REPORT NO. 2012-016
OCTOBER 2011

DEPARTMENT OF FINANCIAL SERVICES

FLORIDA ACCOUNTING INFORMATION RESOURCE (FLAIR) SUBSYSTEM

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. During the period under audit, the following individuals served as Chief Financial Officer:

The Honorable Alex Sink	January 2, 2007, through January 4, 2011
The Honorable Jeff Atwater	From January 4, 2011

The audit team leader was Sarah Beth Hall, 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) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF FINANCIAL SERVICES

Florida Accounting Information Resource (FLAIR) 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 Subsystem. We also determined the status of corrective actions regarding audit findings included in our report No. 2011-030.

The results of our audit are summarized below:

Finding No. 1: The access privileges of some Department users were not appropriate for their job responsibilities.

Finding No. 2: As similarly noted in prior audits of the Department, most recently our report No. 2011-030, the Department did not disable the network access privileges of some former employees in a timely manner.

Finding No. 3: Certain Department security controls related to security event logging, logical access, and data transmission needed improvement. Some of the issues were also noted in our report No. 2011-30.

Finding No. 4: Contrary to the requirements of the State of Florida, *General Records Schedule* for the retention of access control records, the Department did not retain some network and Natural Security access control records.

Finding No. 5: As similarly noted in our report No. 2011-030, the Department did not maintain a comprehensive configuration repository of its IT infrastructure and applications.

Finding No. 6: As similarly noted in prior audits of the Department, most recently our report No. 2011-030, the Department did not provide initial security awareness training for some agency workers or periodic refresher training for all agency workers.

Finding No. 7: As similarly noted in our report No. 2011-030, Department firewall configuration management controls needed improvement.

Finding No. 8: Some Department policies and procedures were outdated, inaccurate, lacking, or not effectively disseminated to staff. The Department also lacked written procedures for some Departmental Accounting Component (DAC) access control processes.

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 DAC, CAC, 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. Additionally, DAC is divided into two database files; one for the Department of Children and Family Services (DCFS) and one for all the other State agencies. The DAC database file for DCFS is referred to as HAC.

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.

Title 26, Section 3402(t), United States Code, requires Federal, State, and other governmental entities to withhold 3 percent from payments to entities providing property or services, except as provided therein, and remit this withholding to the U. S. Treasury. Federal Regulations governing the 3-percent withholding were finalized on May 9, 2011. Title 26, Section 31.3402(t), Code of Federal Regulations provided a one-year extension of the previous statutory effective date (payments made after December 31, 2011). The effective date of the withholding requirement is now for payments made after December 31, 2012. Withholding is now scheduled to begin on January 1, 2013, with the first Federal reporting to be submitted in January 2014.

Although the Federal Regulations provided the one-year extension, the Department continued the process of designing changes to its processes and systems in order to implement the requirements of the law. Department management indicated that the law has already and will continue to require extensive program modifications to FLAIR. As a result of the one-year extension, the Department revised its target date for implementation of the 3-percent withholding to January 2013.

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. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction. As discussed in the following paragraphs, some inappropriate access privileges existed to DAC, CAC, the Payroll Component, W-9 Web site production code, and specific network folders.

DAC

Our review of users with Statewide or Department update access privileges to selected functions within DAC as of May 31, 2011, disclosed that three A&A users had update access privileges to one or more functions that were inappropriate for their job responsibilities. Specifically:

- One A&A user's Statewide access privileges to the Vendor Client function was inappropriate for her job responsibilities.
- One A&A user's Statewide access privileges to the Invoice Tracking function was inappropriate for his job responsibilities.

- One A&A user's access privileges to the Cash Receipts, Vendor Employee, Expansion, General Accounting, and Accounts Payable functions were contrary to the *DAC Access Control Business Process Procedures for OLO 4390*. The *DAC Access Control Business Process Procedures for OLO 4390* were developed by A&A and provide the business rules for granting DAC access privileges to positions within A&A, operating level organization (OLO) 4390.

We reviewed the access privileges of 29 user identifications (IDs) belonging to Department users with the ability to add vendors to the Statewide Vendor File and all users with the ability to update non-MyFloridaMarketPlace vendor records on the Statewide Vendor File as of May 31, 2011. Our review disclosed that 5 of the 29 user IDs, belonging to 4 users, had update or add access privileges that were inappropriate for their job responsibilities. In response to audit inquiry, Department staff modified the access privileges of 4 of the 5 user IDs.

CAC

The *CAC Access Control Business Process Procedures* were developed by A&A and provide the business rules for granting CAC access privileges. Our review of the 44 CAC users assigned the Audit Override or Special Flag Override capability as of March 16, 2011, disclosed that, contrary to the *CAC Access Control Business Process Procedures*, 10 users were assigned Audit Override or Special Flag Override capabilities that were inappropriate for their job responsibilities. Through additional audit procedures, we noted another user with update access privileges to two CAC functions that was also contrary to the *CAC Access Control Business Process Procedures* developed by A&A.

Payroll Component

Our review of the 99 user IDs with Statewide or Department inquiry, update, or override access privileges to the Payroll Component as of April 21, 2011, disclosed that 2 DIS users had Statewide Payroll access privileges that were inappropriate for their job responsibilities. In response to audit inquiry, Department staff removed the Payroll Component access privileges of the 2 DIS users on May 6, 2011.

W-9 Web Site Production Program Code

Our review of 19 users with access privileges to FLAIR production program code for the W-9 Web site disclosed that 14 users had inappropriate update access privileges based on their job responsibilities.

Network Folder Access

In the Department's directory service, security permissions can be set on folders. Folder permissions include full control, modify, read and execute, list folder contents, read, and write. Users may be granted folder access privileges (explicit access) or group access (inherited access) by adding the user as a member of a group. Our review of 40 users with either explicit or inherited access privileges to the Bureau of State Payrolls (BOSP) network folder as of May 24, 2011, disclosed inappropriate levels of access privileges. Although only modify, read and execute, read, or write access privileges were needed to perform their assigned duties, many users were granted full control (unrestricted) access privileges to the BOSP network folder. Full control access privileges allow users the ability to make changes to the access privileges granted to the folder and, therefore, should only be granted to administrators. Specifically:

- Five of the 11 users with explicit access privileges had inappropriate full control access privileges to the BOSP network folder at the time of our testing.
- All 29 users with inherited access privileges had inappropriate full control access privileges to the BOSP network folder at the time of our testing.

Our audit disclosed that 195 users had either inappropriate explicit or inherited access privileges to a network folder containing sensitive information regarding the Department's DIS disaster recovery plan. Users with inappropriate

access privileges included individuals within the Bureaus of Accounting Systems Design, Financial Applications, Insurance Applications, Infrastructure Support, and Programming Design, and the Office of the Director. In response to audit inquiry, Department staff removed the inappropriate network access privileges of the 195 users.

Review of Access Privileges

Effective access controls include provisions for the periodic review of the appropriateness of access privileges. We noted that the Department's review of application access privileges needed improvement. Specifically:

- The DIS Help Desk performed a quarterly Departmental FLAIR Statewide security access authorization review of users with DAC and HAC Statewide access privileges. The report used in the Help Desk review listed the users with DAC and HAC Statewide access privileges, but did not detail the access privileges that users had been granted to functions within DAC and HAC. For example, the report did not list whether users had inquiry or update access privileges to specific DAC and HAC functions. In response to audit inquiry, Department staff modified the report to identify the access privileges that users had been granted to the DAC and HAC functions.
- BOSP performed a quarterly review of users with Payroll Component access privileges. However, the review did not include DIS users with access privileges to the Payroll Component.

The above-mentioned conditions increase the risk of unauthorized disclosure, modification, or destruction of data and IT resources.

Recommendation: The Department should limit user access privileges to only what is necessary for user job responsibilities. Additionally, the Department should ensure that periodic reviews of DAC and HAC Statewide access privileges contain sufficient information to determine whether assigned access privileges remain appropriate and commensurate with job responsibilities. The Department should also expand its review of Payroll Component access privileges to include users within DIS.

Finding No. 2: Timely Disabling of Network Access Privileges

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

We reviewed logical access privileges for the network for a sample of 30 of the 344 Department employees and contractors who terminated employment or contractual services during the period July 1, 2010, through March 31, 2011. Our review disclosed instances where, as similarly noted in prior audits of the Department, most recently our report No. 2011-030, the network access privileges of some former employees had not been timely disabled. Specifically, we noted 4 former employees whose network access privileges remained active for periods ranging from 4 to 8 days after termination. The Department was unable, upon audit inquiry, to determine whether the network access privileges of the 4 former employees were used after their dates of termination. Without timely disabling of former employee access privileges, the risk is increased that the access privileges could be misused by the former employee or others.

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

Finding No. 3: 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 security event logging, logical access, and data transmission that needed improvement or were deficient. Some of the issues were also noted in our report No. 2011-030. 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. Without adequate security controls related to security event logging, logical access, and data transmission, 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 improve security controls related to security event logging, logical access, and data transmission to ensure the confidentiality, integrity, and availability of data and IT resources.

Finding No. 4: Access Control Records Retention

The *State of Florida, General Records Schedule GS1-SL for State and Local Government Agencies (General Records Schedule)*, revised by the Department of State effective August 2010, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment. Contrary to the *General Records Schedule* requirements, the Department did not retain some network and Natural Security access control records. Without the retention of access control records, the risk is increased that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur. Additionally, the Department is not in compliance with the State's record retention requirements.

Recommendation: The Department should ensure that access control records are retained as required by the *General Records Schedule*.

Finding No. 5: Comprehensive Configuration Repository

Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of a comprehensive configuration repository. A comprehensive configuration repository would include the collection of initial configuration information, establishment of baselines, verification and review of configuration information, and the update of the configuration repository as needed. Effective configuration management facilitates greater system availability, minimizes production issues, and resolves issues more quickly.

As similarly noted in our report No. 2011-030, the Department did not have a comprehensive configuration repository of its IT infrastructure and applications. Examples of the components that should be identified in a configuration repository include hardware; systems software (including operating systems); firmware; custom-built applications; commercial off-the-shelf software packages; database products; physical databases; environments; and interfaces between databases, applications, and network components. Because there was no comprehensive configuration repository, the Department did not have a means to easily identify relationships between a component item that is to be changed and other components of the IT infrastructure and applications, limiting management's ability to identify and involve the owners of all affected components in assessing the impact of the change on the overall operation of the IT infrastructure and applications.

Without a comprehensive configuration repository, the risk is increased that changes to components of the IT infrastructure and applications may not be appropriately assessed or implemented or that needed changes may be overlooked, impacting the proper functioning and security of the Department's IT infrastructure and applications.

Recommendation: The Department should implement a central comprehensive configuration repository to facilitate the management and control of its IT infrastructure and applications.

Finding No. 6: Security Awareness Training

Effective security awareness programs include initial training for all new employees and periodic refresher training for all employees. Additionally, security awareness training should include not only agency personnel but also contractors and other users of information systems that support the agency's operations and assets. Agency for Enterprise Information Technology (AEIT) Rule 71A-1.008(3), Florida Administrative Code, provides that agency workers shall receive initial security awareness training within 30 days of employment start date. AEIT Rule 71A-1.002(101 and 102), Florida Administrative Code, defines worker and workforce to include employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for an agency, is under the direct control of the agency.

Our audit disclosed that, contrary to AEIT Rules, Department workers other than salaried employees, such as contractors, volunteers, and other personal services (OPS) employees, were not required by the Department to attend new employee orientation that would have included security awareness training. In response to audit inquiry, the Department began requiring new employee orientation, including security awareness training, for OPS employees. However, initial security awareness training for contractors and volunteers had not yet been provided. Additionally, we determined that, contrary to AEIT Rules, 16 of 45 employees included in our sample, whose employment start date was on or after November 15, 2010, received their initial security awareness training from 36 to 155 days after their employment start date.

AEIT Rule 71A-1.008(2), Florida Administrative Code, provides that, at a minimum, agency workers shall receive annual security awareness training. As similarly noted in prior audits of the Department, most recently our report No. 2011-030, the Department had not, as of March 11, 2011, implemented an ongoing security awareness training program to provide periodic refresher training for employees.

The lack of security awareness training for contractors, volunteers, and OPS employees and periodic refresher training for all existing Department workers increases the risk that employees may inadvertently compromise security because of an inadequate awareness or understanding of security requirements.

Recommendation: The Department should provide initial and periodic refresher security awareness training for all Department workers, including salaried employees, contractors, volunteers, and OPS employees.

Finding No. 7: Firewall Configuration Management

Firewalls are hardware and software components that protect system resources from attack by outside users by blocking and checking all incoming network traffic. Effective network management practices include provisions to ensure that all changes to the firewall configuration are assessed in a structured way, subject to written configuration management procedures. The DIS NI-028, *Firewall Configuration Procedure,* provides that all firewall changes are to be

approved by management prior to implementation, affected users are to be notified of approved changes, and successful testing is to be certified by application owners.

Upon audit inquiry, the Department provided us with a list from the Department's document management system of 25 completed firewall changes made during the period July 1, 2010, through June 8, 2011. We noted that, contrary to *DIS Firewall Configuration Procedure* and as similarly noted in connection with our report No. 2011-030, 11 completed firewall changes were not approved by management prior to implementation. We further tested 5 of the completed firewall configuration changes. Our audit tests disclosed that, as similarly noted in connection with our report No. 2011-030, Department staff were unable to provide documentation of notifications to affected users or certification of successful testing by application owners for any of the 5 changes. Under these conditions, the risk was increased that firewalls may not be adequately configured to protect IT resources from attack.

Recommendation: The Department should ensure that all changes to the firewall configuration are approved and tested and that affected users are notified of the changes as provided in the *Firewall Configuration Procedure*.

Finding No. 8: Policies and Procedures

Each Division within the Department needs complete, well-documented policies and procedures to describe the scope of the function, its activities, and the interrelationships with other Divisions. Policies establish the Department's direction, while procedures indicate how policies are to be implemented and followed. Effective policies and procedures are periodically updated to reflect changes that have occurred in the business environment and clearly communicated and disseminated to staff.

Our audit disclosed that some Department policies and procedures relating to FLAIR were outdated, inaccurate, lacking, or not effectively disseminated to staff. Specifically:

DIS Policies and Procedures

- Some DIS policies and procedures referenced obsolete or outdated methods for granting and reviewing the appropriateness of user access privileges and described incorrect password length requirements.
- Confidential procedures DIS-102, *FLAIR Resources Security Administration and Access Control,* and DIS-125, *Natural Security Access Control Procedures,* were not accessible to DIS staff responsible for Natural Security administration.

BOSP Policies and Procedures

- Some portions of the *BOSP Payroll Preparation Manual* were outdated and contained inaccuracies with regard to the use of payroll certifications, methods to submit change orders, and the processing of nonrecurring payments and beneficiary payments.
- Some BOSP payroll desk procedures for reconciling biweekly and supplemental payrolls and miscellaneous adjustments did not reflect current practices and contained inaccuracies with regard to the use of reports and processes used in the reconciliation of payrolls, the change in processing of insurance refunds, and the use of Batch Control Input Sheets.

DAC Access Control Procedures

The Department's Administrative Policies and Procedures (AP&P) 1-02, *Internal Controls Policy*, Section VII, provides that business process owners are responsible for developing policies that identify the business process owner, describe the process and its objectives, and identify roles and responsibilities for managing risk areas. AP&P 4-05, *Application Access Control*, Section VIII, requires application owners to develop written procedures for controlling access to their

applications. Specifically, AP&P 4-05 provides that written procedures shall include standards detailing how the business unit determines who should have access to their applications and any approvals that may be needed.

Our audit disclosed that the Department did not have written procedures that provided standards for how business units were to determine who should have Statewide access privileges to DAC. Additionally, the Division of Administration did not have written procedures that provided standards for determining who should have access privileges to DAC.

The Department's *Access Control Business Process Procedure for OLO 4390* did not reflect changes to available DAC access privileges resulting from the consolidation of the Statewide vendor file that occurred in February 2011.

Without current, accurate, written, and well-disseminated policies and procedures, the risk was increased that IT controls may not be followed consistently and in a manner pursuant to management's expectations.

Recommendation: The Department should update and correct inaccuracies in existing policies and procedures. Additionally, the Department should ensure that procedures are communicated and made available to all appropriate staff.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2011-030.

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 2011 through July 2011 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. An additional objective was to determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2011-030.

The scope of our audit focused on evaluating selected Department IT controls applicable to financial reporting during the period July 1, 2010, through June 30, 2011. The audit included selected general IT controls over systems modification; business contingency plans and backups; logical access to programs, data, and data files; and physical access. The audit also included selected application IT controls and selected user controls relevant to the FLAIR components: CAC, DAC, and Payroll.

In conducting our audit, we:

- Interviewed Department personnel.
- 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; and the user account administration process.
- Observed and tested the effectiveness of selected controls over the authorization, documentation, testing, approval, and implementation of 30 DAC, CAC, and Payroll Component program changes completed between July 1, 2010, and March 15, 2011.
- Observed and tested the effectiveness of selected input, processing, and output controls, as well as exception reporting and manual follow-up procedures, for the General Ledger Subsystem, Contracts and Grants Subsystem, SWFS Subsystem, 1099 Processing Subsystem, W-9 Web site, Salary Calculate Subsystem, and Cancellation and Adjustments Subsystem.
- Observed and evaluated the controls surrounding the transfer of data between DAC, CAC, the Payroll Component, and other applications and external entities, including reconciliation processes and procedures.
- Observed and evaluated the effectiveness of selected logical access controls in ensuring that access privileges to DAC, CAC, the Payroll Component, network, database, production data files, and operating system was appropriately restricted and provided an adequate separation of duties.
- Tested the effectiveness of DAC, CAC, Payroll Component, network, Resource Access Control Facility (RACF), and Natural Security password settings to evaluate the effectiveness of the settings in adequately protecting IT resources.
- Evaluated on a sample basis the effectiveness of procedures for documenting and authorizing user access privileges to DAC, CAC, the Payroll Component, and system resources. Specifically, we reviewed a sample of 30 new hires to the Division of Administration, A&A, and DIS with Department start dates between July 1, 2010, and March 31, 2011, to determine whether the access granted was documented and authorized.
- Observed and evaluated the adequacy of physical access controls to IT resources and other sensitive application processing areas located within the Department's facilities. In addition, we reviewed the appropriateness of physical access privileges to the DIS secured IT areas.
- Evaluated the effectiveness of controls for timely disabling the access privileges of former employees and contractors. Specifically, we reviewed a list of 344 employees and contractors who terminated employment or contractual services during the period July 1, 2010, through March 31, 2011, to determine if DAC, CAC, and Payroll Component access privileges were timely disabled. Additionally, from the Department-provided list, we reviewed a sample of 30 former employees and contractors to determine if network, RACF, Natural Security, Fletcher Building, and Larson Building access privileges were timely disabled.
- Observed and evaluated the appropriateness of selected control activities surrounding backup and retention procedures for network, DAC, CAC, and Payroll Component data and program files.
- Observed and evaluated the appropriateness of the Department's security awareness program. Specifically, we reviewed a sample of 45 of 313 employees hired by the Department between July 1, 2010, and March 31, 2011, to determine if employees received security awareness training.
- Observed and evaluated Department policies and procedures that provide for management and implementation of application, firewall, and production schedule changes including authorization, documentation, testing, security reviews, and problem resolution.
- Observed and evaluated the appropriateness of the FLAIR application contingency plans including the DIS and A&A Disaster Recovery Plans.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.
- Made inquiries and reviewed related documentation regarding the status of the Department's plans to implement the 3-percent withholding of Federal tax from applicable payments pursuant to Title 26, Section 3402(t), United States Code.

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 24, 2011, 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 24, 2011

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 audit finding to be included in the Auditor General's information technology operational audit of the *Department of Financial Services Florida Accounting Information Resource (FLAIR) Subsystem*.

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

Sincerely,

Jeff Atwater

JA/sll

Enclosure

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

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES

INFORMATION TECHNOLOGY OPERATIONAL AUDIT OF THE

DEPARTMENT OF FINANCIAL SERVICES

FLORIDA ACOCUNTING INFORMATION RESOURCE (FLAIR) SUBSYSTEM

Finding No. 1: Appropriateness of Access Privileges

The access privileges of some Department users were not appropriate for their job responsibilities.

Recommendation: The Department should limit user access privileges to only what is necessary for user job responsibilities. Additionally, the Department should ensure that periodic reviews of DAC and HAC Statewide access privileges contain sufficient information to determine whether assigned access privileges remain appropriate and commensurate with job responsibilities. The Department should also expand its review of Payroll Component access privileges to include users within DIS.

Response: We concur. The Division of Accounting and Auditing will create new access control procedures for users needing Statewide access to Departmental FLAIR's environments for the Departmental Accounting Component (DAC) and the DAC data base file for the Department of Children and Families (HAC). These procedures will identify all the positions that should be granted access and the type of access to be granted based on the position's job responsibilities. In conjunction with the new procedures, the Division of Accounting and Auditing will implement quarterly reviews to ensure compliance with the Statewide access procedures.

The Division of Accounting and Auditing will update access control procedures for users needing access to the available budget override function in the Central FLAIR Central Accounting Component (CAC), for all Division of Accounting and Auditing users (OLO 4390) accessing Departmental FLAIR's DAC and HAC environments, and for all users accessing FLAIR's payroll component. The Division of Accounting and Auditing will verify that the procedures reflect all the positions that should be granted access and the type of access to be granted based on the position's job responsibilities. In conjunction with the revised procedures, the Division of Accounting and Auditing will take steps to include all positions in the quarterly reviews to ensure compliance with the division's OLO 4390 and Payroll access procedures that was previously missing.

The Division of Information Systems has limited access privileges to the W-9 Web Site Production Program Code to only those positions necessary based on user job responsibilities. The Division of Information Systems has also limited network folder access privileges to only those positions necessary based on user job responsibilities. Additionally, inherited access privileges are denied for the Bureau of State Payrolls folder. As noted in the audit report, the Division of Information Systems has modified the access review report to include sufficient detail for determining the appropriateness of access privileges.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 2: Timely Disabling of Network Access Privileges

As similarly noted in prior audits of the Department, most recently our report No. 2011-030, the Department did not disable the network access privileges of some former employees in a timely manner.

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

Response: We concur. Department management is actively working to enhance procedures to ensure timely disablement of network access privileges for separating employees. Additionally, the Division of Information Systems has already implemented a monitoring tool to more accurately record the actual date privileges were disabled.

Finding No. 3: Other Security Controls

Certain Department security controls related to security event logging, logical access, and data transmission needed improvement. Some of the issues were also noted in our report No. 2011-30.

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

Response: We concur. The Department has implemented improvements in some areas, and is working to enhance security controls in other areas noted in the report.

Finding No. 4: Access Control Records Retention

Contrary to the requirements of the State of Florida, ***General Records Schedule*** for the retention of access control records, the Department did not retain some network and Natural Security access control records.

Recommendation: The Department should ensure that access control records are retained as required by the ***General Records Schedule***.

Response: We concur. The Division of Information Systems has taken steps to ensure proper retention of network and Natural Security access control records through proper logging and retention of log files for the time period required by the ***General Records Schedule***.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 5: Comprehensive Configuration Repository

As similarly noted in our report No. 2011-030, the Department did not maintain a comprehensive configuration repository of its IT infrastructure and applications.

Recommendation: The Department should implement a central comprehensive configuration repository to facilitate the management and control of its IT infrastructure and applications.

Response: We concur. The Department is in the process of implementing a multi-repository solution to expand management of its information technology infrastructure. Existing repositories are being updated, as needed. The Department has also procured an additional configuration management database and is defining business requirements for planned deployment.

Finding No. 6: Security Awareness Training

As similarly noted in prior audits of the Department, most recently our report No. 2011-030, the Department did not provide initial security awareness training for some agency workers or periodic refresher training for all agency workers.

Recommendation: The Department should provide initial and periodic refresher security awareness training for all Department workers, including salaried employees, contractors, volunteers, and OPS employees.

Response: We concur. The Department, in coordination with the Division of Information Systems, will provide initial and periodic refresher security awareness training for all Department workers beginning November 2011.

Finding No. 7: Firewall Configuration Management

As similarly noted in our report No. 2011-030, Department firewall configuration management controls needed improvement.

Recommendation: The Department should ensure that all changes to the firewall configuration are approved and tested and that affected users are notified of the changes as provided in the ***Firewall Configuration Procedure***.

Response: We concur. The Division of Information Systems will enhance procedures related to firewall configuration changes.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 8: Policies and Procedures

Some Department policies and procedures were outdated, inaccurate, lacking, or not effectively disseminated to staff. The Department also lacked written procedures for some Departmental Accounting Component (DAC) access control processes.

Recommendation: The Department should update and correct inaccuracies in existing policies and procedures. Additionally, the Department should ensure that procedures are communicated and made available to all appropriate staff.

Response: We concur. The Division of Information Systems is in the process of reviewing all Division policies and procedures. The Division of Information Systems' operating policies and procedures are available to Division employees on the Division's intranet. Each Division employee will have access only to those policies and procedures for which they have security rights. The Division of Information Systems is in the process of developing procedures to ensure division employees are informed of changes to internal operating policies and procedures.

The Division of Accounting and Auditing will update the *Payroll Preparation Manual* and the Bureau of State Payrolls' desk procedures for *Biweekly Payroll, Supplemental Payroll, and Miscellaneous Adjustments* to reflect the current payroll processing practices. The Division issues memoranda to agencies of updates to the preparation manual and communicates directly with the appropriate staff concerning updates to the desk procedures.

The Division of Administration has updated its written procedures to ensure they are current, accurate, and complete. The Division of Administration provides direct, verbal notification to its employees of revisions to internal procedures. These procedures are available to Division of Administration employees on a shared drive. The Division of Administration also notifies Department employees by e-mail of changes to Departmental Administrative Policies and Procedures.