REPORT NO. 2011-030
NOVEMBER 2010

DEPARTMENT OF FINANCIAL SERVICES

FLORIDA ACCOUNTING INFORMATION RESOURCE (FLAIR) SUBSYSTEM

Information Technology Operational Audit

For the Period
July 1, 2009, Through June 30, 2010,
and Selected Actions Through August 18, 2010

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

CHIEF FINANCIAL OFFICER

Pursuant to Article IV, Sections 4(c) and 5(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Alex Sink served as Chief Financial Officer during the audit period.

The audit team leader was 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) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF FINANCIAL SERVICES

Florida Accounting Information Resource (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 system during the period July 1, 2009, through June 30, 2010, and selected actions through August 18, 2010. We also determined the status of corrective actions regarding audit findings included in our report No. 2010-021.

The results of our audit are summarized below:

Finding No. 1: The access privileges of some Division of Information Systems (DIS) users were not appropriate for their job responsibilities and did not enforce an appropriate separation of duties.

Finding No. 2: As similarly noted in our report No. 2010-021, the Department did not disable or remove the access privileges of some former and reassigned employees in a timely manner.

Finding No. 3: The Department did not maintain a comprehensive configuration repository of its IT infrastructure and applications.

Finding No. 4: As similarly noted in our report No. 2010-021, the Department did not provide initial security awareness training for some employees or periodic refresher training for all employees. Additionally, the Department did not identify and document training requirements for systems administrators, contrary to Department policy.

Finding No. 5: In addition to the matters discussed in Finding Nos. 1, 2, and 4, certain Department security controls needed improvement. Our prior reports on the Department have included some of the same issues.

Finding No. 6: Network backup processes needed improvement with regard to the rotation of backup tapes to an off-site storage location and review of network backup reports.

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. 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 deduct and withhold a tax of 3 percent from all payments to entities providing property or services, except as provided therein. The effective date of the withholding requirement is for payments made after December 31, 2011. Withholding is scheduled to begin on January 1, 2012, with the first Federal reporting to be submitted in January 2013.

Although Federal regulations to govern the 3-percent withholding had not been finalized, the Department was in 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 will require extensive program modifications to FLAIR. At the completion of our audit period, the Department was in the business requirements and design phase. The target date for implementation of the 3-percent withholding is January 2012.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to only what is needed in the performance of assigned job responsibilities. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

Our audit disclosed that some DIS users had inappropriate access privileges to FLAIR production program code, job control language (JCL), and database files. These conditions increase the risk of unauthorized disclosure, modification, or destruction of Department data. Specifically:

- Five users had inappropriate update access privileges to the FLAIR Natural production code. The users included a systems programmer within the Bureau of Operations and Customer Services, Mainframe Systems Section, and four database administrators (DBAs) within the Office of Enterprise Applications and Infrastructure, Data Management Section. In response to audit inquiry, Department staff indicated that the systems programmer and DBAs often assist the programmers in researching production problems but did not need to have the ability to update the programs. Therefore, on June 25, 2010, Department staff modified the inappropriate update access privileges for the five users to read-only access privileges.
- Forty-five user accounts belonging to 17 users within DIS had inappropriate update access privileges to production JCL. The user accounts belonged to users in the Mainframe Systems and Operations Sections within the Bureau of Operations and Customer Services. In response to audit inquiry, Department staff removed the inappropriate update access privileges to the production JCL for the users in the Bureau of Operations and Customer Services, Mainframe Systems Section on May 20, 2010, and for the users in the Bureau of Operations and Customer Services, Operations Section on June 23, 2010.
- Twenty-four user accounts belonging to 16 users had inappropriate update access privileges to production database files that contained both production program code and data. The user accounts belonged to the PRODCNT group and included staff in the Mainframe Systems and Operations Sections within the Bureau

of Operations and Customer Services. In response to audit inquiry, Department staff indicated that these access privileges had been required to perform backup and restore procedures; however, in recent years the process was changed and the access privileges were no longer required to perform these procedures. Accordingly, Department staff removed the update access privileges for the PRODCNT group on August 2, 2010.

Additionally, through our review of users with access privileges to FLAIR production program code, our audit disclosed that seven application programmers were defined as Natural administrators in Natural Security within the production databases. Natural administrators may use libraries directly and create and modify security profiles. The combination of programming and security administration capabilities was contrary to an appropriate separation of duties and increased the risk that Department data and IT resources could be subject to improper disclosure, modification, or destruction. In response to audit inquiry, Department staff indicated that the programmers' Natural administrator access privileges were removed on August 12, 2010.

Recommendation: The Department should continue its efforts to limit access privileges to only what is needed in the performance of employee job functions.

Finding No. 2: Timely Disabling and Removing of Access Privileges

Effective management of system access privileges includes provisions to timely disable or remove employee and contractor access privileges when employment or contractual terminations and reassignments occur. The access privileges that should be timely disabled or removed include both logical and physical access privileges to information and facilities. Prompt action is necessary to ensure that a former employee's or contractor's access privileges are not misused by the former or reassigned employee, contractor, or others.

We reviewed logical access privileges for DAC, HAC, CAC, the Payroll Component, the network, Resource Access Control Facility (RACF), and Natural Security for 379 Department, Office of Insurance Regulation (OIR), and Office of Financial Regulation (OFR) employees and contractors, who terminated employment or contractual services during the period July 1, 2009, through March 31, 2010. Our review disclosed instances where, as similarly reported in our report No. 2010-021, the access privileges of some former employees had not been timely disabled. For our review purposes, we considered the disabling of access privileges to have been timely if it occurred within the next business day after termination. Specifically:

- One former A&A employee whose DAC and HAC access privileges were still active at the time of our testing. In response to audit inquiry, Department staff disabled the former employee's access privileges on June 7, 2010, 158 days after termination.
- One former DIS employee whose DAC access privileges remained active for a period of 2 days after termination.
- One former OFR employee whose Payroll Component access privileges remained active for 7 days after termination.
- Two former employees whose network access privileges were still active at the time of our testing on May 14, 2010. One of the former employees terminated employment from the Division of State Fire Marshall and the other from OFR. In response to audit inquiry, Department staff indicated that the network access privileges of the former Division of State Fire Marshall employee were active on May 14, 2010, because of a request to have the network access privileges restored. However, the restored network access privileges were not subsequently disabled. In response to audit inquiry, Department staff disabled the network access privileges but were unable to provide us the date the access privileges were disabled. Additionally, Department staff indicated that a defined process did not exist for restoring network access

privileges. Although Department staff had documentation indicating that the network access privileges of the former OFR employee had been disabled on March 19, 2010, staff could not provide an explanation as to why the network access privileges were subsequently active on May 14, 2010. In response to audit inquiry, Department staff again disabled the former employee's network access privileges on June 11, 2010, 86 days after termination.

- Three former employees, two from A&A and one from the Office of the Deputy Chief Financial Officer, whose RACF access privileges remained active for periods ranging from 112 to 174 days after termination. In response to audit inquiry, Department staff disabled (revoked) the RACF access privileges of the three former employees. The accounts of the three employees had a password expiration of 30 days at which point the system would automatically disable the account upon the next logon attempt. All three accounts were in a password expired status at the time of our test, indicating that, at the next logon attempt, the account would be disabled. Therefore, the accounts were at the highest risk of compromise for, at the most, 30 days.
- One former DIS employee whose Natural Security access privileges were still active. In response to our audit inquiry, Department staff indicated that the employee's access privileges were disabled on June 23, 2010, 279 days after termination.

Additionally, from a sample of 30 of the 379 Department, OIR, and OFR employees and contractors who terminated employment or contractual services during the period July 1, 2009, through March 31, 2010, we noted 2 former employees, one from OFR and one from the Division of Insurance Fraud, whose network access privileges remained active for periods of 6 and 8 days, respectively, after termination.

Through additional audit procedures, we noted that one former A&A employee who had terminated from the Department on July 14, 2006, continued to have Natural Security access privileges to one of the informational reporting databases used to retrieve accounting data for report purposes. In response to audit inquiry, Department staff indicated that the former employee's access privileges were disabled on June 23, 2010, 1,439 days after termination. Additionally, another former A&A employee who terminated from the Department on April 16, 2010, continued to have RACF access privileges. In response to audit inquiry, Department staff disabled the account on May 21, 2010, 35 days after termination.

Our review of physical access privileges of the 379 Department, OIR, and OFR employees and contractors who terminated employment or contractual services during the period July 1, 2009, through March 31, 2010, disclosed that two employees who were reassigned to other positions within the Department retained physical access to areas within Department facilities that were no longer required. Specifically:

- One DIS employee whose physical access privileges to the State Chief Financial Officer's Data Center and Fletcher Building were not removed upon the employee's reassignment to a position in another Division that did not require physical access to these facilities. In response to audit inquiry, Department staff indicated that the access privileges to the State Chief Financial Officer's Data Center were subsequently removed on May 4, 2010, 61 days after the date of the employee's reassignment. Department staff later indicated that, effective July 1, 2010, the employee was reassigned to a position that required access to the Fletcher Building. Nevertheless, the employee did not require access to the Fletcher Building between March 4, 2010, and June 30, 2010.
- One Office of Strategic Planning employee whose physical access privileges to the Fletcher Building were not removed upon the employee's reassignment to a position in another Division that did not require access to the Fletcher Building. In response to audit inquiry, Department staff indicated that access privileges to the Fletcher Building were subsequently removed on July 29, 2010, 303 days after the date of reassignment.

Without timely deletion of former or reassigned employee access privileges, the risk is increased that the access privileges could be misused by the former or reassigned employee or others.

Department management indicated they were in the process of approving changes to its Administrative Policy and Procedure (AP&P) 4-05 Application Access Control, which specifically addressed timely removal of access privileges of former employees. Additionally, the Department implemented a Remedy Help Desk process to track and notify all Division access control administrators of employee terminations. Furthermore, Department management indicated that they had designed a long-term solution and developed an implementation plan for an Information Technology Infrastructure Library (ITIL)-based configuration management database to maintain a record of all access privileges. ITIL is a widely adopted approach for IT service management best practices.

Recommendation: The Department should continue to enhance its practices to ensure that the access privileges of all former or reassigned employees are disabled or removed in a timely manner. Additionally, the Department should continue with its plans to implement an ITIL-based configuration management database to maintain a current record of all access privileges.

Finding No. 3: Comprehensive Configuration Repository

Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of a comprehensive configuration repository. A 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.

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. The Department had several separate systems (the BMC Remedy Asset Configuration Management Module, Microsoft SharePoint, Microsoft's System Center Configuration Manager, and Big Brother) that contained some of this information, but the available information did not include every component of the Department's infrastructure and applications.

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

The Department recently purchased an Auto Discovery and Dependency Mapping tool that can be used to populate a configuration management database that would serve as a repository. In response to audit inquiry, Department staff indicated that they planned to prepare a Statement of Work and Request For Quote for IT Consulting Services to assist with the implementation of the tool.

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

Finding No. 4: Security Awareness Training

Effective security awareness programs include initial training for all new employees and periodic refresher training for all employees. The Department developed a new employee orientation program that included security awareness training for new Tallahassee and non-Tallahassee employees. The Department accomplished this training using Cisco's WebEx Web Conferencing solution. However, our audit disclosed that five of the eight non-Tallahassee employees previously identified in our report No. 2010-021 as lacking security awareness training still had not received the new employee orientation training, including security awareness training. In response to audit inquiry, Department staff indicated that notification would be provided to the employees' supervisors to prompt them once more to complete the new employee orientation training class.

In addition, as similarly noted in our report No. 2010-021, the Department had not, as of June 30, 2010, fully implemented an ongoing security awareness training program to provide periodic refresher training for all employees. In response to audit inquiry, Department staff indicated that the full implementation of the online security awareness tool, webSTART, was delayed as a result of final customization requirements and a legal review.

The Department's AP&P 4-03 Information Technology Security Policy required that training requirements for systems administrators be identified and documented. AP&P 4-03 further required that the training requirements should cover areas such as network security, access controls, backup policies, and employee security obligations. However, the Department, as of June 30, 2010, had not identified or documented these training requirements for systems administrators. In response to audit inquiry, Department staff indicated that time constraints and other priorities prevented the development of training requirements for systems administrators and would be developed in the future. The lack of security awareness training for new employees, periodic refresher training for all existing employees, and training requirements for systems administrators increases the risk that employees may inadvertently compromise security.

Recommendation: The Department should provide initial security awareness training for new employees and periodic refresher training for all employees. Additionally, the Department should develop training requirements for systems administrators.

Finding No. 5: 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 that needed improvement in the areas of logical access, network boundary protection, movement of programs into production, and data transmission. 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 logical access, network boundary protection, movement of programs into production, 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 logical access, network boundary protection, movement of programs into production, and data transmission to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Finding No. 6: Network Backup Processes

There are a number of steps that an agency can take to prevent or minimize the damage to automated operations that may occur from unexpected events. One example is routinely backing up data files and programs and securely storing them at an off-site storage location. Such actions maintain the agency's ability to restore data files, which otherwise may be impossible to recreate, if lost.

The Department's network was backed up to disk and copied to tapes on a weekly basis. Once copied to tapes, the tapes were taken to the Department's off-site storage location where the tapes remained for one week. During our audit, we conducted a test to determine if the network backups were available for restoration from the off-site storage location. At the time of our testing, Department staff indicated that there were no off-site network backup tapes for the requested servers. These backups would have contained network data relating to FLAIR, OIR's Electronic Document Management System (EDMS), OIR's Financial Analysis and Monitoring Electronic Document Management System (FAME), and OFR's Regulatory Enforcement and Licensing (REAL) System. In response to audit inquiry, Department staff indicated that there were issues with the process of completing the creation of the off-site tapes before the next week's backup started; however, the process has since been corrected.

Although Department staff monitored the completion of network backup jobs for errors, follow-up was only conducted by staff if an entire server backup failed. Department staff did not follow up on individual files that failed to complete the backup process. Therefore, the Department could not be assured that all network files were backed up successfully and available to be recovered in the event of a data loss. In response to audit inquiry, Department staff indicated that the backup practice did not include a review of reports showing the results of the network backup jobs. Under these conditions, the risk is increased that, should an event occur causing a loss of production data and on-site backups, the Department's ability to timely and completely restore the lost information could be jeopardized.

Recommendation: The Department should review the frequency with which it rotates network tapes to the off-site storage location and implement a practice to review network backup reports.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2010-021.

OBJECTIVES, SCOPE, AND METHODOLOGY

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

We conducted this IT operational audit in accordance with applicable generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to the FLAIR Subsystem in achieving management's control objectives in the categories of compliance with controlling

laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; the safeguarding of IT resources; the effectiveness and efficiency of IT operations; and to determine whether the Department had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2010-021.

The scope of our audit focused on evaluating selected Department IT controls applicable to financial reporting during the period July 1, 2009, through June 30, 2010, and selected actions through August 18, 2010, including selected general IT controls over the systems development and modification, computer operations and disaster recovery, systems software and database, logical access to programs and data, and physical safeguards. The audit also included selected application IT controls and selected user controls applicable to Departmental Accounting, Central Accounting, and Payroll.

In conducting our audit, we:

- Interviewed Department personnel.
- Observed and tested the effectiveness of selected input, processing, and output controls for the General Ledger Subsystem, Contracts and Grants Subsystem, Statewide Financial Statement (SWFS) Subsystem, Voucher Audit Subsystem, Journal Transfer Audit Subsystem, 1099 Processing Subsystem, Salary Calculate Subsystem, Cancellation and Adjustments Subsystems, and different payroll input methods outside of People First (On-Demand Payroll and On-Line Data Entry).
- Observed and tested the effectiveness of selected controls over the authorization of EFT payments.
- Observed and tested the effectiveness of selected controls over the authorization, documentation, testing, approval, and implementation of application program modifications.
- Evaluated Department policies and procedures that provide for management and implementation of systems software patches including testing, maintenance, and problem resolution.
- Evaluated the adequacy of the Department's backup procedures for selected Department, OIR, and OFR programs and data.
- Evaluated the appropriateness of the Department's firewall administration procedures.
- Obtained an understanding of the Department's efforts regarding vulnerability testing.
- Evaluated the appropriateness of the Department's Business Continuity and IT Disaster Recovery Plans.
- Evaluated the Department's controls over data transmissions.
- Obtained an understanding of logical access paths to FLAIR and documented and tested whether logical access controls ensured that access to the application, software, and data was appropriately restricted.
- Evaluated Department policies and procedures that provide for access control to DAC, CAC, Payroll Component, network, RACF, and Natural Security, including the Department's security awareness program.
- Observed and tested the effectiveness of selected access controls for DAC, CAC, Payroll Component, network, RACF, and Natural Security.
- Evaluated the adequacy of physical security controls to the Department's IT resources and buildings.
- 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 29, 2010, the Chief Financial Officer provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

ALEX SINK

October 29, 2010

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 responses are 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 (FLAIR) Subsystem, for the period July 1, 2009, through June 30, 2010, and selected Department actions through August 18, 2010.

If you have any questions or would like to discuss the matter further, please contact Alan Sands, Audit Director, at (850) 413-4962.

Sincerely,

Alex Sink

Enclosure

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

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Financial Services

Response to Preliminary and Tentative Audit Findings
Florida Accounting Information Resource (FLAIR) Subsystem
Information Technology Operational Audit
For the Period July 1, 2009, through June 30, 2010, and
Selected Department Actions through August 18, 2010

Finding No. 1: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to only what is needed in the performance of assigned job responsibilities. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

Our audit disclosed that some DIS users had inappropriate access privileges to FLAIR production program code, job control language (JCL), and database files. These conditions increase the risk of unauthorized disclosure, modification, or destruction of Department data. Specifically:

- Five users had inappropriate update access privileges to the FLAIR Natural production code. The users included a systems programmer within the Bureau of Operations and Customer Services, Mainframe Systems Section, and four database administrators (DBAs) within the Office of Enterprise Applications and Infrastructure, Data Management Section. In response to audit inquiry, Department staff indicated that the systems programmer and DBAs often assist the programmers in researching production problems but did not need to have the ability to update the programs. Therefore, on June 25, 2010, Department staff modified the inappropriate update access privileges for the five users to read-only access privileges.
- Forty-five user accounts belonging to 17 users within DIS had inappropriate update access privileges to production JCL. The user accounts belonged to users in the Mainframe Systems and Operations Sections within the Bureau of Operations and Customer Services. In response to audit inquiry, Department staff removed the inappropriate update access privileges to the production JCL for the users in the Bureau of Operations and Customer Services, Mainframe Systems Section on May 20, 2010, and for the users in the Bureau of Operations and Customer Services, Operations Section on June 23, 2010.
- Twenty-four user accounts belonging to 16 users had inappropriate update access privileges to production database files that contained both production program code and data. The user accounts belonged to the PRODCNT group and included staff in the Mainframe Systems and Operations Sections within the Bureau of Operations and Customer Services. In response to audit inquiry, Department staff indicated that these access privileges had been required to perform backup and restore procedures; however, in recent years the process was changed and the access privileges were no longer required to perform these procedures. Accordingly, Department staff removed the update access privileges for the PRODCNT group on August 2, 2010.

Additionally, through our review of users with access privileges to FLAIR production program code, our audit disclosed that seven application programmers were defined as Natural administrators in Natural Security within the production databases. Natural administrators may use libraries directly and create

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

and modify security profiles. The combination of programming and security administration capabilities was contrary to an appropriate separation of duties and increased the risk that Department data and IT resources could be subject to improper disclosure, modification, or destruction. In response to audit inquiry, Department staff indicated that the programmers' Natural administrator access privileges were removed on August 12, 2010.

Recommendation: The Department should continue its efforts to limit access privileges to only what is needed in the performance of employee job functions.

Response: The Department concurs. The exceptions noted have been corrected. Immediately upon notification of this condition, Department staff modified the inappropriate update access privileges to read-only. In the future, our procedures will assure that only authorized employees will receive update access.

Finding No. 2: Timely Disabling and Removing of Access Privileges

Effective management of system access privileges includes provisions to timely disable or remove employee and contractor access privileges when employment or contractual terminations and reassignments occur. The access privileges that should be timely disabled or removed include both logical and physical access privileges to information and facilities. Prompt action is necessary to ensure that a former employee's or contractor's access privileges are not misused by the former or reassigned employee, contractor, or others.

We reviewed logical access privileges for DAC, HAC, CAC, the Payroll Component, the network, Resource Access Control Facility (RACF), and Natural Security for 379 Department, Office of Insurance Regulation (OIR), and Office of Financial Regulation (OFR) employees and contractors, who terminated employment or contractual services during the period July 1, 2009, through March 31, 2010. Our review disclosed instances where, as similarly reported in our report No. 2010-021, the access privileges of some former employees had not been timely disabled. For our review purposes, we considered the disabling of access privileges to have been timely if it occurred within the next business day after termination. Specifically:

- One former A&A employee whose DAC and HAC access privileges were still active at the time of our testing. In response to audit inquiry, Department staff disabled the former employee's access privileges on June 7, 2010, 158 days after termination.
- One former DIS employee whose DAC access privileges remained active for a period of 2 days after termination.
- One former OFR employee whose Payroll Component access privileges remained active for 7 days after termination.
- Two former employees whose network access privileges were still active at the time of our testing on May 14, 2010. One of the former employees terminated employment from the Division of State Fire Marshall and the other from OFR. In response to audit inquiry, Department staff indicated that the network access privileges of the former Division of State Fire Marshall employee were active on May 14, 2010, because of a request to have the network

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

access privileges restored. However, the restored network access privileges were not subsequently disabled. In response to audit inquiry, Department staff disabled the network access privileges but were unable to provide us the date the access privileges were disabled. Additionally, Department staff indicated that a defined process did not exist for restoring network access privileges. Although Department staff had documentation indicating that the network access privileges of the former OFR employee had been disabled on March 19, 2010, staff could not provide an explanation as to why the network access privileges were subsequently active on May 14, 2010. In response to audit inquiry, Department staff again disabled the former employee's network access privileges on June 11, 2010, 86 days after termination.

- Three former employees, two from A&A and one from the Office of the Deputy Chief Financial Officer, whose RACF access privileges remained active for periods ranging from 112 to 174 days after termination. In response to audit inquiry, Department staff disabled (revoked) the RACF access privileges of the three former employees. The accounts of the three employees had a password expiration of 30 days at which point the system would automatically disable the account upon the next logon attempt. All three accounts were in a password expired status at the time of our test, indicating that, at the next logon attempt, the account would be disabled. Therefore, the accounts were at the highest risk of compromise for, at the most, 30 days.
- One former DIS employee whose Natural Security access privileges were still active. In response to our audit inquiry, Department staff indicated that the employee's access privileges were disabled on June 23, 2010, 279 days after termination.

Additionally, from a sample of 30 of the 379 Department, OIR, and OFR employees and contractors who terminated employment or contractual services during the period July 1, 2009, through March 31, 2010, we noted 2 former employees, one from OFR and one from the Division of Insurance Fraud, whose network access privileges remained active for periods of 6 and 8 days, respectively, after termination.

Through additional audit procedures, we noted that one former A&A employee who had terminated from the Department on July 14, 2006, continued to have Natural Security access privileges to one of the informational reporting databases used to retrieve accounting data for report purposes. In response to audit inquiry, Department staff indicated that the former employee's access privileges were disabled on June 23, 2010, 1,439 days after termination. Additionally, another former A&A employee who terminated from the Department on April 16, 2010, continued to have RACF access privileges. In response to audit inquiry, Department staff disabled the account on May 21, 2010, 35 days after termination.

Our review of physical access privileges of the 379 Department, OIR, and OFR employees and contractors who terminated employment or contractual services during the period July 1, 2009, through March 31, 2010, disclosed that two employees who were reassigned to other positions within the Department retained physical access to areas within Department facilities that were no longer required. Specifically:

- One DIS employee whose physical access privileges to the State Chief Financial Officer's Data Center and Fletcher Building were not removed upon the employee's reassignment to a position in another Division that did not require physical access to these facilities. In response to audit inquiry, Department staff indicated that the access privileges to the State Chief Financial Officer's Data Center were subsequently removed on May 4, 2010, 61 days after the date of the

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

employee's reassignment. Department staff later indicated that, effective July 1, 2010, the employee was reassigned to a position that required access to the Fletcher Building. Nevertheless, the employee did not require access to the Fletcher Building between March 4, 2010, and June 30, 2010.

- One Office of Strategic Planning employee whose physical access privileges to the Fletcher Building were not removed upon the employee's reassignment to a position in another Division that did not require access to the Fletcher Building. In response to audit inquiry, Department staff indicated that access privileges to the Fletcher Building were subsequently removed on July 29, 2010, 303 days after the date of reassignment.

Without timely deletion of former or reassigned employee access privileges, the risk is increased that the access privileges could be misused by the former or reassigned employee or others.

Department management indicated they were in the process of approving changes to its Administrative Policy and Procedure (AP&P) 4-05 Application Access Control, which specifically addressed timely removal of access privileges of former employees. Additionally, the Department implemented a Remedy Help Desk process to track and notify all Division access control administrators of employee terminations. Furthermore, Department management indicated that they had designed a long-term solution and developed an implementation plan for an Information Technology Infrastructure Library (ITIL)-based configuration management database to maintain a record of all access privileges. ITIL is a widely adopted approach for IT service management best practices.

Recommendation: The Department should continue to enhance its practices to ensure that the access privileges of all former or reassigned employees are disabled or removed in a timely manner. Additionally, the Department should continue with its plan to implement an ITIL-based configuration management database to maintain a current record of all access privileges.

Response: The Department concurs. The exceptions have been corrected. The Department continues to enhance its procedures to ensure that the access privileges of all former employees are removed in a timely manner. To strengthen this process, the Department has updated its current access control policy (AP&P 4-05).

We have instituted a process change that includes notification by HR to the Facilities Section whenever there is an internal transfer to ensure that changes are made to physical access levels as appropriate.

Finding No. 3: Comprehensive Configuration Repository

Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of a comprehensive configuration repository. A 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.

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

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

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. The Department had several separate systems (the BMC Remedy Asset Configuration Management Module, Microsoft SharePoint, Microsoft's System Center Configuration Manager, and Big Brother) that contained some of this information, but the available information did not include every component of the Department's infrastructure and applications.

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

The Department recently purchased an Auto Discovery and Dependency Mapping tool that can be used to populate a configuration management database that would serve as a repository. In response to audit inquiry, Department staff indicated that they planned to prepare a Statement of Work and Request For Quote for IT Consulting Services to assist with the implementation of the tool.

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

Response: The Department concurs. The Department has prepared a Statement of Work and Request for Quote (RFQ) for IT Consulting Services to assist with the implementation of an ITIL-based help desk and service management application with a supporting configuration management database (CMDB). Currently, the release of the RFQ and determination of an implementation timeframe is on hold due to budget constraints.

Finding No. 4: Security Awareness Training

Effective security awareness programs include initial training for all new employees and periodic refresher training for all employees. The Department developed a new employee orientation program that included security awareness training for new Tallahassee and non-Tallahassee employees. The Department accomplished this training using Cisco's WebEx Web Conferencing solution. However, our audit disclosed that five of the eight non-Tallahassee employees previously identified in our report No. 2010-021 as lacking security awareness training still had not received the new employee orientation training, including security awareness training. In response to audit inquiry, Department staff indicated that notification would be provided to the employees' supervisors to prompt them once more to complete the new employee orientation training class.

In addition, as similarly noted in our report No. 2010-021, the Department had not, as of June 30, 2010, fully implemented an ongoing security awareness training program to provide periodic refresher training for all employees. In response to audit inquiry, Department staff indicated that the full implementation of the online security awareness tool, webSTART, was delayed as a result of final customization requirements and a legal review.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

The Department's AP&P 4-03 Information Technology Security Policy required that training requirements for systems administrators be identified and documented. AP&P 4-03 further required that the training requirements should cover areas such as network security, access controls, backup policies, and employee security obligations. However, the Department, as of June 30, 2010, had not identified or documented these training requirements for systems administrators. In response to audit inquiry, Department staff indicated that time constraints and other priorities prevented the development of training requirements for systems administrators and would be developed in the future. The lack of security awareness training for new employees, periodic refresher training for all existing employees, and training requirements for systems administrators increases the risk that employees may inadvertently compromise security.

Recommendation: The Department should provide initial security awareness training for new employees and periodic refresher training for all employees. Additionally, the Department should develop training requirements for systems administrators.

Response: The Department concurs. The exceptions have been corrected. As of October 15, all current employees noted in the audit exception have received individualized security awareness training. DIS plans to require new employees to participate and pass the web based course and acknowledge the Department's information security policies before access to the DFS Network will be authorized and granted. The Department also plans to deliver periodic refresher training to all employees and has piloted a web based security awareness course to achieve this objective.

Additionally, the Department will define, deliver and document receipt of security awareness training for systems administrators.

Finding No. 5: 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 that needed improvement in the areas of logical access, network boundary protection, movement of programs into production, and data transmission. 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 logical access, network boundary protection, movement of programs into production, 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 logical access, network boundary protection, movement of programs into production, and data transmission to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Response: The Department concurs with the recommendation and will implement appropriate security controls.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 6: Network Backup Processes

There are a number of steps that an agency can take to prevent or minimize the damage to automated operations that may occur from unexpected events. One example is routinely backing up data files and programs and securely storing them at an off-site storage location. Such actions maintain the agency's ability to restore data files, which otherwise may be impossible to recreate, if lost.

The Department's network was backed up to disk and copied to tapes on a weekly basis. Once copied to tapes, the tapes were taken to the Department's off-site storage location where the tapes remained for one week. During our audit, we conducted a test to determine if the network backups were available for restoration from the off-site storage location. At the time of our testing, Department staff indicated that there were no off-site network backup tapes for the requested servers. These backups would have contained network data relating to FLAIR, OIR's Electronic Document Management System (EDMS), OIR's Financial Analysis and Monitoring Electronic Document Management System (FAME), and OFR's Regulatory Enforcement and Licensing (REAL) System. In response to audit inquiry, Department staff indicated that there were issues with the process of completing the creation of the off-site tapes before the next week's backup started; however, the process has since been corrected.

Although Department staff monitored the completion of network backup jobs for errors, follow-up was only conducted by staff if an entire server backup failed. Department staff did not follow up on individual files that failed to complete the backup process. Therefore, the Department could not be assured that all network files were backed up successfully and available to be recovered in the event of a data loss. In response to audit inquiry, Department staff indicated that the backup practice did not include a review of reports showing the results of the network backup jobs. Under these conditions, the risk is increased that, should an event occur causing a loss of production data and on-site backups, the Department's ability to timely and completely restore the lost information could be jeopardized.

Recommendation: The Department should review the frequency with which it rotates network tapes to the off-site storage location and implement a practice to review network backup reports.

Response: The Department concurs. Confidential Backup procedure DIS-111 is currently being followed. Process improvements have been implemented to allow backup tapes to be created and taken offsite on a weekly basis. Additionally, upgraded equipment has been acquired and installed, reducing the time it takes to create backup tapes. Backup jobs are checked to verify that they complete successfully. Weekly backup reports are delivered to the Active Directory section supervisor for review to verify that all data has been backed up successfully and follow up on any exceptions.