REPRESENTING
ALEX SINK
CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

March 25, 2010

The Honorable Alex Sink
Chief Financial Officer
The Capitol, PL-11
Tallahassee, Florida 32399-0301

Dear CFO Sink:

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. 2010-021, Florida Accounting Information Resource (FLAIR) Subsystem Information Technology Operational Audit.

If you have any questions or would like to discuss the matter further, please contact me at (850) 413-4960.

Sincerely,

Robert E. Clift

REC:sc

Enclosure

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

RECEIVED
MAR 29 2010

FLORIDA DEPARTMENT OF FINANCIAL SERVICES
Robert E. Clift • Inspector General
200 E. Gaines St. • Tallahassee, FL 32399-0312 • Tel. 850-413-3112 • Fax 850-413-4973
Email • Bob.Clift@myfloridacfo.com
Affirmative Action • Equal Opportunity Employer

Florida Department of Financial Services
Information Technology Operational Audit
Florida Accounting Information Resource (FLAIR) Subsystem
Six-Month Audit Response
For the Period July 1, 2008, through June 30, 2009

Finding No. 1: Management of Access Privileges – Timely Removal of Former Employee Access

We noted instances where, as similarly noted in our report No. 2009-053, the Department did not remove the access privileges of former employees in a timely manner.

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

Response: The Department concurs. The Department will continue to enhance its procedures to ensure that the access privileges of all former employees are removed in a timely manner. The Department will update its current access control policy (AP&P 4-05) by December 31, 2009, to strengthen this process. The Department will also pursue a short term solution by creating a database based on employee's role to identify all access privileges so that once the employee's employment status changes, the appropriate access rights can be disabled quickly. A long term strategy of the Department is to adapt ITIL based CMDB to maintain a record of all the access rights.

Six-Month Status: The Department is in the approval process for revisions of the access control policy (AP&P 4-05) to specifically address timely removal of access privileges of former employees. The Department implemented an immediate solution using the Remedy Help Desk process to track and notify all Division Access Control Administrators of departed employees. The Department has designed a long-term solution and developed an implementation plan for an ITIL-based CMDB to maintain a record of all access rights.

Finding No. 2: Management of Access Privileges - Other

The Department was unable to identify the Payroll Component user associated with a specific user identification (ID), and a Department employee who had transferred to another Department position inappropriately retained job control language access privileges.

Recommendation: The Department should implement appropriate controls to properly identify users and ensure that access privileges granted are appropriate and commensurate with employee job functions.

Response: The Department concurs. The Department has implemented an Application Access Control Workgroup to review Department procedures and make recommendations for improvement to the access control process.

Six-Month Status: The Department has mitigated this risk by using the Remedy Help Desk process to track and notify all Division Access Control Administrators of departed employees. Regular analysis of employee departures compared to existing Active Directory is performed using comparison reports.

The Department is in the approval process for revisions of the access control policy (AP&P 4-05) to specifically address timely removal of access privileges of former employees.

Finding No. 3: Security Awareness Training

The Department did not provide initial security awareness training for some employees or ongoing security awareness training for all employees.

Recommendation: The Department should continue with its plan to institute online training for both initial and ongoing security awareness training.

Response: The Department concurs. The Department plans to develop an on-line security awareness training tool and train all employees by June 30, 2010. This tool will be used for annual refresher training.

Six-Month Status: The Department now includes information security awareness training as a required part of new employee orientation. The Department has surveyed other state agencies' practices and identified cost effective online training options for both initial and ongoing security awareness training. The Department has developed a statement of work to acquire online security awareness training and has initiated the procurement process for same.

Finding No. 4: Other Security Controls

In addition to the matters discussed in Finding Nos. 1, 2, and 3, certain Department security and application controls needed improvement. Our prior reports on the Department have included some of the same issues.

Recommendation: The Department should implement the appropriate security controls 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 is in the process of designing short term mitigations and assessing long-term solutions for an ITIL based CMDB to strengthen overall security controls.

Finding No. 5: Electronic Funds Transfer (EFT) Authorization Process

The Department's electronic funds transfer (EFT) authorization process needed improvement.

Recommendation: The Department should update the Direct Deposit Operating Procedures, as appropriate, and take steps to ensure that staff consistently follow the approved Procedures.

Response: The Department concurs. The Direct Deposit Operating Procedures will be updated by December 31, 2009, and periodically reviewed, and steps will be taken to ensure that applicable staff members follow the approved Procedures.

Six-Month Status: The Direct Deposit Operating Procedures were updated as appropriate and implemented by December 31, 2009.