REPRESENTING
ALEX SINK
CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

June 1, 2009

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

Dear CFO Sink:

Pursuant to Section 11.45(4) (d), 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. 2009-053, 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

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

JLAC
Rec 6/2/2009

Florida Department of Financial Services
Six-Month Audit Response
Information Technology Operational Audit
Florida Accounting Information Resource (FLAIR) Subsystem
For the Period July 1, 2007, through June 30, 2008, and
Selected Actions Through September 17, 2008

Finding No. 1: We noted instances where, as similarly noted in audit report No. 2008-026, the Department did not remove the access privileges of former and transferred employees in a timely manner.

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

Response: The Department concurs.

Division of Accounting and Auditing: The Division has established an access control team to improve the procedures and documentation for the review of access. The Division's access control team will complete the revision of access control procedures for the 19 applications owned by the Division by March 31, 2009. The revised procedures will be implemented April 1, 2009, for the Division's quarterly review for April – June 2009.

Six-Month Status: The Division's access control team has completed the access control procedures for 17 of the 19 applications owned by the Division. The procedures for the remaining 2 applications will be completed by June 30, 2009. Although the revised procedures are not completed, the Division has conducted the third quarter reviews according to the access control rules that will be in the revised procedure.

Division of Administration: The Division has designated an Accountant III position to serve as the primary access control administrator responsible for removal and update of access privileges and a Finance and Accounting Director II position to serve as the backup. Additional controls have been put in place whereby termination notices and notices of position changes received from the Bureau of Human Resource Management are forwarded to both the primary access control administrator and the backup via e-mail. Notices of terminations/changes set to occur in the future are placed on the Outlook calendars for both the primary access control administrator and the backup. The Finance and Accounting Director II confirms that all DAC access privileges for future terminations/changes are timely executed. Access privileges for immediate terminations are removed as soon as the notice is received. These actions have been completed.

Six-Month Status: The Division has made internal personnel changes to ensure the Accountant III who is the primary access control administrator has the necessary skills to perform these duties. This individual has been trained on how to properly remove/update access privileges. In addition, the following steps have been implemented to ensure access privileges are removed in a timely manner:

- Increased number of staff who receive email notifications of terminated or transferred employees from two to three;
- Tracking of future dated removal of access privileges via calendar in Microsoft Outlook;
- Updated Internal Policy and Procedures and detailed desk procedures; and
- Discussions with staff every six months regarding importance of timely removal of access privileges.

Division of Information Systems (DIS): The Division will continue to improve the timeliness of deleting access privileges when employment is terminated. DIS is reviewing its current policies and procedures associated with application access and has reevaluated centralized access control in favor of a decentralized approach which provides better separation of duties and better internal control. DIS will report on the status of these improvements in conjunction with the six month audit follow-up.

During the audit period, when the Help Desk staff created tickets to terminate accesses, standard tasks were completed manually. Effective July 27, 2008, the Help Desk implemented program changes to automatically generate the standard tasks. Changing from manually creating the standard tasks to automatically generating the tasks has reduced the error rate (i.e., accesses not being terminated) by ensuring all the required tasks are created for access removal. In addition, follow-up e-mail reminders are system created and sent to the security administrators and Help Desk DP Coordinators the day following separation date to validate access removal. These actions have been completed.

Six Month Status: The Internal Controls project is addressing the department's application access control process and this project is scheduled to be completed August 31, 2009.

Finding No. 2: The primary Departmental Accounting Component (DAC) access control custodian shared a user identification (ID) with a backup access control custodian.

Recommendation: The Department should continue to assign individual IDs to all system users.

Response: The Department concurs.

Division of Administration: The Division has set up separate user identifications for the DAC primary access control administrator and backup. This action has been completed.

Six-Month Status: This action has been completed.

Finding No. 3: The Department lacked procedures for the Statewide Financial Statements (SWFS) Subsystem security administration process and for the reconciliation of data loaded from the Purchasing Card Module and DAC into the Information Warehouse.

Recommendation: The Department should establish written procedures to govern the SWFS Subsystem security administration process and the reconciliation of data loaded from the Purchasing Card Module and DAC into the Information Warehouse.

Response: The Department concurs.

Division of Accounting and Auditing: The Division will work with DIS to establish written procedures to govern the security administration process for the SWFS Subsystem by March 31, 2009.

Six-Month Status: The Division has established written procedures for access control related to the Statewide Financial Statements (SWFS) Subsystem. The procedures explain the security administration process the access control custodian must go through when granting access to new employees and removing access from terminated employees. Access to the SWFS Subsystem is reviewed quarterly, and all changes are made promptly.

Division of Information Systems: Procedures to reconcile the data load from the Purchasing Card Module and DAC were written and implemented effective September 30, 2008.

Six-Month Status: These procedures were implemented effective September 30, 2008.

Finding No. 4: In addition to the matters discussed in Finding Nos. 1, 2, 3, and 7, certain Department security and application controls needed improvement. Some of the issues were also included in audit report No. 2008-026.

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 continuing its efforts to implement appropriate security controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Finding No. 5: As similarly noted in audit report No. 2008-026, we noted a programming error in the salary refund calculation of net pay.

Recommendation: The Department should continue with its efforts to implement the appropriate programming changes to prevent future occurrences of salary refund calculation errors.

Response: The Department concurs.

Division of Accounting and Auditing: Programming changes were implemented last year to correct this issue; however, another calculation discrepancy was discovered this year. This new discrepancy was fixed in August 2008. The Division of Accounting and Auditing will continue efforts to implement all necessary programming changes, if needed, to prevent future

occurrences of salary refund calculation discrepancies. Two reports have been identified that can assist with identifying any salary refund calculation errors in a timely manner. One of the reports was implemented in October 2008 and the other one will be implemented by December 31, 2008.

Six-Month Status: The Division implemented the second report for daily verification on February 11, 2009. There have been no occurrences of the out-of-balance net situation since the implementation of the verification reports. The Division will continue to monitor for out-of-balance situations and address any discrepancies that may arise.

Division of Information Systems: On August 11, 2008, DIS implemented the appropriate programming changes to prevent errors in salary refund calculations.

Six-Month Status: The appropriate programming changes were implemented on August 11, 2008.

Finding No. 6: Department staff did not follow established job scheduling procedures during a nightly production run, resulting in discrepancies in the balances on the general ledger master file. A similar finding was included in audit report No. 2008-026.

Recommendation: The Department should take the necessary steps to reinforce to staff the importance of following established procedures.

Response: The Department concurs.

Division of Information Systems: Appropriate steps have been taken to improve communication and workflow. In addition, staffing changes at the supervisory level and disciplinary actions have occurred. These actions have been completed.

Six-Month Status: The appropriate steps were taken to improve communication and workflow.

Finding No. 7: As also noted in audit report No. 2008-026, contrary to the Department's Enterprise Security Policy, the Department had not established an approved baseline firewall configuration.

Recommendation: The Department should ensure that the baseline firewall configuration continues to be appropriately documented.

Response: The Department concurs.

Division of Information Systems: DIS has implemented an application to record, track, and route firewall configuration changes. Approval is required prior to a change implementation. A full description of the change is contained in the approval request. A tool has been implemented to automatically record all firewall and router code modifications. This tool is properly backed-up to maintain and preserve the record. This action has been completed.

Six-Month Status: DIS has taken the following steps:

a) A procedure titled "Backing Up Cisco Infrastructure Devices" has been put in place. The procedure covers changes to the firewall configuration.
b) A baseline of the firewall configuration is certified by the assistant director in charge of infrastructure on a yearly basis and preserves the record for refresh and inspection.

Finding No. 8: The Department did not consistently document the release of output data tapes to other entities.

Recommendation: The Department should reinforce to staff the importance of following established output data tape handling procedures.

Response: The Department concurs.

Division of Information Systems: Appropriate steps have been taken to reinforce that staff ensures sign out procedures are followed when all tapes are released. This action has been completed.

Six-Month Status: Effective April 30, 2008, this action was completed.

Finding No. 9: On July 16, 2008, a fraud occurred that resulted in $5,700,352 in vendor electronic funds transfer (EFT) payments being inappropriately diverted to the bank account of a third party. The Department, subsequent to the fraud, revised and expanded its EFT procedures; however, the procedures needed further improvement.

Recommendation: The Department should implement the appropriate internal controls to ensure the integrity of Department data and the processing of EFT payments.

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

Six-Month Status: The Division revised its Direct Deposit Operating Procedures to include additional internal controls for the Vendor EFT Section in October 2008. The Division has also requested system enhancements for tracking all changes made to an EFT record by a user and for creating a dual verification screen for the approval and posting of changes to an EFT record. The Department has developed an Internal Controls Policy Document, which will be utilized to help ensure risks of fraud are mitigated to within acceptable levels for each process we perform. This high-level policy document specifies that the designated process owner identify the inherent risk to achievement of each process objective, and that procedures be developed to mitigate each identified risk to acceptable levels. The Department policy for funds transfers is current under development.