REPORT NO. 2010-021
OCTOBER 2009

DEPARTMENT OF FINANCIAL SERVICES

FLORIDA ACCOUNTING INFORMATION RESOURCE SUBSYSTEM

Information Technology Operational Audit

For the Period
July 1, 2008, Through June 30, 2009

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

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, CISA, 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 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, 2008, through June 30, 2009. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2009-053.

The results of our audit are summarized below:

Finding No. 1: We noted instances where, as similarly noted in our report No. 2009-053, the Department did not remove the access privileges of former employees in a timely manner.

Finding No. 2: The Department was unable to identify the Payroll Component user associated with a specific user identification (ID), and a Department employee who had transferred to another Department position inappropriately retained job control language access privileges.

Finding No. 3: The Department did not provide initial security awareness training for some employees or ongoing security awareness training for all employees.

Finding No. 4: In addition to the matters discussed in Finding Nos. 1, 2, and 3, certain Department security and application controls needed improvement. Our prior reports on the Department have included some of the same issues.

Finding No. 5: The Department's electronic funds transfer (EFT) authorization process needed improvement.

BACKGROUND

The FLAIR Subsystem is utilized to perform 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 (CAFR) is presented in accordance with appropriate standards, rules, regulations, and statutes. The accounts of all State agencies are coordinated through FLAIR that 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 State's CAFR.

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.

Finding No. 1: Management of Access Privileges – Timely Removal of Former Employee Access

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

We reviewed the access privileges for the network, Resource Access Control Facility (RACF), CAC, DAC, the Payroll Component, and the SWFS Subsystem for all 357 Department employees who terminated employment during the period July 1, 2008, through March 31, 2009. Our review noted instances where, as similarly reported in our report No. 2009-053, the access privileges of former employees had not been timely removed. Specifically:

- Three employees whose CAC access privileges were not removed for periods ranging from 4 to 40 days after termination.
- Two employees whose DAC access privileges were not removed for periods ranging from 19 to 64 days after termination.
- Two employees whose Payroll Component access privileges were not removed for periods ranging from 2 to 27 days after termination.

Additionally, from a sample of 30 of the 357 former employees, we noted 4 employees whose network access privileges were not removed for periods ranging from 2 to 40 days after termination.

In each of the above-described instances, although access was not removed in a timely manner, Department staff had removed the access by March 31, 2009. Without timely deletion of access privileges of employees who terminated employment with the Department, the risk is increased that access privileges could be misused by the former employee or others.

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

Finding No. 2: Management of Access Privileges - Other

An important aspect of IT security management is the establishment of system access privileges that restrict identifiable users to only those system functions necessary to perform their assigned duties. Additionally, properly configured access privileges help enforce an appropriate separation of incompatible duties and minimize the risk of unauthorized system actions.

Our audit disclosed aspects of the Department's management of access privileges that needed improvement, in addition to the matters discussed in Finding No. 1. Specifically:

- Upon audit inquiry, the Department was unable to identify the Payroll Component user who was associated with a user identification (ID) that the Department had deleted on July 11, 2008. As a result, the Department

could not demonstrate whether the user's account was deleted in a timely manner or whether the access privileges assigned to the user ID were appropriate.

- One employee with two RACF user IDs inappropriately retained the ability to move job control language into the production environment for 166 days after transferring to a position within the Department that no longer required this ability. This condition increased the Department's risk of unauthorized job control language being moved into the production environment by the reassigned employee or others. In response to audit inquiry, the Department removed the employee's access privileges.

Recommendation: The Department should implement appropriate controls to properly identify users and ensure that access privileges granted are appropriate and commensurate with employee job functions.

Finding No. 3: Security Awareness Training

Effective security awareness programs include first-time training for all new employees and periodic refresher training for all employees. The Department developed a security awareness training program for new employees. The program was provided as a part of a new employee orientation class held in Tallahassee. New non-Tallahassee employees traveled to Tallahassee to attend class. Beginning on February 6, 2009, non-Tallahassee staff were no longer permitted to travel to Tallahassee for training because of a moratorium on travel, pursuant to Chapter 2009-15, Laws of Florida. From a sample of 33 of 259 new employees hired from July 1, 2008, through March 30, 2009, we noted 8 non-Tallahassee employees who had not received security awareness training.

In addition, the Department had not developed an ongoing security awareness training program to provide periodic refresher training for all employees. The Department noted this issue in a 2008 IT Risk Assessment Survey that it conducted pursuant to Section 282.318(2)(a)2., Florida Statutes, and planned to develop ongoing online security awareness training.

In response to audit inquiry, Department management indicated that they intend to develop an online security awareness training tool and train all employees by June 30, 2010. Department management also indicated that, in the future, all employees will receive annual refresher training using the training tool. The lack of security awareness training for new employees and ongoing security awareness training for all existing employees increases the risk that employees may inadvertently compromise security.

Recommendation: The Department should continue with its plan to institute online training for both initial and ongoing security awareness training.

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, DAC, the Payroll Component, and the SWFS Subsystem, in addition to the matters discussed in Finding Nos. 1, 2, and 3, 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 our prior reports on the Department, most recently report No. 2009-053. 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: Electronic Funds Transfer (EFT) Authorization Process

Input controls ensure that source documents are complete, authorized, and accurate and that there is an adequate separation of duties regarding the origination and approval of source documents. Output controls ensure that a complete and accurate record of the results of processing is reported to appropriate individuals for review.

Vendors, employees, and retirees may receive payments from the State via EFT. Vendors doing business with the State who wish to be paid by EFT must submit a State of Florida Electronic Payment Authorization form to the Department for new EFT authorizations, as well as for changes to existing EFT authorizations. The information on this form, including vendor and bank account information, is used to make changes to the EFT Authorization file that is used by CAC's EFT Subsystem to process EFT payments.

Our review of a sample of 36 new vendor EFT authorizations and account changes disclosed two State of Florida Electronic Payment Authorizations where the dates contained in the Authorization Date field of the EFT Authorization file did not correspond to the dates the forms were signed by the vendors, contrary to the Department's Direct Deposit Operating Procedures. Our sample also disclosed four approved State of Florida Electronic Payment Authorizations for which the requested changes to the vendors' contact information were not entered into the EFT Authorization file. In response to audit inquiry, Department management stated that in most of the noted instances, the actions taken were appropriate under the circumstances but their Direct Deposit Operating Procedures needed to be updated to provide guidance to staff for documenting those situations. The lack of complete procedures increased the possibility that staff will not understand or follow management's intent.

Additionally, our review disclosed instances where an EFT verification procedure was not followed by Division of A&A, EFT Section staff. We are not disclosing specific details of the issue in this report to avoid the possibility of compromising the Department's data. However, we have notified appropriate Department management of the specific issue. When staff do not follow procedures, management's ability to ensure that staff are performing the verification as intended is limited.

Recommendation: The Department should update the Direct Deposit Operating Procedures, as appropriate, and take steps to ensure that staff consistently follow the approved Procedures.

PRIOR AUDIT FINDINGS

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2009-053.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational 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.

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; 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 our report No. 2009-053.

The scope of our audit focused on evaluating selected IT controls relevant to financial reporting during the period July 1, 2008, through June 30, 2009, including selected general IT controls over the control environment, systems development and modification, computer operations, systems software and database, and logical access to programs and data. 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, we:

- Interviewed Department personnel.
- Evaluated the adequacy of the Department's Comprehensive Risk Analysis, Business Continuity Plan, Security Awareness Training Program, succession plans for key employees, and ongoing communication program.
- Obtained an understanding of the Agency Dashboard and Accountability Measures relevant to FLAIR, the Vendor Payment Information Web site, and the Department's plans to achieve compliance with Section 511 of Public Law 109-222 regarding the 3 percent withholding of Federal tax.
- Obtained an understanding of logical access paths to FLAIR and documented and tested whether logical access controls ensured that access to data files, software, and databases was restricted to authorized users (RACF, network, and database).
- Observed, documented, and tested the effectiveness of selected access controls for the network, RACF, CAC, DAC, Payroll, SWFS Subsystem, and the Employee Information Web site.
- Observed, documented, and tested selected controls surrounding the computer operations function.
- Evaluated Department policies and procedures that provide for systems software testing, maintenance, and problem resolution.
- Observed, documented, and tested the effectiveness of selected controls over the design, testing, approval, and implementation of application program modifications.
- Observed, documented, and tested the effectiveness of selected input, processing, and output controls for the Voucher Audit Subsystem, General Ledger Subsystem, Property Subsystem, Statewide Financial Statement (SWFS) Subsystem, On-Demand Payroll Subsystem, Salary Calculate Subsystem, and Cancellation and Adjustments Subsystem.
- Observed, documented, and tested the effectiveness of selected controls over the authorization of EFT payments.

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 September 29, 2009, the Chief Financial Officer provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

ALEX SINK

September 29, 2009

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 Operational Audit of the Florida Accounting Information Resource (FLAIR) Subsystem, for the period July 1, 2008, through June 30, 2009.

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

Enclosure

DEPARTMENT OF FINANCIAL SERVICES
THE CAPITOL, TALLAHASSEE, FLORIDA 32399-0301 • (850) 413-2850 • FAX (850) 413-2950

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Financial Services
Information Technology Operational Audit
Florida Accounting Information Resource (FLAIR) Subsystem
Preliminary and Tentative Audit Findings
For the Period July 1, 2008, through June 30, 2009

Finding No. 1: Management of Access Privileges – Timely Removal of Former Employee Access

We noted instances where, as similarly noted in our report No. 2009-053, the Department did not remove the access privileges of former employees in a timely manner.

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

Response: The Department concurs. The Department will continue to enhance its procedures to ensure that the access privileges of all former employees are removed in a timely manner. The Department will update its current access control policy (AP&P 4-05) by December 31, 2009, to strengthen this process. The Department will also pursue a short term solution by creating a database based on employee's role to identify all access privileges so that once the employee's employment status changes, the appropriate access rights can be disabled quickly. A long term strategy of the Department is to adapt ITIL based CMDB to maintain a record of all the access rights.

Finding No. 2: Management of Access Privileges - Other

The Department was unable to identify the Payroll Component user associated with a specific user identification (ID), and a Department employee who had transferred to another Department position inappropriately retained job control language access privileges.

Recommendation: The Department should implement appropriate controls to properly identify users and ensure that access privileges granted are appropriate and commensurate with employee job functions.

Response: The Department concurs. The Department has implemented an Application Access Control Workgroup to review Department procedures and make recommendations for improvement to the access control process.

Finding No. 3: Security Awareness Training

The Department did not provide initial security awareness training for some employees or ongoing security awareness training for all employees.

Recommendation: The Department should continue with its plan to institute online training for both initial and ongoing security awareness training.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Response: The Department concurs. The Department plans to develop an on-line security awareness training tool and train all employees by June 30, 2010. This tool will be used for annual refresher training.

Finding No. 4: Other Security Controls

In addition to the matters discussed in Finding Nos. 1, 2, and 3, certain Department security and application controls needed improvement. Our prior reports on the Department have included some of the same issues.

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: Electronic Funds Transfer (EFT) Authorization Process

The Department's electronic funds transfer (EFT) authorization process needed improvement.

Recommendation: The Department should update the Direct Deposit Operating Procedures, as appropriate, and take steps to ensure that staff consistently follow the approved Procedures.

Response: The Department concurs. The Direct Deposit Operating Procedures will be updated by December 31, 2009, and periodically reviewed, and steps will be taken to ensure that applicable staff members follow the approved Procedures.