

DEPARTMENT OF FINANCIAL SERVICES

**FLORIDA ACCOUNTING INFORMATION
RESOURCE SUBSYSTEM (FLAIR)**

Information Technology Operational Audit



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 Jeff Atwater served as Chief Financial Officer during the period of our audit.

The audit team leader was Earl M. Butler, CISA, CFE, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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) 412-2722; 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 (FLAIR)

SUMMARY

The Florida Accounting Information Resource Subsystem (FLAIR) 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 function, as provided in State law, includes 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 focused on evaluating selected information technology (IT) controls relevant to financial reporting and applicable to FLAIR. We also determined the status of corrective actions regarding audit findings included in our report No. 2014-033 that were applicable to the scope of this audit.

Our audit disclosed areas in which improvements in FLAIR controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: The access privileges of some FLAIR users did not promote an appropriate separation of duties, restrict users to only those functions necessary for their assigned job duties, or provide for individual accountability.

Finding No. 2: Department procedures for the periodic review of access privileges needed improvement.

Finding No. 3: Department processes relating to the performance of periodic special reviews of agency-exempt invoice payment types needed improvement. In addition, the Department did not have written procedures defining the periodic special review of agency-exempt invoices.

Finding No. 4: Certain security controls related to logical access and the protection of confidential and exempt information needed improvement.

In October 2013, the Department contracted with North Highland Worldwide Consulting to complete a study of FLAIR and provide a recommendation to either replace or enhance FLAIR. The recommendation received in March 2014 was for the Department to replace FLAIR and the Cash Management System (CMS). The Department has begun the initial planning steps for the FLAIR and CMS Replacement Project (see the Background and Additional Matter sections of this report for further information).

BACKGROUND

In 1980, the Legislature enacted the Florida Fiscal Accounting Management Information System (FFAMIS) Act requiring that Statewide financial statements must be prepared. As a result of this Act, the State Automated Management Accounting Subsystem (SAMAS) was developed. Between 1983 and 1986, agencies implemented SAMAS for managing their accounting needs. In 1997, SAMAS was renamed as FLAIR.

FLAIR is used 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. The Statewide Financial Statements (SWFS) Subsystem

assists and supports the Division of Accounting and Auditing (A&A) in the preparation of the State’s CAFR. Primary users of DAC are State agencies.

- 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. A&A is the primary user of CAC.
- The Payroll Component processes the State’s payroll. A&A is the primary user of the Payroll Component. Payroll processing is administered by the Bureau of State Payrolls (BOSP) within A&A.
- The Information Warehouse is a reporting system that allows users to access information extracted from DAC, CAC, the Payroll Component, and certain systems external to FLAIR. Primary users of the Information Warehouse are State agencies.

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.

On October 3, 2013, the Department entered into a contract with North Highland Worldwide Consulting to complete a study of FLAIR and to provide a recommendation to either replace or enhance FLAIR. In compliance with contract requirements, North Highland Worldwide Consulting delivered the final *FLAIR Study* to the Department on March 21, 2014. Once received, Department management reviewed and published the final *FLAIR Study* on April 1, 2014.

According to Department management, the Department agreed with the North Highland Worldwide Consulting recommendation to replace FLAIR and the Cash Management System (CMS) as outlined in the *FLAIR Study* and has begun the initial planning of the Pre-Design, Development, and Implementation (pre-DDI) steps for the FLAIR and CMS Replacement Project. The Department tentatively plans to start working on the FLAIR and CMS Replacement Project action plan in July 2014, anticipates starting the project procurement process in December 2014, and expects to complete the project procurement process by September 2016.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to data and IT resources that promote an appropriate separation of duties and that restrict employees to only those functions necessary for their assigned job duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, or destruction. Our audit disclosed that some inappropriate and unnecessary access privileges existed to selected functions within DAC, CAC, the Payroll Component, and the Report Distribution System (RDS) of FLAIR as discussed in the following paragraphs:

DAC Cash Receipts (CR) and Cash Disbursements (DB) Functions

Our review of 13 Bureau of State Payrolls (BOSP) DAC users with update access privileges to CR or DB functions disclosed that 5 BOSP employees had inappropriate or unnecessary update access privileges to the CR or DB functions. Specifically:

- Two of the 13 users had inappropriate update access privileges as a result of having incompatible access privileges to the CR and DB functions.
- One user had update access privileges to the DB function that was not necessary for the user’s assigned job duties.

- One former user had update access privileges to the DB function during the user's employment with the Department that was not necessary for the user's assigned job duties and was not timely removed upon termination.
- One former user had update access privileges to the DB function that was not timely removed upon termination.

While the access of the two terminated users noted above was not used subsequent to their terminations, the length of time access remained active after termination ranged from 11 to 35 days. A similar finding regarding DAC access privileges was noted in prior audits of the Department, most recently our report No. 2014-033.

DAC State CFO Files (SC) Function and Related SC ET (EFT Authorization Inquiry Request) Mini-Menu Function

Our review of 12 users with Statewide access privileges to the DAC SC function disclosed that 3 users had excessive access privileges to the DAC SC function. These 3 users had inappropriate update access privileges to the DAC SC function based on the users' assigned job duties.

Our review of 13 users with Statewide access privileges to the DAC SC ET mini-menu function containing confidential information disclosed that 11 users had inappropriate inquiry access privileges to the mini-menu function based on the users' assigned job duties. However, 2 of the 11 users did not have access privileges to the DAC SC function and that prevented actual use of the DAC SC ET mini-menu function.

CAC Functions

Our review of 1 Department of Management Services, Division of Retirement user with inquiry access privileges to the Central EFT Authorization (ET) and EFT Payment Detail (EP) functions that contained confidential information disclosed that the user's access privileges to the ET and EP functions were inappropriate based on the user's assigned job duties.

Payroll Component Functions

Our review of 9 Department users with update access privileges to the Payroll Tax Reporting (TAXR), Warrant Cancellation Approval (WCXA), or Non-Cash Approval (NCA) functions disclosed that 3 users had inappropriate update access privileges to one or more of those functions based on the users' assigned job duties. Specifically:

- One Bureau of Financial Services user within the Division of Administration had inappropriate update access privileges to the TAXR, WCXA, and NCA functions. Due to inactivity, this user's access privileges became inactive on September 5, 2013, and were deleted on October 3, 2013.
- One BOSP Employee Records Section Supervisor had inappropriate update access privileges to the TAXR function.
- One BOSP Payroll Processing employee had inappropriate access privileges to the WCXA function.

A similar finding regarding Payroll Component access privileges was disclosed in our report No. 2014-033.

RDS Payroll Reports

Our review of an access group that provided group members global access privileges to the RDS payroll reports, including the RDS Statewide Payroll Register, disclosed that the 12 users in the access group could not be uniquely identified to provide for individual accountability when accessing the RDS payroll reports. In addition, 10 of the 12 users had continuous access privileges to the RDS payroll reports that were not necessary for their job duties. In response to audit inquiry, Department management indicated that these access privileges were used for data comparison and troubleshooting issues. Although access to the RDS payroll reports may have been needed to periodically research data comparison and troubleshooting issues, continuous access privileges were not necessary.

Access to inappropriate or unnecessary functions and the lack of individual accountability when accessing the RDS payroll reports increase the risk of unauthorized disclosure, modification, or destruction of Department data and IT resources.

Recommendation: The Department should limit user access privileges to data and IT resources to promote an appropriate separation of duties, restrict users to only those functions necessary for their assigned job duties, and provide for individual accountability. Additionally, the Department should only grant access privileges on an as-needed basis to those users who periodically need access for data comparison and troubleshooting issues.

Finding No. 2: Periodic Review of Access Privileges

Periodic review of access privileges helps ensure that access privileges assigned to users are monitored on a regular basis to ensure the access privileges are authorized and remain appropriate. The Department’s procedures related to the periodic review of access privileges of certain users with access to programming systems and reporting systems needed improvement. Specifically:

- The Department had not performed periodic reviews of user access privileges for COmmon Business-Oriented Language (COBOL) and UNIX users. In addition, there were no procedures with specific instructions related to the periodic review of access privileges of COBOL or UNIX users.
- Periodic access review procedures did not comprehensively include access privileges defined for the RDS reports, the DAC SC function, and the related DAC SC ET mini-menu function.

Without an adequate periodic review of user access privileges, there is an increased risk that inappropriate access to data files and programs may exist that could result in compromised data integrity.

Recommendation: The Department should improve procedures to include periodic reviews of all user access privileges to ensure that the privileges assigned are authorized and appropriate.

Finding No. 3: Auto Pay Continued Eligibility Determination

Section 17.03(1), Florida Statutes, provides the authority for the Chief Financial Officer (CFO) to examine, audit, and settle all accounts, claims, and demands against the State, arising under any law or resolution of the Legislature, and issue a warrant directing the payment out of the State Treasury of such amount as he or she allows thereon. Section 17.03(2), Florida Statutes, provides that the CFO may establish dollar thresholds applicable to each invoice amount and other criteria for sampling or testing invoices on a preaudit and postaudit basis. The CFO may revise such thresholds and other criteria for an agency or the unit of any agency as he or she deems appropriate.

The Department’s Bureau of Auditing is responsible for the sampling and testing of invoices on a preaudit and postaudit basis. In an effort to redirect staff resources toward payments of greater risk and materiality, the Bureau of Auditing implemented Auto Pay processes to reduce the number of low-risk invoices subject to preaudit based on invoice payment type. Auto Pay payments are typically high-volume, low-risk payments that are exempt from the preaudit process and automatically post in FLAIR. A sample of Auto Pay invoices is selected for postaudit on a monthly basis. Auto Pay postaudits are similar to preaudits in that they focus on the review of documentation to support the payment. Critical error rates are reviewed on a monthly basis and, if deemed excessive for any agency, site, object code, or combination thereof, the invoice payment type is removed from Auto Pay and added back to the preaudit process until the error rate improves.

As described above, a sample of Auto Pay invoices is selected for postaudit on a monthly basis. However, there are some approved invoice exceptions for some agencies where specific invoice payment types are exempt from being included in the population from which a sample is selected for postaudit. While the Department conducted special reviews on an ad-hoc basis of some agencies that used Auto Pay for specific invoice payment types that were normally exempt from postaudits, the Department did not have a defined process in place for performing periodic special reviews of specific agency invoice payment types exempt from postaudit to determine if the exempt invoice payment types continued to meet the requirements for use of Auto Pay and remain exempt from postaudits. In addition, the Department did not have written procedures indicating when, how often, or under what circumstances a periodic special review of agency-exempt invoices was to be performed.

Without a defined process and written procedures for performing periodic special reviews of agency-exempt invoice payment types and agency-exempt invoices, the risk is increased that payments may be made that are invalid or inaccurate.

Recommendation: The Department should improve its processes relating to the performance of periodic special reviews of agency-exempt invoice payment types to ensure that agencies remain eligible to use Auto Pay and therefore exempt from postaudits. In addition, the Department should establish written procedures defining the periodic special review of agency-exempt invoices.

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 that certain Department security controls related to logical access and the protection of confidential and exempt information needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues. Some of the issues were communicated to Department management in connection with prior audits of the Department, most recently our report No. 2014-033. Without adequate security controls related to logical access and the protection of confidential and exempt information, the confidentiality, integrity, and availability of Department data and IT resources may be compromised.

Recommendation: The Department should improve certain security controls related to logical access and the protection of confidential and exempt information to ensure the confidentiality, integrity, and availability of Department data and IT resources.

PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for four of the six findings included in our report No. 2014-033 that were applicable to the scope of this audit. Corrective actions were not taken for one of the six prior audit findings as described in the findings above. In addition, one prior audit finding was only partially corrected. One prior audit finding included in our report No. 2014-033 was not in the scope of this audit.

ADDITIONAL MATTER

On June 3, 2014, subsequent to the completion of our field work in May 2014, the Department encountered a production control issue with the nightly batch processing for expense warrant and electronic fund transfer (EFT) payments for which nightly batch processing was halted. All State agencies were impacted. The Department

determined through its normal production control monitoring and escalation procedures that the issue related to a limitation in the FLAIR programming code used for reporting during the nightly batch processing that prevented the State from processing expense warrant and EFT payments when the daily total amount of all payments equaled or exceeded \$1 billion. As a result, the Division of Accounting and Auditing temporarily unposted some vouchers in FLAIR to reduce the total amount of all payments below the \$1 billion limit so that the nightly batch processing could proceed.

To address this issue going forward, the Department developed an interim solution to manage the issue while the permanent solution will be included in the system replacement of FLAIR. The Department's interim solution was to modify the expense warrant and EFT payment report programs to accommodate a daily total amount of all expense warrant and EFT payments in excess of \$1 billion. Additionally, a trending report was to be developed for the Division of Accounting and Auditing based on historical expense data for expense warrant and EFT payments for ongoing monitoring and analysis.

On September 4, 2014, the Department indicated that the interim solution had been implemented in the production environment.

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 from March 2014 through May 2014 in accordance with 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 operational audit were to determine the effectiveness of selected IT controls 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. Other objectives were to determine the status of the study for the replacement of FLAIR; the status of the vendor maintenance agreements for continued support of Adaptable DATA Base System (ADABAS), COBOL, and Natural; and the effectiveness of selected controls regarding the Payroll Component files that were provided to State agencies, the Quick Pay process, and the unbalanced TR10 transactions. An additional objective was to determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2014-033 that were within the scope of this audit.

The scope of this audit focused on selected Department IT controls applicable to financial reporting during the period July 2013 through May 2014 and selected actions through September 4, 2014. The audit included selected application-level general controls related to access controls and separation of duties and selected general controls related to physical security. The audit also included selected application IT controls and selected user controls relevant to FLAIR components: DAC, CAC, and the Payroll Component.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls and IT controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of ineffective or inefficient IT operational policies, procedures, or practices. The focus of

this IT operational audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of the audit, the audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.


In conducting our audit, we:

- Interviewed Department personnel.
- Determined the Department's progress towards the replacement of FLAIR including whether an action plan had been established.
- Determined the Department's status regarding vendor maintenance agreements for continued support of ADABAS, COBOL, and Natural including whether such support had or would expire.
- Obtained an understanding of the Department's Auto Pay processes including how entities qualify to use the Auto Pay processes and identified all agencies that processed payments through the Auto Pay processes.
- Obtained an understanding of the Department's procedures related to State agencies' unbalanced TR10 transactions.
- Obtained an understanding of the Department's procedures for providing Payroll component files to State agencies.
- Evaluated the Department's vendor maintenance agreements for the continued support of ADABAS, COBOL, and Natural and determined whether the Department routinely monitors the configuration.
- Evaluated the Department's Auto Pay processes. For agencies that the Department approved the use of the Auto Pay processes, we determined whether evidence existed to indicate that the Department reviewed the agencies' related internal controls.
- Evaluated the Department's monitoring of the State agencies' unbalanced TR10 transactions.
- Evaluated the Department's transaction interface processing procedures regarding the Payroll component files and reports that are provided to State agencies to enter into and reconcile with the Departmental component of FLAIR.
- Evaluated the Department's agency monitoring procedures for timely payment of interest penalties associated with untimely invoice payments.

- Obtained an understanding of the Department’s process for authorizing access privileges to move Natural, COBOL, and UNIX programs into the production environment.
- Obtained an understanding of the Department’s process for conducting periodic reviews of access privileges granted through Natural, COBOL, and UNIX security.
- Evaluated the Department’s authorization controls regarding users with access privileges to move Natural, COBOL, and UNIX changes into the production environment and perform periodic access reviews.
- Evaluated the Department’s physical security controls regarding the Fletcher Data Center.
- Evaluated the Department’s identification and authentication mechanisms regarding the Network and RACF passwords.
- Evaluated the Department’s application access controls applicable to Cash Receipts (CR) and Cash Disbursements (DB) functions from July 2013 to March 2014.
- Evaluated the Department’s application access controls applicable to the DAC State CFO File (SC) and the related DAC SC ET (EFT Authorization) mini-menu functions from August 2013 through March 2014.
- Evaluated the Department’s application access controls applicable to the Central EFT Authorization (ET) and EFT Payment Detail (EP) functions from August 2013 through March 2014.
- Evaluated the Department’s application access controls applicable to the Payroll Tax Reporting (TAXR), Warrant Cancellation Approval (WCXA), and Non-Cash Approval (NCA) functions from July 2013 through March 2014.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe those matters requiring corrective action.

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 4, 2014, 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**.

THIS PAGE INTENTIONALLY LEFT BLANK

**EXHIBIT A
MANAGEMENT'S RESPONSE**



CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

September 4, 2014

Mr. David W. Martin
Auditor General
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 *Department of Financial Services, Florida Accounting Information Resource Subsystem (FLAIR)*.

If you have any questions concerning this response, please contact Teresa Michael, Inspector General, at (850) 413-4960.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jeff Atwater".

Jeff Atwater

JA:rlg

Enclosure

**EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE**

**DEPARTMENT OF FINANCIAL SERVICES
FLORIDA ACCOUNTING INFORMATION RESOURCE SUBSYSTEM
Information Technology Operational Audit**

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Appropriateness of Access Privileges

The access privileges of some FLAIR users did not promote an appropriate separation of duties, restrict users to only those functions necessary for their assigned job duties, or provide for individual accountability.

Recommendation: The Department should limit user access privileges to data and IT resources to promote an appropriate separation of duties, restrict users to only those functions necessary for their assigned job duties, and provide for individual accountability. Additionally, the Department should only grant access privileges on an as-needed basis to those users who periodically need access for data comparison and troubleshooting issues.

Response: We concur. The Division of Information Systems terminated the inappropriate access to the Departmental Accounting Component (DAC) State CFO Files (SC) Function and Related SC ET (EFT Authorization Inquiry Request) Mini-Menu Function on May 13, 2014. Additionally, the Division of Information Systems evaluated access to the Report Distribution System (RDS) Payroll Reports and determined that all users except one required this access for ongoing job responsibilities. Access was terminated on June 2, 2014, for the one user determined to no longer require the access.

Expected Completion Date for Corrective Action: Ongoing

**EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE**

**DEPARTMENT OF FINANCIAL SERVICES
FLORIDA ACCOUNTING INFORMATION RESOURCE SUBSYSTEM (FLAIR)
Information Technology Operational Audit**

Finding No. 2: Periodic Review of Access Privileges

Department procedures for the periodic review of access privileges needed improvement.

Recommendation: The Department should improve procedures to include periodic reviews of all user access privileges to ensure that the privileges assigned are authorized and appropriate.

Response: We concur. The Department is currently evaluating access reviews to ensure all FLAIR related access is included in the review process.

Expected Completion Date for Corrective Action: Ongoing

**EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE**

**DEPARTMENT OF FINANCIAL SERVICES
FLORIDA ACCOUNTING INFORMATION RESOURCE SUBSYSTEM (FLAIR)
Information Technology Operational Audit**

Finding No. 3: Auto Pay Continued Eligibility Determination

Department processes relating to the performance of periodic special reviews of agency-exempt invoice payment types needed improvement. In addition, the Department did not have written procedures defining the periodic special review of agency-exempt invoices.

Recommendation: The Department should improve its processes relating to the performance of periodic special reviews of agency-exempt invoice payment types to ensure that agencies remain eligible to use Auto Pay and therefore exempt from postaudits. In addition, the Department should establish written procedures defining the periodic special review of agency-exempt invoices.

Response: We concur. The Division of Accounting and Auditing will improve its processes related to the periodic and special review of agency-exempt invoices. The written procedures for the periodic and special review will be incorporated into the Bureau of Auditing's annual audit plan.

Expected Completion Date for Corrective Action: October 31, 2014

**EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE**

**DEPARTMENT OF FINANCIAL SERVICES
FLORIDA ACCOUNTING INFORMATION RESOURCE SUBSYSTEM (FLAIR)
Information Technology Operational Audit**

Finding No. 4: Other Security Controls

Certain security controls related to logical access and the protection of confidential and exempt information needed improvement.

Recommendation: The Department should improve certain security controls related to logical access and the protection of confidential and exempt information to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Response: The Department will continue to address security controls, as appropriate.

Expected Completion Date for Corrective Action: Ongoing