REPORT NO. 2013-078
JANUARY 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 Brenda Shiner, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CITP, 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 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 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. 2012-016.

The results of our audit are summarized below:

Finding No. 1: As similarly noted our report No. 2012-016, 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. 2012-016, the Department did not deactivate the access privileges of some former employees and contractors in a timely manner.

Finding No. 3: The Department did not maintain access authorization forms for some users.

Finding No. 4: Certain Department security controls related to security event logging, logical access, the protection of confidential and exempt information, and risk management needed improvement. Some of the issues were communicated to Department management in connection with our report No. 2012-016.

Finding No. 5: As similarly noted in prior audits of the Department, most recently our report No. 2012-016, the Department did not maintain a comprehensive configuration repository of its IT infrastructure and applications.

Finding No. 6: The Department's monitoring of program changes needed improvement.

Finding No. 7: As similarly noted in our report No. 2012-016, some Department procedures were outdated, inaccurate, or lacking.

BACKGROUND

FLAIR 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 as a cash-basis system 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 Families (DCF) and one for all the other State agencies. The DAC database file for DCF 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.

The 2012 General Appropriations Act, Chapter 2012-118, Laws of Florida, 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 provide a recommendation for the replacement or remediation of FLAIR and CMS. It also provided that, at a minimum, the study shall include:

- An inventory of all agency financial business systems to include a description of each system's accounting and reporting functions and its number of users;
- The completion of a gap analysis to determine which agency accounting and reporting requirements are currently not provided in FLAIR or CMS and an identification of those requirements that are common across agencies;
- Documentation of all business and technical requirements needed for FLAIR and CMS to automate system interfaces with the personnel information system, the purchasing subsystem, and the planning and budgeting subsystem and adhere to the current statutes related to financial reporting and information;
- A cost-benefit analysis for replacing or remediating FLAIR and CMS to accommodate the needs of all State agencies for compliance with State and Federal financial accounting and reporting laws.

On October 19, 2012, the Department issued a Statement of Work and Request for Quotes (SOW) for a FLAIR Replacement Study. The SOW specified that the Department intended to follow an incremental and deliberate approach to replacing FLAIR using a phased approach. Phase 1 (the scope of the SOW) will include a validation and critique of the Department's proposed approach for replacing FLAIR and a review of the business requirements previously identified in 2002. Phase 2 will include the planning, procuring, and implementing of the replacement of CAC. Phase 3 will include organization change management activities. Phase 4 will include a requirements gap analysis and planning, procuring, and implementing the replacement of DAC.

The Department does not anticipate the total of all services in the SOW, Phase 1 (excluding optional services), to exceed $700,000. The contractor responses to the SOW were due on November 9, 2012. As of November 19, 2012, the Department was working with legislative staff to review the requirements in the SOW and determine how to proceed with the award.

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. Some inappropriate access privileges existed to DAC, CAC, W-9 and W-2 Web site production code, and group e-mail account access, as discussed in the following paragraphs.

DAC

Our review of users with Statewide or Departmental update access privileges to selected functions within DAC as of April 30, 2012, disclosed that eight users from various areas of the Department had update access privileges to one or more functions that were inappropriate for their job responsibilities. A similar finding regarding inappropriate DAC access was disclosed in our report No. 2012-016. Specifically:

- One user's Statewide update access privileges to the State Chief Financial Officer files were inappropriate for his job responsibilities.
- One user's update access privileges to the Cash Receipts and Disbursements functions were inappropriate for her job responsibilities.
- One user's update access privileges to the Fixed Assets Custodial Account function were inappropriate for her job responsibilities.
- Five users' update access privileges to the Statewide Financial Statements functions that allowed them to execute batch jobs were inappropriate for their job responsibilities.

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 users with CAC override or update access privileges as of March 30, 2012, disclosed that, contrary to the *CAC Access Control Business Process Procedures*, some CAC users had access privileges to one or more functions that were inappropriate for their job responsibilities. A similar finding regarding CAC access privileges was disclosed in our report No. 2012-016. Specifically:

- Of the 22 users who had access privileges to Audit Override functions, 10 had access privileges that were inappropriate for their job responsibilities.
- Of the 32 users who had access privileges to Special Flag Override functions, 2 had access privileges that were inappropriate for their job responsibilities.
- Of the 94 users who had access privileges to update functions, 2 had access privileges that were inappropriate for their job responsibilities. Specifically, one user had inappropriate update access to the Vendor Request for 1099 Returns function and one user had inappropriate update access privileges to the Accounting Input function.

Our review of 76 users with inquiry access privileges as of March 30, 2012, to CAC functions that contained confidential banking information such as bank account numbers disclosed that 45 Division of Retirement users had been granted inquiry access privileges to the two CAC functions containing confidential information. The inquiry access privileges were inappropriate for the Division of Retirement employees' job responsibilities.

We reviewed the 12 user accounts with inquiry access privileges to the CAC production database that contains confidential and exempt information. Our review disclosed that one user account was inappropriate. In response to audit inquiry, Department staff deactivated the user account on October 17, 2012.

Selected CAC Functions – DAC Users

Our review of 31 DAC users who had update access privileges to selected CAC functions disclosed that 7 DAC users were assigned inappropriate CAC update access privileges based on their job responsibilities. Specifically, 6 users had inappropriate access to CAC Warrant Cancellation functions. One user had inappropriate access to CAC Warrant Cancellation and Prompt Payment Compliance functions.

W-9 Web Site Production Program Code

Our review of users with access privileges to the FLAIR production program code for the W-9 Web site disclosed that a programmer access group was configured incorrectly. As a result, eight users had inappropriate update access privileges to the FLAIR production program code for the W-9 Web site based on their job responsibilities. A similar finding regarding inappropriate W-9 Web site production program code access privileges was disclosed in our report No. 2012-016.

W-2 Web Site Production Program Code

Our review of users with access privileges to the FLAIR production program code for the W-2 Web site disclosed that a programmer access group was configured incorrectly. As a result, seven users had inappropriate update access privileges to the FLAIR production program code for the W-2 Web site based on their job responsibilities.

Group E-Mail Account Access

FLAIR reports containing confidential information and exempt information such as social security numbers and bank account numbers were routinely e-mailed from the mainframe to a group e-mail account, Direct Deposit. Our review of user accounts that were granted full control access privileges to the Direct Deposit group e-mail account disclosed that 6 of the 14 user accounts were inappropriate based on the job responsibilities of the users.

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 the users' job responsibilities.

Finding No. 2: Timely Deactivation of Access Privileges

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(6), Florida Administrative Code, provides that access authorization shall be promptly removed when the user's employment is terminated or access to the information is no longer required. Prompt action is necessary to ensure that a former employee, contractor, or others do not misuse the former employee's or contractor's access privileges. Department Administrative Policies and Procedures (AP&P) 4-05, *Application Access Control*, *(AP&P 4-05)*, states that retaining user accounts for separated users beyond their last day of work is a security risk and is prohibited. Contrary to *AP&P 4-05*, the network and DAC access privileges of some former employees and contractors were not timely deactivated after their dates of termination. Specifically:

Network

We reviewed network access privileges for a sample of 29 of the 367 Department employees and contractors who terminated employment or contractual services during the period July 1, 2011, through April 30, 2012, as provided by Department staff. Our review disclosed instances where, as similarly noted in prior audits of the Department, most recently our report No. 2012-016, the network access privileges of some former employees and contractors had not

[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.

been timely deactivated. Specifically, the network access privileges of 2 former employees and 2 former contractors remained active for periods ranging from 5 to 42 days after termination. The network access privileges of the 2 former employees and 1 of the former contractors were not used after their dates of termination. However, for the remaining former contractor, the Department was unable to determine if his access was used after his termination date.

DAC

Of the 367 former Department employees and contractors, 28 former employees had DAC access privileges during the period. Our review of the DAC access privileges for the 28 former employees disclosed that 4 former employees retained access privileges after their dates of termination. The access privileges for 3 of the 4 former employees had been deactivated as of the date of our test, but had remained active for periods ranging from 2 to 81 days after their dates of termination. The access privileges of the remaining former employee remained active as of the date of our test, which was 38 days after termination. The Department was unable, upon audit inquiry, to determine whether the DAC access privileges of the 4 former employees were used after their dates of termination.

Without timely deactivation of former employee and contractor access privileges, the risk is increased that the access privileges could be misused by the former employees, contractors or others.

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

Finding No. 3: Access Authorizations

AEIT 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. For 16 of the 19 user accounts, authorization documentation for the user access privileges did not exist.

The access request process currently in place was implemented in June 2006 and 16 of the 19 users included in our test had been granted access before the implementation of the current process. Access authorization documentation for 15 of the 16 users noted above was unavailable from the current process, and other prior access authorization documentation that might have existed had not been retained. 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 responsibilities.

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

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 in the areas of security event logging, logical access, protection of confidential and exempt information, and risk management 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 our report No. 2012-016. Without adequate security controls in the areas of security event logging, logical access, the protection of confidential and exempt information, and risk management, the confidentiality, integrity, and availability of data and IT resources may be compromised.

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

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 prior audits of the Department, most recently our report No. 2012-016, 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.

As of August 6, 2012, the Department was in the process of upgrading and enhancing its IT service management application, Remedy, to include the building of a configuration management database to serve as a component of its configuration repository. The Department finished phase one of a three-phase Remedy rollout in July 2012. Phase two was planned by the Department to include the building of the configuration management database. However, a planned implementation date for the Remedy enhancements and the configuration management database had not been established by the Department.

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 continue efforts to implement a central comprehensive configuration repository to facilitate the management and control of its IT infrastructure and applications.

Finding No. 6: Change Management

Effective controls over the modification of application programs include provisions for ranking (prioritizing) and scheduling program changes so that authorized change requests are implemented timely, efficiently, and in accordance with user needs. DIS operating procedure *DIS-001, FLAIR Applications Systems Development*, Section III, sets forth requirements for assessing requested programming changes based on need, technical feasibility, and priority.

We reviewed a report of all Data Processing Requests (DPRs) as of June 1, 2012, that showed all requested program changes related to FLAIR. Of the 2,558 DPRs shown on the report, we noted that 84 DPRs requested prior to the current fiscal year were not completed or canceled as of June 1, 2012. In response to audit inquiry, Department management reviewed all 84 open DPRs and determined that 50 of the 84 DPRs should have been marked as canceled or completed; however, the status of the DPRs had not been updated accordingly. The remaining 34 DPRs were either currently in process or on hold. Department management indicated that the status of the DPRs was not always being updated because the Department had not implemented an ongoing review process for monitoring aged DPRs. Our inspection of the 34 remaining DPRs and discussions with Department management disclosed that none of the DPRs would have had a significant effect on IT controls relevant to FLAIR financial reporting for the period under audit. Nevertheless, the lack of effective procedures for prioritizing and monitoring program change requests increases the risk that authorized change requests may be overlooked and not implemented timely, efficiently, or in accordance with user needs.

Recommendation: The Department should implement a process to monitor the status of existing DPRs and ensure that the status information for each DPR is current.

Finding No. 7: Department Procedures

To remain relevant and effective, written procedures should be periodically reviewed and updated to reflect the changes in the business focus and environment. As similarly noted in our Report No. 2012-016, some Department procedures relating to FLAIR were outdated, inaccurate, or lacking. Specifically:

DIS Procedures

Some DIS procedures referenced obsolete or outdated methods for granting and reviewing the appropriateness of user access privileges and described incorrect password length requirements. In response to audit inquiry, Department staff provided a revised copy of one of the procedures, *DIS-126, Providing and Monitoring of Data Center and Computer Room Access*, that was approved and implemented on September 7, 2012. The revised procedure reflected DIS practices in effect as of the completion of our audit.

DAC Procedures

The Department's *AP&P 1-02, Internal Controls Policy*, Section VII, provides that business process owners are responsible for developing policies that 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 determined 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. Also, Agency Addressed Memorandum No. 20, 2010-2011, issued by the Department on February 7, 2011, stated that a limited number of users within each agency will be granted the ability to add new vendors to the Statewide vendor file. Although users requiring access privileges for adding vendors must request access in writing on the *Statewide Vendor File "ADD" Authorization Request* form, the Vendor Management Section within A&A did not have procedures in place for approving and assigning the access privileges for adding vendors.

Without current, accurate, and written procedures, the risk is 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 procedures. Additionally, pursuant to *AP&P 4-05*, the Department should develop procedures that detail how the business units determine who should have access to their applications. Furthermore, the Department should develop procedures for approving and assigning access privileges for adding vendors to the Statewide vendor file.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2012-016.

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 April 2012 through September 2012 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. 2012-016.

The scope of our audit focused on evaluating selected Department IT controls applicable to financial reporting during the period July, 1, 2011, through June 30, 2012, and selected Department actions through November 19, 2012. The audit included selected general IT controls over systems modification; logical access to programs, data, and data files; physical access; and patch management. The audit also included selected application IT controls and selected user controls relevant to FLAIR components: Central Accounting, Departmental Accounting, 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 CAC, DAC, 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, documentation, testing, approval, and implementation of 25 CAC, DAC, and Payroll Component program changes completed between July 1, 2011, and June 22, 2012.
- Evaluated 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, Prompt Payment Subsystem, and Cancellation and Adjustments Subsystem.
- Evaluated the effectiveness of the controls surrounding the transfer of data between CAC, DAC, the Payroll Component, and other applications and external entities, including reconciliation processes and procedures.
- Evaluated the effectiveness of selected logical access controls in ensuring that access privileges to CAC, DAC, the Payroll Component, network, database, production data files, and operating system were appropriately restricted and provided an adequate separation of duties.
- Tested the effectiveness of DAC, Payroll Component, network, mainframe, database, and program library security password settings to evaluate the effectiveness of the settings in adequately protecting IT resources.
- Evaluated the effectiveness of procedures for documenting and authorizing user access privileges to CAC, DAC, the Payroll Component, and other IT resources. Specifically, we reviewed access granted for a sample of 10 of 57 new hires in the Division of Administration, A&A, and DIS with Department start dates between July 1, 2011, and April 30, 2012, to determine whether the access granted was documented and authorized. Additionally, we tested 19 users with access to move FLAIR program changes to production as of July 23, 2012, to determine whether the access granted was documented and authorized.

- Evaluated the effectiveness of controls for timely deactivating the access privileges of former employees and contractors. Specifically, we reviewed a list of 367 employees and contractors as provided by the Department who terminated employment or contractual services during the period July 1, 2011, through April 30, 2012, to determine if CAC, DAC, and Payroll Component access privileges, if assigned, were timely deactivated. Additionally, on a sample basis from the Department-provided list of 367 former employees and contractors, we reviewed access privileges for 30 former employees and contractors to determine if network, mainframe, program library, Fletcher Building, and Larsen Building access privileges, if granted, were timely deactivated.
- Evaluated the effectiveness of the Department's security awareness training program. Additionally, we reviewed a sample of 20 of 192 employees hired by the Department between July 1, 2011, and April 30, 2012, to determine if they received timely security awareness training when hired.
- Evaluated the effectiveness of software patch management procedures followed by the Department.
- Evaluated the effectiveness of selected controls over the authorization, testing, approval, and implementation of Department firewall configuration changes. Specifically, we reviewed a sample of 7 of 56 firewall configuration changes made by the Department between March 22, 2012, and June 30, 2012.
- Evaluated the adequacy of physical access controls to IT resources and other sensitive areas located within the Department's facilities. In addition, we reviewed the appropriateness of physical access privileges to DIS secure IT areas for 73 individuals as of June 5, 2012.
- Evaluated Department policies and procedures for prioritizing and monitoring the status of FLAIR program changes.
- Evaluated the appropriateness of access privileges to Department confidential and exempt information, including the disaster recovery plan, bank account information, and social security numbers.
- 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 January 7, 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.

EXHIBIT A
MANAGEMENT'S RESPONSE

CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

January 7, 2013

Via Hand-Delivery

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

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's 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, Interim Inspector General, at (850) 413-4960.

Sincerely,

Jeff Atwater

JA:Kg

Enclosure

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

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Financial Services
Florida Accounting Information Resource Subsystem (FLAIR)
Information Technology Operational Audit
Preliminary and Tentative Findings
Audit Response

Finding No. 1: Appropriateness of Access Privileges

As similarly noted in our report No. 2012-016, 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 the users' job responsibilities.

Response: We concur. The Division of Information Systems limited statewide access privileges to select functions in the Departmental Accounting Component. Additionally, the Division limited access to the W-9 and W-2 Web Site Production Program Code to the extent possible, based on user job responsibilities and enhanced procedures to further ensure appropriate separation of duties.

CAC access privileges to the Audit Override function, Special Flag Override function, Vendor Request for 1099 Returns function, and the Accounting Input function have been reviewed and updated by the Division of Accounting and Auditing based on the employee's job responsibilities. The Division has reviewed CAC access to functions that contained confidential banking information for the 45 Division of Retirement employees. Access has been entirely removed for three (3) employees and access has been reduced for another nine (9) employees. Once the Division of Retirement implements its Direct Deposit Website in March 2013, CAC access will be terminated for all Division of Retirement staff.

The Division of Accounting and Auditing reviewed the Direct Deposit group E-Mail account in August 2012. Inappropriate access was removed, and is now limited to EFT personnel and Division management.

Finding No. 2: Timely Deactivation of Access Privileges

As similarly noted in prior audits of the Department, most recently our report No. 2012-016, the Department did not deactivate the access privileges of some former employees and contractors in a timely manner.

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

Response: We concur. The Department has enhanced procedures to further ensure timely disablement of network access privileges for separating employees. Additionally, the Department continues to communicate the importance of timely reporting of separations to ensure timely deactivation of accounts.

1

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 3: Access Authorizations

The Department did not maintain access authorization forms for some users.

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

Response: We concur. The Department, however, has accepted the risk associated with the absence of access authorization documentation for employees who began employment prior to the implementation of the documentation in 2006. Since the document was implemented, it is completed for all new employees and for any employees who move positions within the Department. Additionally, the Department will provide training on procedures to ensure access to Department secure applications is reviewed on a quarterly basis.

Finding No. 4: Other Security Controls

Certain Department security controls related to security event logging, logical access, the protection of confidential and exempt information, and risk management needed improvement. Some of the issues were communicated to Department management in connection with our report No. 2012-016.

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

Response: The Department has improved security controls in some areas noted in the report and will continue to address security controls in other areas, as appropriate.

Finding No. 5: Comprehensive Configuration Repository

As similarly noted in prior audits of the Department, most recently our report No. 2012-016, the Department did not maintain a comprehensive configuration repository of its IT infrastructure and applications.

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

Response: We concur. The Department continues to leverage multiple repository solutions to manage its information technology infrastructure. Existing repositories are being updated as needed, and the remaining phases of the Remedy enhancement are being planned.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 6: Change Management

The Department's monitoring of program changes needed improvement.

Recommendation: The Department should implement a process to monitor the status of existing DPRs and ensure that the status information for each DPR is current.

Response: We concur. The Department has enhanced procedures to ensure that Data Processing Request statuses are updated timely.

Finding No. 7: Department Procedures

As similarly noted in our report No. 2012-016, some Department procedures were outdated, inaccurate, or lacking.

Recommendation: The Department should update and correct inaccuracies in existing procedures. Additionally, pursuant to ***AP&P 4-05***, the Department should develop procedures that detail how the business units determine who should have access to their applications. Furthermore, the Department should develop procedures for approving and assigning access privileges for adding vendors to the Statewide vendor file.

Response: We concur. The Division of Information Systems continues in its efforts to review and update existing Division policies and procedures. The Division of Accounting and Auditing's *Access Control Business Process Procedures for OLO 4390* will be updated to reflect DAC access changes associated with the Statewide Vendor File. The Division of Accounting and Auditing has also updated, corrected inaccuracies, and implemented its desk procedures related to agency requests for access to the Statewide Vendor (VS) file.

The Division of Administration updated Internal Policy & Procedure 2.2.01, FLAIR Access Control, as a result of last year's audit finding. Specifically, the Department requires supervisors to certify that the requested FLAIR access is compatible with the employee's duties and is reflected in the official position description. AP&P 4-05 states that the supervisor is responsible for ensuring that access privileges are based on the user's job responsibilities (see VII.J.1.). In addition, AP&P 4-05 states that it is the supervisor's role to determine the user's access (see VIII.A.1.). This is consistent with the procedure outlined in IP&P 2.2.01. The Division will modify said policies to resolve any discrepancies.