STATE OF
NORTH CAROLINA

AUDIT OF THE FOOD STAMP INFORMATION SYSTEMS
APPLICATION CONTROLS

DEPARTMENT OF HEALTH AND HUMAN SERVICES
DIVISION OF SOCIAL SERVICES

MARCH 2008

OFFICE OF THE STATE AUDITOR
LESLIE W. MERRITT, JR., CPA, CFP
STATE AUDITOR

AUDIT OF THE FOOD STAMP INFORMATION SYSTEMS APPLICATION CONTROLS

DEPARTMENT OF HEALTH AND HUMAN SERVICES DIVISION OF SOCIAL SERVICES

MARCH 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.osa.state.nc.us

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Mr. Dempsey Benton, Secretary,
North Carolina Department of Health and Human Services

Ladies and Gentlemen:

We have completed our information systems (IS) application audit at the Department of Health and Human Services, Division of Social Services. The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate controls for the Food Stamps Information System (FSIS) application. The scope of our audit was to review the application controls for the FSIS application. Application controls for the FSIS application systems include data completeness, data accuracy, data validity, and data authorization. The purpose of application controls is to ensure that as data passes through the FSIS application, it is complete, accurate, valid, timely, and it is protected from unauthorized access.

This report contains an executive summary that highlights the areas where the Department of Health and Human Services, Division of Social Services, has performed satisfactorily relevant to our audit scope and where improvements should be made.

We wish to express our appreciation to the staff at the Department of Health and Human Services, Division of Social Services, 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 Department of Health and Human Services (DHHS), Division of Social Services (DSS), from November 08, 2007, through January 18, 2008. The primary objective of this audit was to evaluate controls for the Food Stamps Information System (FSIS) application. The critical application controls that we tested in this application review are: (a) data completeness, (b) data accuracy, (c) data validity and (d) data authorization. Our conclusions for the application review of the FSIS application are organized into these four categories. Based on our objective, we report the following conclusions.

Data completeness controls are designed to ensure that all transactions are entered into the system once and only once, that all errors are corrected without any being lost, duplicated or added, that all transactions are processed, that databases are updated completely, and that all output reports are complete. Our audit identified a significant weakness in the completeness controls for the FSIS application. *Audit Finding # 1: No SAS 70 Report for a Third Party Vendor*

Data accuracy controls ensure that the details of transactions are entered and processed correctly, and that printed output is not distributed to the user until it is checked for reasonableness. Our audit identified significant weaknesses in accuracy controls for the FSIS application. *Audit Finding # 2: Lack of Program Change Controls and Audit Finding # 3: Lack of Program Run Books, Programmer's Manual or Restart Procedures*

Data Validity ensures the data entered into the application is valid. Data is compared with the type of data that should be properly included in each input field. In addition, a division of roles and responsibilities should exist, which should exclude the possibility for a single individual subverting a critical process. Our audit identified a significant weakness in the data validity for the FSIS application. *Audit Finding # 4: Lack of Segregation of Duties in the Recording and Approval of Applications through the FSIS System*

Data Authorization controls are designed to ensure that access to data is appropriate and authorized and that access is granted on a need to know, need to use basis. The access control environment should consist of access control software and information security policies and procedures that are implemented appropriately to protect the application data. *Audit Finding # 5: Information Leakage on Internet Webpage, Audit Finding # 6: Inadequate Review of UAudit and Excessive Activity Reports, and Audit Finding 7: Lack of Source Code Comparison*

[This Page Left Blank Intentionally]

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 ascertain the effectiveness of application controls at the Department of Health and Human Services, Division of Social Services.

SCOPE

Application controls govern whether the design of the critical application control supports management's financial statement assertions and that the controls are functioning effectively. The scope of our IS application controls audit was to review application controls which directly affect the Division of Social Services' FSIS application. Other IS access control topics were reviewed as considered necessary.

METHODOLOGY

We audited policies and procedures, interviewed key administrators and other personnel, examined system configurations, tested on-line system controls, reviewed appropriate technical literature, and reviewed computer generated reports 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]

North Carolina has a federally mandated, state-supervised, and county administered, social services system. This means the federal government authorizes national programs and a majority of the funding and the state government provides oversight and support, but it is the 100 local county departments of social services that deliver the services and benefits.

Department of Health and Human Services

In North Carolina, the single administrative agency providing oversight and support is the North Carolina Department of Health and Human Services (DHHS). This umbrella agency has evolved over time and now includes separate divisions. One of the DHHS divisions is the Division of Social Services.

Division of Social Services

The Division of Social Services (DSS) provides application programming and support, security, training, technical assistance, and consultation to the local staff who work in programs for families and children including Child Welfare, Family Support, Work First, Child Support, and Food and Nutrition Services (Food Stamps).

The Food Stamp Information System

The Food Stamp Information System (FSIS) maintains information regarding individuals applying for and receiving Food and Nutrition Services (Food Stamps). The county division of social services case-workers take in and process applications, and enter information into the application to determine both eligibility and the amount of Food Stamps benefits the client will receive. FSIS also generates multiple reports to ensure the completeness, accuracy, and validity of the data processed. The report logs, notices, claims, and issuances are utilized by the client, county DSS, DHHS, and the Federal government to ensure that the Food and Nutrition Services program is run efficiently and effectively.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where The Department of Health and Human Services, Division of Social Services, has performed satisfactorily and where recommendations have been made for improvement.

APPLICATION CONTROLS

Application reviews consist of determining whether the design of the critical application control supports management's financial statement assertions and that the controls are functioning effectively. These reviews are performed when the auditor intends to rely on an application system control to reduce the amount of substantive testing of details required before rendering an opinion on the financial statements.

DATA COMPLETENESS

Data completeness controls are designed to ensure that all transactions are entered into the system once and only once, that all errors are corrected without any being lost, duplicated or added, that all transactions are processed, that databases are updated completely, and that all output reports are complete. Our audit identified a significant weakness in completeness controls for the FSIS application.

AUDIT FINDING 1: NO SAS 70 REPORT FOR A THIRD PARTY VENDOR

DHHS management failed to require Oberthur, an EFunds subcontractor, to submit a SAS 70 report for review. In addition, an internal control evaluation of Oberthur's operations was not included in the EFunds SAS 70 report. Because Oberthur is responsible for manufacturing the food stamp EBT cards and mailing the cards to recipients, DHHS should review the internal controls over this process. Failure of a third party vendor to submit a SAS 70 report could result in undetected fraud. Additionally, completeness and accuracy of their process cannot be adequately assessed.

The status of each external service provider's internal controls should be assessed by management. External service providers' compliance with legal and regulatory requirements and contractual obligations should be confirmed by management. This can be provided by a third-party audit or obtained from a review by management's internal audit function.

Recommendation: If Oberthur continues to perform the services they currently perform for EFunds, DHHS' management should request a SAS No. 70 report from Oberthur or ensure that the EFunds vendor makes provision for Oberthur in its SAS No. 70 report. If Oberthur just generates the food stamp cards without having access to the recipients account information and returns the card stock to EFunds to be mailed, then Oberthur would not be subject to the SAS 70 requirement.

Auditee's Response: We do not believe that this is a valid finding. The Department appropriately requested and received a SAS No.70 report from EFunds, the contractor. In terms of the EFunds subcontractor, Oberthur, the Federal Register, Vol. 65, No. 40, February 29, 2000, page 10677 cites an exemption and states *"Subcontractors providing other services, such as EBT Help Desk Services, Point of Sale installation, or plastic cards are not subject."* Thus, it appears that a SAS No.70 report is not required by Federal regulations. However, the Department will further review this situation and will consider requiring the contractor to provide a SAS No. 70 report for any of its subcontractors in future contracts. The Department does hold the contractor, EFunds, responsible for complying with the terms of the contract, adequate controls and compliance with Federal regulations.

Auditor's Note: The EFunds subcontractor, Oberthur, provides more services than plastic card generation. EFunds has also delegated to Oberthur the task of mailing the food stamp EBT cards to the food stamp recipients. EFunds sends Oberthur recipient account information, which includes the recipient's name, address, card verification code, and the EBT card number, which is tied to the recipient's case number. At this point, Oberthur not only has custody of the EBT card, but the card can be activated by anyone that has physical possession of the food stamp card. Without a SAS No.70, there is no assurance that adequate controls are in place to minimize the potential for fraud.

DATA ACCURACY

Data accuracy controls ensure that the details of transactions are entered and processed correctly, and that printed output is not distributed to the user until it is checked for reasonableness. Our audit identified significant weaknesses in data accuracy controls for the FSIS application.

AUDIT FINDING 2: LACK OF PROGRAM CHANGE CONTROLS

DHHS does not enforce segregation of duties for program changes. In several instances, the person making a change to a program was also the person who approved the change. Consequently, programmers are able to implement changes to the production environment through Endeavor without any secondary approval. Additionally, the agency does not maintain an adequate audit trail of the program change request by the user, approval of the change to be made, program change made by the programmer, and approval of the program change prior to putting into production by another programmer. The information is either hard to obtain or is retained within the system for a few days. As a result, unauthorized changes in applications, including FSIS, could go undetected. This could have a material impact on the Food Stamp Information System.

All changes, including emergency program maintenance and patches, relating to infrastructure and applications within the production environment should be formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) should be logged, assessed, and authorized prior to implementation and reviewed against planning outcomes following implementation.

In addition, DHHS policy states that an audit trail should include sufficient information to establish what events occurred and who (or what) caused them. The policy also states that audit logs should be retained for a period specified by the system owner (typically one year) unless otherwise specified by federal or state regulations.

Recommendation: Management should review its policies and procedures for program changes made to the application software. Management should maintain a system whereby it is possible to determine who made and who approved changes to the application software.

Auditee's Response: The Department of Health and Human Services concurs with the finding. DIRM staff (Endeavor team) will implement the changes to the Endeavor to incorporate the appropriate controls with a quorum of two. This control will prohibit any FSIS staff from approving a package they have created. Audit trail request by the user, approval of the change, and implementation is tracked by the QA Track Record application used by both IT and client entities.

AUDIT FINDING 3: LACK OF PROGRAM RUN BOOKS, PROGRAMMER'S MANUAL OR RESTART PROCEDURES

DHHS was not able to provide program run books, a programmer's manual, and restart procedures for the FSIS application. Without the aforementioned, critical knowledge of how to run the FSIS application is not thoroughly documented for new programmers. If experienced programmers leave the agency, transfer of knowledge of the application will be limited, and unnecessary errors may be made and these errors may not be corrected in an accurate or a timely manner.

ITS policy states that whether the system is developed or updated by in-house staff or by a third-party vendor, agencies should ensure that each new or updated system includes adequate system documentation. Agencies should create, manage, and secure system documentation libraries and should restrict access to authorized personnel only. Agencies should ensure that system documentation is readily available to support the staff responsible for operating, securing, and maintaining new and updated application systems.

Recommendation: Management should create and maintain program run books; a programmer's manual and application restart procedures to promote an adequate transfer of knowledge of the FSIS application.

Auditee's Response: The Department of Health and Human Services concurs with the finding. The FSIS application team will develop and maintain program run books, programmers manual and restart procedures. The documents will be restricted to the appropriate personnel, and will be made available no later than June 30, 2008.

DATA VALIDITY

Data Validity ensures the data entered into the application is valid. Data is compared with the type of data that should be properly included in each input field, for example, only letters should be in a name field. In addition, a division of roles and responsibilities should exist, which should exclude the possibility for a single individual subverting a critical process. Our audit identified a significant weakness in the data validity for the FSIS application.

AUDIT FINDING 4: LACK OF SEGREGATION OF DUTIES IN THE RECORDING AND APPROVAL OF APPLICATIONS THROUGH THE FSIS SYSTEM

Proper segregation of duties is not logically enforced within the Food Stamp Information System (FSIS). We found that case workers could initiate, record, and approve a food stamp application without the FSIS application requiring evidence of supervisory review from another person. Improper segregation of duties, whether organizational or logical, reduces the validity of a transaction, and may provide an individual with the opportunity to circumvent internal control procedures. In addition, poor segregation of duties may allow an individual to commit illegal acts and limit the ability of management to detect those activities. Senior management should implement a division of roles and responsibilities which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions.

Recommendation: DHHS management should implement a division of roles that separate the recording and approval functions for Food Stamp eligibility. This rule should be enforced by the FSIS application. Management should also make sure that personnel are only performing those duties stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained between inputting, recording and approving claims processed by the case workers. The small staff size at some of the counties may not allow management to fully segregate duties. However, in the absence of proper segregation of duties, management should ensure that controls such as audit checks are developed and implemented within the process to prevent the same person from recording the application and approving the same application.

Auditee's Response The Department of Health and Human Services concurs with the finding, in principle. However, to impose this mandate on the 100 county departments of social services at this time could have negative consequences for our program applicants, state and federal program error rates, and county and state administrative costs. While we are aware that state staff need to closely monitor the county staff regarding errors in application processing, we feel that we have existing safeguards in place that are outlined below.

Existing Processes That Would Detect Fraud:

State monitors conduct Management Evaluation (ME) Reviews on the following schedule: Smaller counties (counties with < 2,000 cases), the ME is conducted every 3 years; Medium counties (counties with < 15,000 cases), the ME is conducted every 2 years; and Large counties (counties with > 15,001 cases); the ME is conducted every year. Cases are read and checked for errors and improper actions during these ME Reviews.

On an annual basis, State QC is required to review a minimum of 1,020 active county records and a minimum of 680 negative. In FFY2007, QC reviewed 1,141 active cases and 716 negative cases for a total of 1,857 cases reviewed. NC samples extra cases because the intervals are based on projections and to allot for the cases that have to be dropped as incomplete. QC also reviews the sampled cases for application processing timeliness. QC reports to USDA FNS if applications are processed in a timely manner. NC's FFY 06 application processing timeliness rate of 96.66% was the 5th best in the nation.

State program representatives visit counties on a monthly basis and pull case records for many different purposes throughout the year. The results of these reviews are shared with both county and state managers for corrective action purposes.

Each county has some type of second party review process where records are pulled internally and checked by a supervisor or lead worker. The number of records checked varies by county. Workers can use the “Form on Hold” indicator in FSIS to put the action/form on hold until the supervisor or lead-worker releases the form for processing. This process is normally used for new workers or at supervisor’s discretion.

There are reports (i.e., Workload Report By Worker, Pending Applications and Emergency Cases, and the Notices of Actions Taken Report) generated for use by county managers that indicate the case actions completed each month. The caseworker who keyed the action is associated on the report with the applicable case action.

Future Actions That Will Detect Fraud:

The State is currently seeking a new case management automation solution that will replace FSIS. This Information Technology initiative is called North Carolina Families Accessing Services through Technology (NC FAST). The NC FAST automation solution will have a role base security that will enable the separation of duties based on role(s) within the system. NC FAST also has a requirement that states the vendor must provide a method to automatically pend a case unit action for second party review based on policy and worker profile.

DATA AUTHORIZATION

Controls are designed to ensure that access to data is appropriate and authorized and that access is granted on a need to know, need to use basis. The access control environment should consist of access control software and information security policies and procedures that are implemented appropriately to protect the application data. Our audit identified several weaknesses in data authorization for the FSIS application.

AUDIT FINDING 5: INFORMATION LEAKAGE ON INTERNET WEBPAGE

DHHS provided too much information on an internet webpage. During our audit, we were able to obtain the following information from the DHHS external website:

- Critical production datasets for the various applications to include the FSIS application
- RACF ID's and corresponding names of key programmers for the FSIS application
- Instructions for navigating the Endeavor program within the mainframe
- EBT (Electronic Banking Interface System) Application Code Information
- List of the key files and DB2 tables for the FSIS application
- Back up procedures for FSIS and the following key information:
  - ➢ DB2 Tables
  - ➢ Batch Files
  - ➢ Transmission Files Backups
  - ➢ XPTR Report Backups
- Information on off-site storage for the FSIS information

In an online information technology environment, management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.

Recommendation: DHHS should remove the sensitive information from the internet webpage and/or move it to the agency intranet as appropriate.

Auditee's Response: The Department of Health and Human Services concurs with the finding. The Department removed the sensitive information from public access on January 17, 2008.

AUDIT FINDING 6: INADEQUATE REVIEW OF UAUDIT AND EXCESSIVE ACTIVITY REPORTS

The agency does not require the DHHS Privacy and Security Office to review the UAudit report or the excessive activity report. The UAudit report can be used to identify any changes to the production environment as well as the person who made the change. The excessive activity report identifies users whose activities, including attempts to access unauthorized areas, warrant further review. Failure to regularly review the UAudit report or the excessive activity report may provide an individual with the opportunity to circumvent internal control procedures and allow an individual to commit illegal acts.

Per DHHS Security Policies and Procedures Security Manual regarding Information System Activity Reviews, "In addition to application or system-level audits, information system activity reviews shall be conducted or facilitated by the DHHS Privacy and Security Office on a periodic basis."

Recommendations: Management should require the DHHS Privacy and Security Office to receive and review the UAudit report for any unauthorized or unwarranted changes to the program code in the production environment. The Privacy and Security Office should review the excessive activity report and follow-up on any items listed on this report.

Auditee's Response: The Department of Health and Human Services concurs with the finding. The DHHS Privacy and Security Office will review UAudit and excessive activity reports for FSIS activity.

AUDIT FINDING 7: LACK OF SOURCE CODE COMPARISON

DHHS programmers do not routinely compare the current program code to the original code to ensure no unauthorized changes have been made. Also, there were instances where the programmer approving the change to a program was also the person making the change to the program. Therefore, failure to routinely compare the current program code to the original code can result in unauthorized changes not being detected, which can lead to critical errors or the commission of illegal acts.

The agency should monitor changes to the information system conducting security impact analyses to determine the effects of the changes. Prior to change implementation, and as part of the change approval process, the agency should analyze changes to the information system for potential security impacts.

Recommendation: Management should require the routine comparison of the program code to the original code to ensure no unauthorized changes have been made. Management should also implement adequate segregation of duties so that the person approving a program change is not the person making the change.

Auditee's Response: The Department of Health and Human Services concurs with the finding. By June 30, 2008, the Division of Information Resource Management (DIRM) will implement a client review and a peer review process, to include unit, system, and regression testing of all changes to FSIS programs to insure that no unauthorized changes are being made that could lead to any critical error or commission of any illegal acts.

[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 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