data.

Auditee's Response: As stated in the ESC Technical Guidance Manual, no programmer should have access to modify, delete, or alter production data, except for emergency change. Current ESC policy and change control practices do not allow such access. The auditors located an instance in which this policy was not adhered to. That access was the result of an artifact from a process that has been obsolete for many years. The "Alter" access described in this finding has been changed to "Read" for all staff effective September 5, 2008.

AUDIT FINDING 6: PROGRAM CHANGE TESTING RESULTS NOT RETAINED

ESC does not document and retain the results of the testing of program changes. Management could not provide evidence that program changes were tested and approved by both the user and the IS department. Programmers did not adhere to their draft Change Control Policies and Procedures, or NC ITS policies when making program changes. Required forms and other documentation could not be provided.

By not adhering to change control policies and procedures, programmers could make changes to programs that are not approved or that could potentially be used to corrupt critical data or misappropriate resources. In addition, by not completing and retaining the required documentation, inappropriate changes made to programs could go undetected.

The testing results for program changes should be documented and retained. Additionally, NC SCIO Policies, Chapter 8, Section 1.080205 requires "successful testing of …updates prior to their being moved into a live environment."

Recommendation: ESC should retain the results of testing and approval of program changes.

Auditee's Response: Test results from major systems testing conducted in cooperation with the SQA group at ITS are retained within the tool.

AUDIT FINDING 7: INADEQUATE CHANGE CONTROL POLICIES AND PROCEDURES

ESC has inadequate Change Control Policies and Procedures. ESC does have a draft document that satisfies the requirements noted below, but this document is incomplete and has not been implemented. This document is used as a technical reference guide for programmers, and provides guidance for initiating, documenting, and gaining approval for program changes.

By not providing guidance in the form of a standardized process for all employees to follow, there could be a lack of continuity in the manner with which program changes are processed. By not clearly stating the required documentation and approvals, personnel could process change without maintaining a sufficient audit trail.

Agencies should have formal change control policies and procedures that are approved by management. These policies and procedures should be implemented for the whole agency.. Additional guidance is provided by North Carolina State Chief Information Officer Policies, Chapter 1.080205, Managing Change Control Procedures.

Recommendation: ESC should finalize and implement the policies outlined in this document.

Auditee's Response: The IS Director has met with the Deputy Chairman, to request the resources necessary to finalize and implement the draft Change Control Policies and Procedures document in accordance with the availability funds and staff resources. The request has been approved.

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. ESC'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 8: DATA BACKUP EQUIPMENT SUBJECT TO WATER DAMAGE

The computer center is located on a floor below ESC's cafeteria. Critical data backup equipment resides directly under a vending machine located in the cafeteria area. ESC indicated that the vending machine has had water leaks in the past that have drained onto this data back-up equipment. If a water leakage occurs, the critical data backup equipment could be damaged and crucial information could be lost.

According to ESC IT personnel, the cost of moving the data backup equipment to a different location was equivalent to purchasing new equipment. Therefore, ESC believes it is not cost effective to move the equipment from its current location.

An agency's computer center should be adequately protected from environmental hazards.

Recommendation: ESC staff should move the vending machine, which is located in the cafeteria, to another location that does not affect the computer center on the floor below.

Auditee's Response: The recommendation associated with this finding has been forwarded to ESC management, including the Support Services Director (who is responsible for facilities management).

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, ESC'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 9: DISASTER RECOVERY TEST RESULTS NOT ADEQUATELY DOCUMENTED

The test of the Disaster Recovery Plan provided to us by ESC and conducted by ITS fails to address the specific tests and/or results performed for the ESC applications maintained by ITS. ESC did not specifically have ITS document its test of results during the Disaster Recovery test. By failing to know the specific test results conducted on the ESC mainframe, management might not be aware of the issues that might influence the recovery process in the event of a disaster and it may be difficult to ascertain if the ESC IT applications can effectively recover from a disaster.

Disaster recovery plans should be tested on a regular basis and the results of the test should be adequately documented.

Recommendation: ESC and ITS should develop a document that specifically reports the results of ESC Application restorations.

Auditee's Response: The IS Director has discussed the need for detailed documentation for future disaster recovery tests with Deputy State CIO, and has been assured that the requested documentation will be provided for upcoming tests.

[This Page Left Blank Intentionally]

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 July 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