REPRESENTING
ALEX SINK
CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

December 15, 2008

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. 2009-004, Selected Division of Treasury Systems, Information Technology Audit, for the period January 2008 through March 2008.

The Divisions of Treasury and Information Systems have reported all planned corrective actions, as previously described in the DFS response to the Auditor General's Preliminary and Tentative Audit Report, have been completed.

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: Terry Shoffstall, Director, Joint Legislative Auditing Committee
Jonathan Ingram, Audit Manager, Office of the Auditor General

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

Florida Department of Financial Services
Audit Response
Selected Division of Treasury Systems
Information Technology Audit
For the Period January 2008 through March 2008

Finding No. 1: Program change controls for the Treasury systems needed improvement.

Recommendation: The Department should follow and adequately document compliance with established program change control procedures to ensure that all program changes are properly authorized, designed, tested, and implemented in a manner consistent with management's intent. Procedures should be implemented to ensure that all program changes within the production environment can be tracked to authorized change requests. Additionally, the Department should separate work responsibilities such that one employee does not control all critical stages of the program change process.

Response: The Department concurs. Effective August 1, 2008, the Division of Treasury will be incorporated into the DIS Application Service Request (ASR) system. The ASR system provides the ability to track requests for changes, document the separation of duties including the identification of the resources assigned for programming, testing, and moving changes into the production environment, and document user acceptance testing. A Request for Change (RFC) will be created within the Remedy Change Management System per DFS AP&P 4-17 Change Management and Control Policy and DIS-015 Change Management Operating Procedures, and the ASR number(s) will be listed in the RFC to provide a cross-reference to the authorized change requests.

System maintenance and deployment responsibilities will be segregated on older platforms by assigning the code development and code promotion to different Bureau of Financial Applications (BFA) staff starting August 1, 2008, and tracked using the ASR system.

All new development since August 2007 using the .NET development and SQL server platforms ensures separation of duties. Programmers do not have access to the production environment on the .Net server or the SQL database server and deployments will be implemented by staff in those sections.

AP&P No. 4-17 Change Management and Control Policy, and DIS-015 Change Management Operating Procedures will be followed for production deployments and database structure changes will follow the DIS-010 Procedures for Database Change Requests for new and old environments.

Six Month Status: **Complete**

Finding No. 2: Some excessive and inappropriate system access privileges existed. Additionally, terminated and reassigned employees' access privileges were not removed in a timely manner.

Recommendation: The Department should continue to modify or remove the system access privileges of current and former employees and others, to the extent practicable, to remove unnecessary capabilities and promote a separation of incompatible duties. Additionally, in future Treasury system development projects, the Department should ensure that all new systems include the ability to grant inquiry and reporting capabilities separate from update capabilities.

Response: The Department concurs. To control system access privileges, effective July 10, 2008, the Bureau of Financial Applications will complete modifications to all end user profiles and groups on the Treasury AS400 to remove individual user access to production code and data.

As of August 2007, new system design incorporates role based security for the system users that includes separation of inquiry, update, and reporting capabilities.

Six Month Status: Complete

Finding No. 3: Aspects of the Department's practices for managing access privileges needed improvement.

Recommendation: The Department should ensure that authorization of all access privileges associated with the Treasury systems is documented to facilitate effective security administration. In addition, periodic reviews of Treasury system access privileges should be performed to ensure that privileges remain necessary and commensurate with employees' job duties.

Response: The Department concurs. The Division of Treasury will follow the access process specified by DFS AP&P 4-05 Application Access Control. Additionally, effective July 1, 2008, a new monthly audit procedure has been implemented by the Division of Treasury to review user access privileges. Final documentation for this procedure is pending completion by August 1, 2008.

Six Month Status: Complete.

Finding No. 4: In addition to the matters discussed in Finding Nos. 2 and 3, certain Department security and application controls needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising the Department's data and IT resources.

Recommendation: The Department should implement the appropriate security and application controls to ensure the continued integrity, confidentiality, 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 Division has implemented appropriate security controls.