REPORT NO. 2014-033
OCTOBER 2013

DEPARTMENT OF FINANCIAL SERVICES

FLORIDA ACCOUNTING INFORMATION RESOURCE SUBSYSTEM (FLAIR)

Information Technology Operational Audit

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

The audit team leader was Arthur Hart, CPA, 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. 2013-078.

The results of our audit are summarized below:

Finding No. 1: As similarly noted in prior audits of the Department, most recently our report No. 2013-078, the access privileges of some Department users were not appropriate for their job responsibilities.

Finding No. 2: The Department's periodic review of access privileges needed improvement.

Finding No. 3: As noted in our report No. 2013-078, the Department did not maintain access authorization forms for some users.

Finding No. 4: Certain Departmental security controls related to logical access needed improvement. This issue was communicated to Department management in connection with our report No. 2013-078.

Finding No. 5: Some automated controls related to Departmental transaction data input and processing were not in place.

Finding No. 6: The Department had not established procedures to ensure that the agencies paid prompt payment interest penalty invoices within the 15 days required by State law.

Finding No. 7: Certain Payroll application processing controls related to payroll processing and payroll processing adjustments needed improvement.

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 to FLAIR.

FLAIR is a double-entry, computer-based, general ledger accounting system, which 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. During the 2012-13 fiscal year, there were 38 individual agencies and related entities across the State that used Departmental FLAIR. For the fiscal year ended June 30, 2013, there were 48,716,801 Departmental Accounting transactions processed in this component.

- The Central Accounting Component (CAC) maintains a separate accounting system used by the Department. This a cash-basis system for the control of budget by line item of the General Appropriations Act. The primary user of CAC is A&A within the Department. For the fiscal year ended June 30, 2013, there were 9,958,873 Central Accounting transactions processed in this component.
- The Payroll Component processes the State's payroll. A&A is the primary user of this component. Within A&A, Payroll is administered by the Bureau of State Payroll (BOSP). Payroll processing encompasses several types of payroll including, but not limited to, biweekly, monthly, and on demand. For the fiscal year ended June 30, 2013, there were 3,086,870 Payroll transactions processed in this component.
- 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.

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.

The 2012 General Appropriations Act (GAA), Chapter 2012-118, Laws of Florida, Specific Appropriation 2360, appropriated $1.5 million from the Administrative Trust Fund for the Department to contract with an independent third-party consulting firm to complete a study of FLAIR, the Cash Management Subsystem (CMS), and agency financial business systems and to provide a recommendation for the replacement or remediation of FLAIR and CMS.

On October 19, 2012, the Department issued a Statement of Work and Request for Quotes for the FLAIR Replacement Study. However, the Statement of Work was not awarded and the applicable appropriated funds of the 2012 GAA reverted.

Subsequently, the 2013 GAA, Chapter 2013-40, Laws of Florida, Specific Appropriation 2279, appropriated $1.75 million from the Administrative Trust Fund for the Department to contract with an independent third-party consulting firm with experience in planning or managing public sector technology projects to complete a study of FLAIR and provide a recommendation to replace or enhance FLAIR. It also provided that the study shall include:

- An assessment of the feasibility of implementing an Enterprise Resource Planning system for the State of Florida.
- An inventory of all systems interfacing with FLAIR and assess the advantages and disadvantages of replacing: (1) FLAIR; (2) FLAIR and CMS; and (3) FLAIR, CMS, and the procurement and personnel information subsystems.

Additionally, the GAA specified that the purpose of the study is to identify and recommend replacement or enhancement options for consideration and shall include all specific changes needed in the Florida Statutes and financial business practices. The study shall be submitted to the Governor, President of the Senate, and Speaker of the House of Representatives. The Request for Quotes (RFQ) for the FLAIR Study was released by the Department on June 28, 2013 and the RFQ was subsequently awarded on October 3, 2013. The final deliverable due date for the FLAIR Study Report is March 21, 2014.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to only what is necessary in the performance of assigned job responsibilities and promote an appropriate separation of job duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction. Some inappropriate access privileges existed to DAC, CAC, and the Payroll Component, as discussed in the following paragraphs.

DAC

Our review of access privileges for 19 DAC users indicated that 1 user in the BOSP Payroll Processing area had access to update Cash Receipts and Disbursements, which was in line with current Department business rules and procedures in place at the time of our testing. Although the access definitions were within defined Department business rules and procedures, the functions noted are incompatible functions. The same user should not have access to enter both Cash Receipts and Cash Disbursements. A similar finding regarding DAC access privileges was disclosed in our report No. 2013-078. Subsequent to our testing, the Department's business rules were revised to no longer allow update access to Cash Receipts for the particular position held by the user whose access privileges we reviewed during our field work.

CAC

Our review disclosed that 38 Department of Management Services, Division of Retirement, users had been granted inquiry access privileges to the two CAC functions containing confidential information. Based on our review, we determined that the inquiry access privileges granted were inappropriate based on the employees' job duties and the principles of need-to-know and least privilege. A similar finding regarding CAC access privileges was disclosed in our report No. 2013-078.

Payroll Component

Our review of 10 users with access to selected functions within the Payroll Component indicated that 2 of the 10 users were granted inappropriate access privileges to some Payroll Component functions with respect to their job duties and positions within the Department.

Access to incompatible and inappropriate functions increase the risk of misappropriation of assets and erroneous manipulation of data.

Recommendation: The Department should limit user access privileges to data and IT resources to only what is necessary to perform job responsibilities and to promote an appropriate separation of duties.

Finding No. 2: Periodic Review of Access Privileges

Periodic review of access privileges helps ensure that access privileges remain appropriate. Although the Department performs periodic reviews of access privileges related to FLAIR data files and programs written in the Natural programming language, we identified the following control deficiencies:

- Automated reports detailing user access privileges for review and verification were being sent to the same users for whom the reports pertained. As a result, assurance could not be given that periodic reviews were

being performed by appropriate supervisory personnel independent of the users for whom the access verification pertained.

- The periodic review process did not comprehensively include all users with access to data files and programs, such as programming and other information systems personnel. As a result, assurance could not be given that periodic reviews of access privileges for all personnel were being performed and, in turn, that the access privileges defined for users continued to be appropriate.

Without an adequate, periodic review of access privileges, there is an increased risk that inappropriate access to data files and programs could exist resulting in inappropriate access to financial data and transactions.

Recommendation: The Department should ensure that the periodic review of access privileges includes verification of access by appropriate supervisory personnel independent of the users for whom the access verification pertains and encompasses all applicable users.

Finding No. 3: Access Authorizations

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(1), Florida Administrative Code, provides that information owners shall be responsible for authorizing access to information. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized.

We requested access authorization documentation for the 19 users with access privileges to move Natural, COBOL, and UNIX changes into the production environment to determine if access granted was adequately documented and authorized. The Department did not provide the documentation requested. This finding regarding missing authorization forms was also disclosed in our report No. 2013-078.

In the Department's response to our finding in report No. 2013-078, the Department indicated that it had accepted the risk associated with the absence of access authorization documentation for users granted information systems access prior to the implementation of the *IT Application Access & Resource Request Form (1820)* in 2006. As part of its risk acceptance, the Department assessed the residual risk level as low. Additionally, the Department identified compensating controls related to quarterly access reviews of all secure applications. Although the Department identified compensating controls to mitigate the risk of not maintaining complete access control definition and authorization documentation, the mitigating controls did not appear to be effective and fully comprehensive to ensure that access assigned to users was properly authorized. For example, as noted in Finding No. 2 of this report, we identified control deficiencies that reduced the effectiveness of the periodic reviews.

The lack of documentation of management's authorization of user access privileges may limit the Department's ability to ensure that user access privileges granted to employees do not exceed what is necessary for the accomplishment of assigned job duties.

Recommendation: The Department should maintain complete documentation of management authorization for user access privileges to move Natural, COBOL, and UNIX changes into the production environment.

[1] During the 2012 Legislative Session, HB 5011 that abolished AEIT and reassigned the functions and duties of AEIT to a new State agency was passed by the Legislature and presented to the Governor for signature. The bill was vetoed by the Governor on April 20, 2012. However, AEIT underwent defacto dissolution as the 2012 General Appropriations Act made no appropriations for the funding of positions in AEIT. As of the completion of our audit, rulemaking authority and responsibility for promoting or enforcing compliance with existing AEIT rules had not been established.

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 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. Prior audits of the Department, most recently our report No. 2013-078, noted similar issues. Without adequate security controls related to logical access, the confidentiality, integrity, and availability of data and IT resources may be compromised.

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

Finding No. 5: DAC Application and Manual Processing

Automated application input and processing controls ensure the completeness, accuracy, and validity of system data. Effective input controls ensure that only correct data is entered and accepted by the system.

Because DAC is the general ledger of the State of Florida, it is used by agencies and other applicable entities across the State. On average, over 4 million transactions were entered into FLAIR on a monthly basis across all agencies and related entities using FLAIR. During our audit, we reviewed DAC for certain automated controls in place to ensure the completeness and accuracy of data regardless of the agency or entity using FLAIR. With respect to this, we focused on automated controls of encumbrance, payable, disbursement, and general accounting transactions in evaluating automated input and processing controls.

Through our review, we determined that DAC did not have automated controls in place to:

- Prevent improper Object Code, Category, and General Ledger Code accounting combinations for encumbrances, payables, disbursements, and general accounting transactions. Without manual review and verification of transaction data, there is the risk that invalid accounting entries resulting from transactions entered into DAC could be processed and posted to the general ledger.
- Prevent a vendor invoice from being paid more than once. Without manual review and verification, there is the risk that a vendor invoice could be paid more than once, resulting in overpayment of a vendor.
- Prevent accounts payable and disbursement transactions related to encumbrance transactions being created for amounts greater than the original encumbrance. Without manual review and validation, there is the risk that an accounts payable or disbursement transaction could be entered for an amount greater than the originating authorized encumbrance amount. As a result, unauthorized amounts could be entered for an accounts payable or disbursement transaction applicable to an encumbrance.
- Prevent accounts payable transactions from being overpaid. Without manual intervention, there is the risk that a disbursement transaction applicable to the payable could be processed for an amount greater than the payable and thus circumventing the amounts and associated controls of the originating payable.
- Prevent the same encumbrance from being paid multiple times through different disbursement transactions. Without manual intervention, there is the risk that multiple disbursement transactions could be processed against the same encumbrance resulting in overpayment of an encumbrance and thus circumventing the controls associated with the originating encumbrance.
- Prevent transactions from being processed and posted to the general ledger without first being approved in the system. Without manual intervention and monitoring, there is the risk that an unapproved transaction could be erroneously entered into DAC and processed, which includes processing of payments and posting to the general ledger.

- Ensure encumbrance transactions were properly reinstated or journal entries were properly reestablished when an encumbrance disbursement or an encumbrance payable transaction was deleted. Without manual intervention and monitoring, encumbrance and associated allotment balances could be misstated in DAC.

To facilitate the mitigation of risks associated with the above deficiencies in the automated controls, reliance is placed on the manual preventive and detective controls of the individual agencies and entities using FLAIR to ensure the completeness and accuracy of transactions and data. Additionally, disbursement transactions, on a sample basis, are subject to audit and manual review by the Bureau of Auditing within the Department, before or after payment processing depending on the type of disbursement transaction. Inherent with manual controls, the risk of incomplete or inaccurate data is increased as compared to automated controls.

As previously mentioned in the BACKGROUND section of this report, the Department received an appropriation of $1.75 million to contract for a study to provide a recommendation for the replacement or enhancement of FLAIR and to include all specific changes needed in Florida Statutes and financial business practices. On June 28, 2013, a Request for Quotes was released by the Department soliciting bids from interested parties.

Recommendation: The Department should continue its process toward the completion of the study for the replacement or enhancement of FLAIR as outlined in Chapter 2013-40, Laws of Florida, Specific Appropriation 2279. The Department should also consider improvements in financial business practices and supporting IT processes and controls to promote an increase in the use of appropriate automated controls in order to facilitate consistency of controls across all user agencies and related entities and thus promote improved reliance on the completeness and accuracy of data in the system.

Finding No. 6: Central Accounting Prompt Payment

Section 215.422(3)(b), Florida Statutes, requires that, if a warrant in payment of an invoice is not issued within 40 days after receipt of the invoice and receipt, inspection, and approval of the goods and services, the agency or judicial branch shall pay to the vendor, in addition to the amount of the invoice, interest at a rate as established pursuant to Section 55.03(1), Florida Statutes, on the unpaid balance from the expiration of such 40-day period until such time as the warrant is issued to the vendor. Such interest shall be added to the invoice at the time of submission to the Chief Financial Officer for payment whenever possible. If addition of the interest penalty is not possible, the agency or judicial branch shall pay the interest penalty within 15 days after issuing the warrant.

Our review of Central Accounting prompt payment processing showed that interest penalty invoices were automatically calculated by FLAIR for all invoices that were approved for payment but failed to meet the requirements set forth in Section 215.422(3)(b), Florida Statutes. These pending interest penalty invoices were retained in FLAIR until processed for payment, provided that these invoices met preestablished criteria, such as meeting minimum amount thresholds. However, the Department had not established procedures to ensure that agencies paid these interest penalty invoices within the 15 days after issuing the overdue warrant.

The lack of controls ensuring that interest penalty invoices are timely paid increases the risk of the agencies not meeting their obligations as set forth in State law. During our audit, the Department began drafting procedures for ensuring that the timely payment of interest penalty invoices by agencies and the judicial branch.

Recommendation: We recommend that the Department finalize and implement its procedures for ensuring that interest penalty invoices are timely paid.

Finding No. 7: Payroll Application Processing

Application processing controls consist of automated and manual controls applied to business transaction flows and relate to the completeness, accuracy, and validity of transactions and data during application processing. Our audit disclosed that certain Payroll application processing controls related to payroll processing and payroll processing adjustments needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of payroll transactions and data. However, we have notified appropriate Department management of the specific issues. Without adequate Payroll application processing controls, the completeness, accuracy, and validity of transactions and data may be compromised.

Recommendation: The Department should improve Payroll application processing controls to ensure the completeness, accuracy, and validity of transactions and data.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2013-078.

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 2013 through August 2013 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; and the safeguarding of IT resources. An additional objective was to determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2013-078.

The scope of our audit focused on evaluating selected Department IT controls applicable to financial reporting during the period July 1, 2012, through June 30, 2013, and selected Department actions through October 3, 2013. The audit included selected general IT controls over systems modification and logical access to programs, data, and data files. The audit also included selected application IT controls and selected user controls relevant to FLAIR components: DAC, CAC, and Payroll.

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 inefficient or ineffective 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 vendors 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.
- Obtained an understanding of the Department's IT strategic planning processes and the degree to which data classification and risk assessment was considered and aligned with strategic planning.
- Evaluated the effectiveness of the Department's Continuity of Operations Plan (COOP) and Disaster Recovery activities including the extent of disaster preparedness off-site testing and the impact of testing on overall disaster preparedness planning.
- Obtained an understanding of DAC, CAC, and the Payroll Component; including the purpose of the system; computing platform and related software; access paths to view, modify, or delete data; system modification process; patch management process; and the user account administration process.
- Evaluated the effectiveness of selected controls over the authorization, testing, approval, documentation, and implementation of 25 DAC, CAC, and Payroll Component program changes completed between July 1, 2012, and May 7, 2013.
- Evaluated the appropriateness, as well as selected program change controls, of two DAC and four CAC blanket Departmental Project Requests (DPRs) between July 1, 2012, and May 7, 2013.
- Evaluated the appropriateness of controls related to processes and data used for testing purposes.
- Evaluated the effectiveness of controls to ensure program changes moved into production were appropriate.
- Evaluated the effectiveness of selected logical access controls in ensuring that access privileges to DAC, CAC, and the Payroll Component; network; database and production data files were appropriately restricted and provided an adequate separation of duties.
- Evaluated the effectiveness of policies and procedures for the overall administration of security access controls.
- Evaluated the effectiveness of controls related to periodic reviews of access privileges for the application, network, and database.
- Evaluated the effectiveness of selected input, processing, and output controls, as well as exception reporting and selected manual follow-up procedures, for DAC, CAC, and the Payroll Component including selected interface controls.

- Obtained an understanding of controls between DAC and CAC that ensure proper and authorized payment processing.
- Evaluated the effectiveness of controls in place related to warrant processing (including prompt payment) and reconciliation.
- Obtained an understanding of controls and criteria used for the Department's audit sampling process and override capabilities.
- Evaluated the appropriateness of controls to prevent or detect fictitious employees.
- Evaluated the appropriateness of controls related to updating and maintenance of the Directory Maintenance table parameters.
- Evaluated the effectiveness of controls related to retirement adjustments.
- Evaluated the effectiveness of controls related to the Payroll Deductions – Drop Priority Sequence processing.
- Evaluated the effectiveness of reconciliation controls in place between the Payroll Component and DAC and CAC.
- Evaluated the effectiveness of controls in place to validate and identify data originating from MyFloridaMarketPlace (MFMP) as of June 6, 2013.
- Evaluated the effectiveness of controls in place related to ensure data transmitted to MFMP is secured.
- Evaluated the effectiveness of controls in place to validate data received from the Florida Accountability Contract Tracking System (FACTS) as of May 7, 2013.
- Evaluated the effectiveness of controls in place to ensure data transmitted to FACTS is complete and accurate.
- Evaluated the appropriateness of controls related to DAC and Statewide Financial Statements (SWFS).
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

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 October 29, 2013, 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

October 29, 2013

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 Tom Kirwin, Inspector General, at (850) 413-4960.

Sincerely,

for 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

As similarly noted in prior audits of the Department, most recently our Report No. 2013-078, the access privileges of some Department users were not appropriate for their job responsibilities.

Recommendation: The Department should limit user access privileges to data and IT resources to only what is necessary to perform job responsibilities and to promote an appropriate separation of duties.

Response:

DAC: The Department concurs. The employee's access was changed to 'inquiry' access on or before September 3, 2013. The Department's business rules were updated to reflect that the appropriate access for this position was 'inquiry' access.

CAC: The Department concurs. As noted in the Department's response to Report No. 2013-078 Finding No. 1, the Department stated that CAC access for the Division of Retirement (Retirement) staff would be terminated once the Retirement Direct Deposit website was implemented. The projected implementation date was originally March 2013. However, the website was not implemented until May 2013. The Department terminated access for all Retirement staff to CAC EFT in June 2013.

Payroll Component: The Department concurs. The two employees' access was changed to 'inquiry' access on or before October 9, 2013. The Department will strengthen its review of access especially as it relates to employees that transfer to new roles in the Department.

Expected Completion Date for Corrective Action: Complete

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

The Department's periodic review of access privileges needed improvement.

Recommendation: The Department should ensure that the periodic review of access privileges includes verification of access by appropriate supervisory personnel independent of the users for whom the access verification pertains and encompasses all applicable users.

Response: We concur. The Department will evaluate and refine this access review process to ensure that it encompasses all appropriate verifications.

Expected Completion Date for Corrective Action: April, 2014

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

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

Finding No. 3: Access Authorizations

As noted in our Report No. 2013-078, the Department did not maintain access authorization forms for some users.

Recommendation: The Department should maintain complete documentation of management authorization for user access privileges to move Natural, COBOL, and UNIX changes into the production environment.

Response: The Department performed a formal risk assessment related to this matter and accepted the minimal risk identified through this process. Department efforts will continue to be focused on the completion of these forms for all new workers and on controls related to the prevention and detection of inappropriate 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. 4: Other Security Controls

Certain Departmental security controls related to logical access needed improvement. This issue was communicated to Department management in connection with our Report No. 2013-078.

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

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

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. 5: DAC Application and Manual Processing

Some automated controls related to Departmental transaction data input and processing were not in place.

Recommendation: The Department should continue its process toward the completion of the study for the replacement or enhancement of FLAIR as outlined in Chapter 2013-40, Laws of Florida, Specific Appropriation 2279. The Department should also consider improvements in financial business practices and supporting IT processes and controls to promote an increase in the use of appropriate automated controls in order to facilitate consistency of controls across all user agencies and related entities and thus promote improved reliance on the completeness and accuracy of data in the system.

Response: The Department concurs. The Department contracted with the North Highland Company to perform the business case study on the replacement or enhancement of FLAIR. The study is scheduled to be completed by March 21, 2014. The Department will, using existing resources, continue to consider improvements and enhancements to FLAIR designed to increase automated controls and improve the reliance on the completeness and accuracy of data in FLAIR.

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. 6: Central Accounting Prompt Payment

The Department had not established procedures to ensure that the agencies paid prompt payment interest penalty invoices within the 15 days required by State law.

Recommendation: We recommend that the Department finalize and implement its procedures for ensuring that interest penalty invoices are timely paid.

Response: The Department concurs. The Department has finalized and implemented its procedures to monitor agency progress in the timely payment of interest penalties. Chief Financial Officer Memorandum No.1 (2013-2014) was issued on August 6, 2013. This memo directs agencies to address prompt payment interest penalties within the 15 days as required by State law. This memo also notifies the agencies that the Department's Vendor Ombudsman will monitor agency progress in processing prompt payment interest penalties generated.

Expected Completion Date for Corrective Action: Complete

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

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

Finding No. 7: Payroll Application Processing

Certain payroll application processing controls related to payroll processing and payroll processing adjustments needed improvement.

Recommendation: The Department should improve payroll application processing controls to ensure the completeness, accuracy, and validity of transactions and data.

Response: The Department is in process of obtaining a legal opinion on certain payroll processing adjustments. Based on the outcome of this opinion, the Department will make any necessary changes to its process for payroll adjustments.

Expected Completion Date for Corrective Action: March 30, 2014