CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

May 27, 2011

The Honorable Jeff Atwater
Chief Financial Officer
The Capitol, PL-11
Tallahassee, Florida 32399-0301

Dear CFO Atwater:

Pursuant to Section 20.055 (5) (h), Florida Statutes, the enclosed response provides a six-month follow-up on the status of corrective actions taken by the Department regarding the findings and recommendations included in the Auditor General's Report No. 2011-030, 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 me.

Sincerely,

Ned Luczynski



NL:Sc

Attachment

cc: Jonathan E. Ingram, Audit Manager, Office of the Auditor General
Kathy DuBose, Staff Director, Joint Legislative Auditing Committee

FLORIDA DEPARTMENT OF FINANCIAL SERVICES
Ned Luczynski • Inspector General
Division • Office of Inspector General
200 East Gaines Street • Tallahassee, Florida 32399-0312 • Tel. 850-413-3112 • Fax 850-413-4973
Email • Ned.Luczynski@MyFloridaCFO.com

# Florida Department of Financial Services
## Information Technology Operational Audit No. 2011-030
## Florida Accounting Information Resource (FLAIR) Subsystem
## Six-Month Audit Response
## 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

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.

**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.

**Six-Month Status:** The Department is very selective when adding staff to a system security group and removes inappropriate access privileges as they are identified. In addition, the Department has initiated an on-going effort to review security groups and the profile of group members to determine appropriate access.

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

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.

**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.

**Six-Month Status:** The Department continues to enhance its procedures to ensure that the access privileges of all former employees are removed in a timely manner. In coming months, the Department will perform an annual access control inspection of secure applications in accordance with AP&P 4-05.

## Finding No. 3: Comprehensive Configuration Repository

The Department did not maintain a comprehensive configuration repository of its IT infrastructure and applications.

**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.

**Six-Month Status:** The Department decided against letting the Statement of Work and RFQ and is instead advancing the knowledge and ability of in-house staff. Our Remedy administrator has participated in several training sessions (including one regarding the configuration management database) and has access to a test environment for configuring the latest version of Remedy. Our target timeframe for going live with the Remedy upgrade is the first quarter of CY 2012. The CMDB functionality may not be in place by that timeframe and the Department is exploring other tools and methods for configuration management.

## Finding No. 4: Security Awareness Training

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.

**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.

**Six-Month Status:** The Department expects to implement the web-based Security Awareness Training by June 30, 2011. New employees will be required to complete training within their first 30 days. Existing employees will be required to complete annual refresher courses.

## Finding No. 5: Other Security Controls

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.

**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.

**Six-Month Status:** The Department has addressed some of the issues and will continue to implement appropriate security controls.

**Finding No. 6: Network Backup Processes**

Network backup processes needed improvement with regard to the rotation of backup tapes to an off-site storage location and review of the backup reports.

**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.

**Six-Month Status:** The Department has addressed the issues for the tape rotation and backup reports. Backup tapes are taken to the Northwest Regional Data Center (NWRDC) on a weekly basis and the Active Directory supervisor is still actively monitoring the reports. Backup reports are also sent to different DIS groups for review.

## Alan Sands

**From:** Paul Whitfield
**Sent:** Wednesday, May 25, 2011 11:36 AM
**To:** Alan Sands
**Subject:** RE: FLAIR IT Audit 2011-030

Approved.

Thanks.

**From:** Alan Sands
**Sent:** Wednesday, May 25, 2011 11:24 AM
**To:** Paul Whitfield
**Subject:** FW: FLAIR IT Audit 2011-030

Mr. Whitfield,

Could you also approve the above response. Christina and Terry have already given their ok. Thanks, Alan.

**From:** Alan Sands
**Sent:** Thursday, May 19, 2011 3:26 PM
**To:** Paul Whitfield; Terry Kester; Christina Smith
**Cc:** Ned Luczynski
**Subject:** FW: FLAIR IT Audit 2011-030

Please send back to me no later than Tuesday, May 24. Thanks again. Alan

**From:** Alan Sands
**Sent:** Thursday, May 19, 2011 3:15 PM
**To:** Paul Whitfield; Terry Kester; Christina Smith
**Cc:** Ned Luczynski
**Subject:** FW: FLAIR IT Audit 2011-030

**From:** Sheryl Cosson
**Sent:** Thursday, May 19, 2011 2:57 PM
**To:** Alan Sands
**Subject:** FLAIR IT Audit 2011-030

Please see the attached proposed 6-month follow up response to the Information Technology/FLAIR audit conducted by the Auditor General's Office (report no. 2011-030). Please review the response and indicate your approval of the document before we send it to the CFO for signature. Thanks for your assistance.