

**DEPARTMENT OF FINANCIAL SERVICES
FLORIDA ACCOUNTING INFORMATION
RESOURCE SUBSYSTEM**

Information Technology Operational Audit

July 1, 2007, Through June 30, 2008,
and Selected Actions Through September 17, 2008



CHIEF FINANCIAL OFFICER

Pursuant to Article IV, Sections 4(c) and 5(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Alex Sink served as Chief Financial Officer during the audit period.

The audit team leader was Chris Gohlke, CPA, and the audit was supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF FINANCIAL SERVICES
Florida Accounting Information Resource Subsystem

SUMMARY

The Florida Accounting Information Resource (FLAIR) Subsystem is the State of Florida's accounting system. Pursuant to Sections 215.93(1)(b) and 215.94(2), Florida Statutes, FLAIR is a subsystem of the Florida Financial Management Information System and the Department of Financial Services (Department) is the functional owner of FLAIR. FLAIR's functions, as provided in State law, include accounting and reporting so as to provide timely data for producing financial statements for the State in accordance with generally accepted accounting principles and for auditing and settling claims against the State.

Our audit of FLAIR focused on evaluating selected information technology (IT) controls relevant to financial reporting and applicable to the system during the period July 1, 2007, through June 30, 2008, and selected actions through September 17, 2008. We also determined the status of corrective actions regarding prior audit findings disclosed in audit report No. 2008-026.

The results of our audit are summarized below:

Finding No. 1: We noted instances where, as similarly noted in audit report No. 2008-026, the Department did not remove the access privileges of former and transferred employees in a timely manner.

Finding No. 2: The primary Departmental Accounting Component (DAC) access control custodian shared a user identification (ID) with a backup access control custodian.

Finding No. 3: The Department lacked procedures for the Statewide Financial Statements (SWFS) Subsystem security administration process and for the reconciliation of data loaded from the Purchasing Card Module and DAC into the Information Warehouse.

Finding No. 4: In addition to the matters discussed in Finding Nos. 1, 2, 3, and 7, certain Department security and application controls needed improvement. Some of the issues were also included in audit report No. 2008-026.

Finding No. 5: As similarly noted in audit report No. 2008-026, we noted a programming error in the salary refund calculation of net pay.

Finding No. 6: Department staff did not follow established job scheduling procedures during a nightly production run, resulting in discrepancies in the balances on the general ledger master file. A similar finding was included in audit report No. 2008-026.

Finding No. 7: As also noted in audit report No. 2008-026, contrary to the Department's Enterprise Security Policy, the Department had not established an approved baseline firewall configuration.

Finding No. 8: The Department did not consistently document the release of output data tapes to other entities.

Finding No. 9: On July 16, 2008, a fraud occurred that resulted in \$5,700,352 in vendor electronic funds transfer (EFT) payments being inappropriately diverted to the bank account of a third party. The Department, subsequent to the fraud, revised and expanded its EFT procedures; however, the procedures needed further improvement.

BACKGROUND

FLAIR performs the State's accounting and financial management functions. It plays a major role in ensuring that State financial transactions are accurately and timely recorded and that the State's Comprehensive Annual Financial Report is presented in accordance with appropriate standards, rules, regulations, and statutes. The accounts of all

State agencies are coordinated through FLAIR, which processes expense, payroll, retirement, unemployment compensation, and public assistance payments.

FLAIR is composed of four components. The Departmental Accounting Component (DAC) maintains agency accounting records and provides agency management with a budgetary check mechanism, while the Central Accounting Component (CAC) maintains a separate accounting system used by the Department on the cash basis for the control of budget by line item of the General Appropriations Act. The Payroll Component processes the State's payroll, and the Information Warehouse is a reporting system that allows users to access information extracted from CAC, DAC, the Payroll Component, and certain systems external to FLAIR. The DAC Statewide Financial Statements (SWFS) Subsystem assists and supports the Division of Accounting and Auditing (A&A) in the preparation of the annual financial statements of the State of Florida.

The Department is responsible for the design, implementation, and operation of FLAIR. The Division of Information Systems (DIS) operates the State Chief Financial Officer's Data Center and maintains FLAIR. A&A is the primary user of CAC and the Payroll Component. DAC and the Information Warehouse are primarily used by State agencies.

In May 2007, Aspire, a Department project to replace FLAIR and the State's Cash Management System with an integrated Statewide financial information system, was suspended. The Department retained ownership of the hardware and software for possible resumption of the development project at a later date. Chapter 2008-132, Laws of Florida, effective July 1, 2008, established a task force to develop a business plan for a successor financial and cash management system.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Access Controls - Management of Access Privileges

Effective management of system access privileges include provisions to timely remove or adjust employee access privileges when employment terminations and job reassignments occur. Prompt action is necessary to ensure that a former or reassigned employee's access privileges are not misused by the former employee or others.

Our review of access privileges for the network, Resource Access Control Facility (RACF), CAC, DAC, and the Payroll Component disclosed that the access privileges of all 356 Department employees who terminated employment during the period July 1, 2007, through March 31, 2008, had been removed as of the date of our testing. However, we noted instances where, as similarly noted in audit report No. 2008-026, the access privileges had not been timely removed. Specifically, from a sample of 30 of the 356 former employees, we noted the following:

- Five employees whose network access privileges were not removed for periods ranging from 2 to 42 days after termination.
- One employee whose RACF access privileges were not removed until 32 days after termination.

Also, our review of the application access privileges of all 356 former employees disclosed the following:

- Eight employees whose CAC access privileges were not removed for periods ranging from 21 to 197 days after termination.
- Nine employees whose DAC access privileges were not removed for periods ranging from 2 to 158 days after termination.
- One employee whose Payroll Component access privileges were not removed for 8 days after termination.

Through additional audit procedures, we noted another former employee whose network and RACF access privileges were not removed until 55 days after termination. Our audit further disclosed that, of the three employees with SWFS Subsystem access privileges who terminated employment or were reassigned within the Department between July 1, 2007, and April 30, 2008, one employee's access privileges were not removed until three days after he was reassigned within the Department.

In response to audit inquiry, Department management indicated that the delays in the removal of access privileges were the result of a variety of reasons, including communication breakdowns within the Department, as well as failure to follow up by Department staff. Department management also indicated that additional procedures were being implemented to centralize and automate access controls. As indicated above, although there were delays, all access privileges had been removed by Department staff prior to our testing. Without timely deletion of access privileges of employees who terminated employment or transferred within the Department, the risk is increased that access privileges could be misused by the former employee or others.

Recommendation: The Department should continue to enhance its procedures to ensure that the access privileges of all former and reassigned employees are removed in a timely manner.

Finding No. 2: Access Controls – User Identification

Rule 60DD-2.004(1)(a), Florida Administrative Code, provides that each user shall be assigned a unique user identification. Effective IT access controls include a process for the unique identification and authentication of users. The unique identification of users allows management to affix responsibility for system activity to an individual person.

The primary access control custodian and one backup custodian for the Division of Administration's DAC security administration shared a single user ID. In response to audit inquiry, Department management indicated that the two employees have now been assigned individual user IDs. The absence of unique user IDs increases the risk that management will be unable to timely determine the persons responsible for inappropriate system actions, should they occur.

Recommendation: The Department should continue to assign individual IDs to all system users.

Finding No. 3: IT Procedures

Sound IT management includes the establishment of procedures that describe management's expectations for controlling the entity's IT operations. Written procedures help ensure that management directives are clearly communicated, understood, accepted, and followed by all staff.

Our audit disclosed the following:

- No procedures existed for the SWFS Subsystem security administration process. Although DIS Procedure No. 102 identified responsibilities of the security administrators for the SWFS Subsystem, specific procedures had not been developed detailing the security administration process.
- Although a process existed for reconciling data loaded from the Purchasing Card Module and DAC into the Information Warehouse, no written procedures existed for the reconciliation. In response to audit inquiry, Department management indicated that written reconciliation procedures would be developed by September 30, 2008.

The absence of written procedures for security administration and reconciliations increases the risk that management's expectations will not be properly or consistently communicated, understood, or carried out.

Recommendation: The Department should establish written procedures to govern the SWFS Subsystem security administration process and the reconciliation of data loaded from the Purchasing Card Module and DAC into the Information Warehouse.

Finding No. 4: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls related to the network and DAC, in addition to the matters discussed in Finding Nos. 1, 2, 3, and 7, that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Department management of the specific issues. Some of the issues were also included in audit report No. 2008-026. Without adequate security controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Department should implement the appropriate security controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Finding No. 5: Salary Refund Calculation

IT controls are intended to ensure that, among other things, all data expected for processing are received and processed completely, accurately, and in a timely manner and all output is delivered in accordance with business requirements.

During each payroll process, the Payroll Component updates the employee year-to-date file and payroll image log from information obtained from the Salary Calculate and Cancellation and Adjustments Subsystems. As a part of our audit, we compared totals of selected payroll amounts for all employees on the employee year-to-date file with corresponding totals from the payroll image logs and cancellation and adjustments files for the 2007 calendar year. Our comparison disclosed differences in the net pay field for eight employees. In response to audit inquiry, Department management stated that the differences occurred during a salary refund process in which the net pay was not appropriately calculated. We noted similar differences in audit report No. 2008-026. In response to audit inquiry, Department management further indicated that they are still aggressively pursuing solutions to this issue and believe the error condition is limited to only those employees who have Earned Income Credits included in their payroll amounts. Department management further indicated that, in the interim, they are developing reports to assist in identifying the errors in a more timely manner, with a planned implementation date of December 2008.

Although the differences in net pay only totaled \$1,156 for the eight employees, the potential impact of future discrepancies resulting from the calculation error, if not corrected, could be greater. In response to audit inquiry, Department management indicated that corrective actions would be taken, including refunding moneys to one of the eight employees.

Recommendation: The Department should continue with its efforts to implement the appropriate programming changes to prevent future occurrences of salary refund calculation errors.

Finding No. 6: Job Scheduling Procedures

Program and operator errors pose risks to data integrity. Common operator errors include running programs out of sequence and forgetting to run critical procedures. The use of documented job scheduling procedures can help prevent these types of errors and mitigate the impact when such errors occur.

As similarly noted in audit report No. 2008-026, during our audit, we noted that Department staff did not follow established job scheduling procedures during a nightly DAC production run. Specifically, on the evening of August 21, 2007, Department staff did not follow the instructions for rerunning an abended (abnormally terminated) job. As a result, 307 duplicate disbursement corrections, spanning 15 agencies, were created, resulting in discrepancies in balances on the general ledger master file. Department of Health staff discovered the master file discrepancies and reported the issue to the Department on September 4, 2007. The Department corrected the discrepancies on September 27, 2007. In response to audit inquiry, Department management indicated that the issue has been addressed with the staff involved and that steps have been taken to improve communications and workflow. When operators do not follow established procedures, the risk is increased that program errors could adversely impact the accuracy of data and efficiency of business processes.

Recommendation: The Department should take the necessary steps to reinforce to staff the importance of following established procedures.

Finding No. 7: Firewall Configurations

Firewalls are hardware and software components that protect system resources from attack by outside users by blocking and checking all incoming network traffic. Effective network management practices include provisions to ensure that baseline firewall configurations are maintained and that all changes to the baseline are assessed in a structured way, subject to written change management procedures. The Department's Enterprise Security Policy dictated that baseline security configurations be documented.

In response to audit inquiry and as previously noted in audit report No. 2008-026, Department management was unable to provide an approved baseline firewall configuration. The absence of an approved baseline firewall configuration increases the risk that the firewall will not adequately protect system resources from unauthorized access. Department management subsequently indicated that a baseline firewall configuration has now been created and approved.

Recommendation: The Department should ensure that the baseline firewall configuration continues to be appropriately documented.

Finding No. 8: Logging of Output Data Tapes

Effective tape management controls include provisions to ensure that all movement of data tapes is authorized and logged. Output data tapes are those tapes created by the Department and distributed to other entities. The Department's Infrastructure Support Output & Printer Operations Office Manual required that all output tapes be signed out by the requesting entity and that the sign-out sheets be maintained until after the tapes are returned to the Department.

The Department creates a daily "picklist" report of outgoing tapes. We selected 73 output tapes from the "picklist" for five days and examined the sign-out sheets to determine if the movement of each tape was appropriately

documented. Our review of the 73 output tapes disclosed that 4 tapes were still checked out at the time of our test; however, each lacked a corresponding sign-out sheet. In response to audit inquiry, Department management indicated that each of the 4 tapes had been subsequently returned. When the release of output tapes is not documented, the risk is increased that the tapes may be lost and the information contained therein inappropriately disclosed.

Recommendation: The Department should reinforce to staff the importance of following established output data tape handling procedures.

Finding No. 9: Electronic Funds Transfer Authorization Process

On July 16, 2008, a fraud occurred that resulted in \$5,700,352 in vendor electronic funds transfer (EFT) payments being inappropriately diverted to the bank account of a third party. In response to the fraud, the Department revised and expanded its internal EFT procedures and took action to recover the diverted funds. As of September 17, 2008, the Department had recovered \$4,332,873 and was seeking to recover the remaining funds.

We performed additional audit procedures at the Department relating to the EFT authorization process. Additionally, in response to the fraud, the Department also engaged a consultant to review its automated clearing house (ACH) and wire transfer payment process.

Our additional audit procedures disclosed that the Department's EFT procedures needed further improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data. However, we have notified appropriate Department management of the specific issues. Without adequate internal controls over EFT authorizations, the risk is increased that errors or fraud related to EFT payments, should they occur, will not be prevented or timely detected by the Department.

Recommendation: The Department should implement the appropriate internal controls to ensure the integrity of Department data and the processing of EFT payments.

PRIOR AUDIT FINDINGS

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2008-026.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected IT controls related to the FLAIR Subsystem in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; the safeguarding of IT resources; and the effectiveness and efficiency of IT operations; and to determine whether the Department had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2008-026.

The scope of our audit focused on evaluating selected IT controls relevant to financial reporting during the period July 1, 2007, through June 30, 2008, and selected actions through September 17, 2008, including selected general IT controls over systems development and modification, computer operations, systems software and database, logical access to programs and data, and physical safeguards. The audit also included selected application IT controls and

selected user controls relevant to the FLAIR components: Central Accounting, Departmental Accounting, and Payroll.

In conducting our audit for the 2007-08 fiscal year, we:

- Interviewed Department personnel.
- Evaluated the access control policies and procedures outlined in the Enterprise Security Policy.
- Obtained an understanding of logical access paths to FLAIR.
- Documented and tested whether logical access controls ensured that access to data files, software, and databases were restricted to authorized users (RACF, network, and database).
- Observed, documented, and tested selected control activities surrounding the computer operations function.
- Observed, documented, and tested physical security controls.
- Obtained an understanding of the Department's progress in addressing system performance and capacity issues.
- Evaluated Department policies and procedures that provide for systems software testing, maintenance, and problem resolution.
- Obtained an understanding of the status of the FLAIR replacement project.
- Obtained an understanding of the status of the FLAIR User Group and FLAIR Enhancement Subcommittee and their coordination with the Department of Management Services regarding MyFloridaMarketPlace and People First.
- Obtained an understanding of the Department's succession plans to prevent and minimize interruption of business should a key employee be unable to fulfill their job duties.
- Observed, documented, and tested the effectiveness of selected input, processing, and output controls for the Voucher Audit Subsystem, Prompt Payment Subsystem, 1099 Subsystem, General Ledger Subsystem, Contracts and Grants Subsystem, Statewide Financial Statement Subsystem, On-Demand Payroll Subsystem, Salary Calculate Subsystem, and Collections Subsystem.
- Observed, documented, and tested the effectiveness of selected DAC, CAC, and Payroll Component application access controls.
- Observed, documented, and tested the effectiveness of selected controls over the design, testing, approval, and implementation of application program modifications.
- Evaluated whether user manuals and system documentation were updated and adequate to maintain efficient and effective operations.
- Evaluated the effectiveness of the reconciliation procedures between the FLAIR Information Warehouse and CAC, DAC, and the Payroll Component.
- Obtained an understanding of the status of the migration of the Statewide Vendor File from the State Purchasing System (SPURS) to FLAIR.

Subsequent to the 2007-08 fiscal year and before the completion of our audit, a fraud occurred on July 16, 2008, involving vendor EFT payments. We performed additional audit procedures at the Department relating to the EFT authorization process.

We conducted this IT audit in accordance with applicable generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.



David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated November 25, 2008, the Chief Financial Officer provided responses to our preliminary and tentative findings. The Chief Financial Officer's response is included as Exhibit A.

**EXHIBIT A
MANAGEMENT'S RESPONSE**



**CHIEF FINANCIAL OFFICER
STATE OF FLORIDA**

ALEX SINK

November 25, 2008


Mr. David W. Martin
Auditor General
State of Florida
Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(4) (d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's Information Technology Audit of the Florida Accounting Information Resource (FLAIR) Subsystem, for the period July 1, 2007, through June 30, 2008, and selected actions through September 17, 2008.

If you have any questions or would like to discuss the matter further, please contact Bob Clift, Inspector General, at (850) 413-4960.

Sincerely,


Alex Sink

AS:Cc

Enclosures

Florida Department of Financial Services
Information Technology Audit
Florida Accounting Information Resource (FLAIR) Subsystem
Preliminary and Tentative Audit Findings
For the Period July 1, 2007, through June 30, 2008, and
Selected Actions Through September 17, 2008

Finding No. 1: We noted instances where, as similarly noted in audit report No. 2008-026, the Department did not remove the access privileges of former and transferred employees in a timely manner.

Recommendation: The Department should continue to enhance its procedures to ensure that the access privileges of all former and reassigned employees are removed in a timely manner.

Response: The Department concurs. As a result of this and other audits presented by the Auditor General and independent consultant audit partners, the Department has established a cross functional agency-wide team to review and correct access control deficiencies. The Divisions of Accounting and Auditing, Administration, and Information Systems are implementing or have implemented the actions outlined below with regard to the specifically noted findings.

Division of Accounting and Auditing: The Division has established an access control team to improve the procedures and documentation for the review of access. The Division's access control team will complete the revision of access control procedures for the 19 applications owned by the Division by March 31, 2009. The revised procedures will be implemented April 1, 2009, for the Division's quarterly review for April – June 2009.

Division of Administration: The Division has designated an Accountant III position to serve as the primary access control administrator responsible for removal and update of access privileges and a Finance and Accounting Director II position to serve as the backup. Additional controls have been put in place whereby termination notices and notices of position changes received from the Bureau of Human Resource Management are forwarded to both the primary access control administrator and the backup via e-mail. Notices of terminations/changes set to occur in the future are placed on the Outlook calendars for both the primary access control administrator and the backup. The Finance and Accounting Director II confirms that all DAC access privileges for future terminations/changes are timely executed. Access privileges for immediate terminations are removed as soon as the notice is received. These actions have been completed.

Division of Information Systems (DIS): The Division will continue to improve the timeliness of deleting access privileges when employment is terminated. DIS is reviewing its current policies and procedures associated with application access and has reevaluated centralized access control in favor of a decentralized approach which provides better separation of duties and better internal control. DIS will report on the status of these improvements in conjunction with the six month audit follow-up.

During the audit period, when the Help Desk staff created tickets to terminate accesses, standard tasks were completed manually. Effective July 27, 2008, the Help Desk implemented program changes to automatically generate the standard tasks. Changing from manually creating the standard tasks to automatically generating the tasks has reduced the error rate (i.e., accesses not being terminated) by ensuring all the required tasks are created for access removal. In addition, follow-up e-mail reminders are system created and sent to the security administrators and Help Desk DP Coordinators the day following separation date to validate access removal. These actions have been completed.

Finding No. 2: The primary Departmental Accounting Component (DAC) access control custodian shared a user identification (ID) with a backup access control custodian.

Recommendation: The Department should continue to assign individual IDs to all system users.

Response: The Department concurs.

Division of Administration: The Division has set up separate user identifications for the DAC primary access control administrator and backup. This action has been completed.

Finding No. 3: The Department lacked procedures for the Statewide Financial Statements (SWFS) Subsystem security administration process and for the reconciliation of data loaded from the Purchasing Card Module and DAC into the Information Warehouse.

Recommendation: The Department should establish written procedures to govern the SWFS Subsystem security administration process and the reconciliation of data loaded from the Purchasing Card Module and DAC into the Information Warehouse.

Response: The Department concurs.

Division of Accounting and Auditing: The Division will work with DIS to establish written procedures to govern the security administration process for the SWFS Subsystem by March 31, 2009.

Division of Information Systems: Procedures to reconcile the data load from the Purchasing Card Module and DAC were written and implemented effective September 30, 2008.

Finding No. 4: In addition to the matters discussed in Finding Nos. 1, 2, 3, and 7, certain Department security and application controls needed improvement. Some of the issues were also included in audit report No. 2008-026.

Recommendation: The Department should implement the appropriate security controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Response: The Department concurs with the recommendation and will implement appropriate security controls.

Finding No. 5: As similarly noted in audit report No. 2008-026, we noted a programming error in the salary refund calculation of net pay.

Recommendation: The Department should continue with its efforts to implement the appropriate programming changes to prevent future occurrences of salary refund calculation errors.

Response: The Department concurs.

Division of Accounting and Auditing: Programming changes were implemented last year to correct this issue; however, another calculation discrepancy was discovered this year. This new discrepancy was fixed in August 2008. The Division of Accounting and Auditing will continue efforts to implement all necessary programming changes, if needed, to prevent future occurrences of salary refund calculation discrepancies. Two reports have been identified that can assist with identifying any salary refund calculation errors in a timely manner. One of the reports was implemented in October 2008 and the other one will be implemented by December 31, 2008.

Division of Information Systems: On August 11, 2008, DIS implemented the appropriate programming changes to prevent errors in salary refund calculations.

Finding No. 6: Department staff did not follow established job scheduling procedures during a nightly production run, resulting in discrepancies in the balances on the general ledger master file. A similar finding was included in audit report No. 2008-026.

Recommendation: The Department should take the necessary steps to reinforce to staff the importance of following established procedures.

Response: The Department concurs.

Division of Information Systems: Appropriate steps have been taken to improve communication and workflow. In addition, staffing changes at the supervisory level and disciplinary actions have occurred. These actions have been completed.

Finding No. 7: As also noted in audit report No. 2008-026, contrary to the Department's Enterprise Security Policy, the Department had not established an approved baseline firewall configuration.

Recommendation: The Department should ensure that the baseline firewall configuration continues to be appropriately documented.

Response: The Department concurs.

Division of Information Systems: DIS has implemented an application to record, track, and route firewall configuration changes. Approval is required prior to a change implementation. A full description of the change is contained in the approval request. A tool has been implemented to automatically record all firewall and router code modifications. This tool is properly backed-up to maintain and preserve the record. This action has been completed.

Finding No. 8: The Department did not consistently document the release of output data tapes to other entities.

Recommendation: The Department should reinforce to staff the importance of following established output data tape handling procedures.

Response: The Department concurs.

Division of Information Systems: Appropriate steps have been taken to reinforce that staff ensures sign out procedures are followed when all tapes are released. This action has been completed.

Finding No. 9: On July 16, 2008, a fraud occurred that resulted in \$5,700,352 in vendor electronic funds transfer (EFT) payments being inappropriately diverted to the bank account of a third party. The Department, subsequent to the fraud, revised and expanded its EFT procedures; however, the procedures needed further improvement.

Recommendation: The Department should implement the appropriate internal controls to ensure the integrity of Department data and the processing of EFT payments.

Response: The Department concurs. As a result of this and other audits presented by the Auditor General and independent consultant audit partners, the Department has established a cross functional agency-wide team to identify activities and associated risks. The Department will evaluate internal controls related to the EFT process that are either currently in place, or implement internal controls that need to be established to mitigate these risks.

