08-026

REPRESENTING
ALEX SINK
CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

April 11, 2008

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

Dear CFO Sink:

Pursuant to Section 20.055(5)(g), Florida Statutes, the attached 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 Information Technology Audit of the Florida Accounting Information Resource Subsystem (FLAIR). The corrective actions now taken for each of the findings substantially reflect the corrective action outlined in your October 18, 2007, response to the Auditor General.

If you have any questions or would like to discuss the matter further, please do not hesitate to contact me.

Sincerely,

Robert E. Clift

REC:sc

Attachment

cc: Jonathan Ingram, IT Audit Manager, Office of the Auditor General
Terry Shoffstall, 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

Florida Department of Financial Services
Six Month Follow-up Audit Response
Information Technology Audit
Florida Accounting Information Resource Subsystem (FLAIR)
For the Period July 1, 2006, through June 30, 2007

Finding No. 1: We noted inconsistencies among the various Department's access control policies and procedures for FLAIR. In addition, we noted instances where the Department's access control policies and procedures for FLAIR were lacking or not being followed.

Recommendation: The Department should review, and update where appropriate, its FLAIR access control policies and procedures, including, in particular, the policies and procedures governing staff access to each component of FLAIR, so that consistent written guidance is provided to staff. Once the access control policies and procedures are finalized, the Department should communicate the updated policies and procedures to staff and ensure that the established procedures are followed. Additionally, the Department should develop procedures to ensure that appropriate access reviews are conducted.

Response: The Department concurs. The Department's Enterprise Security policy (AP&P 04-03) will be reviewed and revisions will be completed, implemented, and communicated by 3-31-2008. The Divisions of Accounting & Auditing, Administration, and Information Systems procedures are currently being reviewed and will be revised accordingly. The individual divisions' responses and corrective actions are as follows:

Division of Accounting and Auditing: A thorough review of draft DIS-011 (Creating, Modifying, and Terminating User Access to IT Resources) procedure was conducted, which provided a foundation for the Division's new access control procedure. The Division's new procedure, effective 11-1-2007, will encompass all user applications, in addition to the FLAIR mainframe system, and will govern the process for administering initial access, password changes, and employee/vendor reassignments and terminations. Written application access control procedures will be maintained for each application, within each bureau, to ensure that internal control procedures are followed and reports will be generated monthly for supervisors to verify that only appropriate users have access to their applications. Supervisors will also be responsible for maintaining documentation that employee/vendor access modification and revocation requests were completed by DIS for CAC and DAC access. Additionally, monthly reports will be disseminated for supervisors to review current user access to CAC and DAC.

Division of Administration: Regarding the instances noted where the Division of Administration did not follow the procedures for Payroll access control as per BOSP's Payroll Preparation Manual, corrective measures have been taken and the corresponding Internal Policy and Procedure No. 33 (FLAIR PYRL) will be updated to reflect these measures by 10-31-2007. The measures taken were to name a back-up Payroll access control custodian, conduct quarterly audits of access capabilities to ensure accuracy and require supervisors to immediately notify the Payroll access control custodian upon termination or transfer of an employee who no longer needs access to Payroll.

Division of Information Systems: Effective 5-29-2007, DIS instituted several improvements to the process for creating, modifying, and terminating user access to IT resources. Revisions to the procedure for the process, DIS-011, are under review and are scheduled to be published by 12-31-2007. The process improvements include quarterly desk audits by a DIS Access Review Team to ensure the procedure is followed. The first audit is scheduled for January 2008. For FLAIR Natural security user administrators DIS staff has developed a program to provide a monthly user authorization report. The report will be sent to user security administrators for their review so that requests to delete user access can be processed per DIS-011 for any terminated employees who still have system accesses through Natural security. The program for the report is complete and documentation for the process is scheduled for completion by 10-31-2007.

6 Month Response: The Department published the new Administrative Policy and Procedure (AP&P) 4-05, Application Access Control on 3-31-2008. The individual divisions' responses and corrective actions are as follows:

Division of Accounting and Auditing: The Division's System Access Control policy was approved and disseminated on 11-2-2007. Application access control procedures that include the processes outlined in AP&P 4-05 are being drafted for the 9 applications owned by the Division. The Financial Administrator in the Director's office is coordinating the review and approval of access control procedures for these applications which will be completed by 5-30-2008. Responsibility for the review of user access to CAC and DAC has been assigned to the Administrative Assistant in the Director's office and the first monthly review is scheduled for completion on 4-30-2008.

Division of Administration: Procedure No. 33 (FLAIR PYRL) was revised and published on 11-1-07. Quarterly audits of access control are being conducted to ensure supervisors are properly notifying the Payroll access control custodian upon termination or transfer of an employee who no longer needs access to Payroll.

Division of Information Systems: The Division has determined that centralizing access control is a better approach than establishing a review process as stated in the original response. Application access control provisions previously included in DIS-011 were transitioned into DFS AP&P 4-05 to ensure applicability agency wide. In concert with AP&P 4-05, the Division is currently in the process of establishing an Access Control Team. The DIS Access Control Team will be tasked with processing all access control requests and will perform daily monitoring to ensure changes are made timely. DIS will be phasing in access control responsibilities for each application in the Department until all access control responsibilities have been centralized. The Division has also created a listing of all employees in the human resource system for the Department that is compared to the Department's master list of employees with system access. An error report is produced for any discrepancies between the two lists and DIS staff take immediate action to resolve the discrepancies.

Finding No. 2: We continued to note that Department staff could not provide a comprehensive and accurate listing of all terminated employees. In addition, we continued to note instances where the Department did not remove the access privileges of terminated and transferred employees in a timely manner.

Recommendation: The Department should enhance its procedures to ensure that complete records of all employee terminations are maintained. Additionally, the Department should ensure that network, RACF, and FLAIR access privileges of terminated and transferred employees are removed in a timely manner.

Response: The Department concurs. The Department's Enterprise Security policy (AP&P 04-03) will be reviewed and revisions will be completed, implemented, and communicated by 3-31-2008. The Divisions of Accounting & Auditing, Administration, and Information Systems procedures are currently being reviewed and will be revised accordingly. The individual divisions' responses and corrective actions are as follows:

Division of Accounting and Auditing: Through the implementation of our new access control policy, effective 11-1-2007, supervisors within each bureau will be responsible for maintaining written application access control procedures, as well as documenting user access modifications and revocations based upon employee reassignments and terminations. A manual listing of current and terminated employees, along with their corresponding date of hire or date of termination, will be documented by each bureau. Supervisors will be held accountable for reconciling their internal listing of current and terminated employees on a monthly basis with monthly user reports distributed to each bureau for various system applications and DAC/CAC access to rectify any discrepancies and ensure the accuracy of their records. The Division will conduct periodic reviews to make certain that these procedures are being followed.

Division of Administration: As previously reported in Audit Report No. 2007-186, the Division developed a manual process to track terminated employees to compensate for the lack of an accurate People First report of employee terminations. The tracking system was set up in a shared database where several users had access and update responsibilities. To eliminate the likelihood of human error we have restricted the access and responsibility of input to one sole senior staff member and appropriate backup.

Division of Information Systems: Effective 5-29-2007, DIS instituted several improvements to the process for creating, modifying, and terminating user access to IT resources. Revisions to the procedure for the process, DIS-011, are under review and are scheduled to be published by 12-31-2007. The process improvements include quarterly desk audits by a DIS Access Review Team to ensure the procedure is followed. The first audit is scheduled for January 2008. When the DIS Help Desk receives notification of employee terminations assignments are created immediately. Changes to ensure follow-up and confirmation that the assignments have been completed within specified timeframes have been implemented. In addition, effective 5-7-07, DIS has revised its inactivity monitoring process to produce a monthly report of accounts that have been inactive for 60 days versus its former 90 day time period. The written procedure for this process will be finalized and published as a DIS procedure by 12-31-2007.

6 Month Response: The Department published the new Administrative Policy and Procedure (AP&P) 4-05, Application Access Control on 3-31-2008. The individual divisions' responses and corrective actions are as follows:

Division of Accounting and Auditing: The Division's System Access Control policy was approved and disseminated on 11-2-2007. Application access control procedures are being drafted for the 9 applications owned by the Division. The procedures will include the monthly review to ensure that user access revocations have occurred for terminated or reassigned employees. The Financial Administrator in the Director's office is coordinating the review and approval of access control procedures for these applications which will be completed by 5-30-2008. Responsibility for the review of user access to CAC and DAC has been assigned to the Administrative Assistant in the Director's office and the first monthly review is scheduled for completion on 4-30-2008. The monthly review will include a validation that terminated or reassigned employees access has been revoked.

Division of Administration: The Division continues to use the tracking system with one senior staff member as the primary user of the system and another staff member as backup.

Division of Information Systems: The Division has determined that centralizing access control is a better approach than establishing a review process as stated in the original response. Application access control provisions previously included in DIS-011 were transitioned into DFS AP&P 4-05 to ensure applicability agency wide. In concert with AP&P 4-05, the Division is currently in the process of establishing an Access Control Team. The DIS Access Control Team will be tasked with processing all access control requests and will perform daily monitoring to ensure changes are made timely. DIS will be phasing in access control responsibilities for each application in the Department until all access control responsibilities have been centralized. The Division has also created a listing of all employees in the human resource system for the Department that is compared to the Department's master list of employees with system access. An error report is produced for any discrepancies between the two lists and DIS staff take immediate action to resolve the discrepancies.

Finding No. 3: Patches to the Department's antivirus software were not maintained at the current version. Additionally, the Department's documentation of certain software patches, including the installation and testing thereof, was lacking.

Recommendation: The Department should ensure that patch management is adequately documented and that patches are installed in a timely manner.

Response: The Department concurs. DIS has different types of anti-virus updates that may be required either as part of daily, regular operational activities or which must be applied due to patches or fixes supplied by the anti-virus software manufacturer. DIS has documented the regular updates and utilizes its change control procedures to manage any updates, patches or fixes that may be required because of major changes by the manufacturer. In order to assure a systematic, disciplined approach in which changes are requested, approved, tested, and documented prior to installation or implementation, DIS has reviewed and updated its change control procedures (DIS-015) effective 8-30-2007, and designated a Change Control Manager who has been assigned responsibility for oversight of and adherence to the change control procedures. All major anti-virus patches or updates must comply with this updated process.

6 Month Response: The DIS Change Control Manager continues to provide oversight of and adherence to the change control procedures which includes anti-virus patches or updates.

Finding No. 4: Contrary to the Department's Enterprise Security Policy, guidelines and procedures had not been developed for administering network firewalls. In addition, the Department had not established an approved baseline firewall configuration.

Recommendation: The Department should develop written guidelines and procedures for managing its firewalls. Additionally, the Department should proceed with its plans to approve a baseline configuration for its firewall.

Response: The Department concurs. A baseline firewall configuration was approved and is recorded within the firewall management tool. The internal process for firewall changes requires compliance with DIS' change control procedures (DIS-015) in order to assure a systematic, disciplined approach in which changes are requested, approved, tested, and documented. DIS has reviewed and updated its change control procedures (DIS-015) effective 8-30-2007, and designated a Change Control Manager who has been assigned responsibility for oversight of and adherence to the change control procedures. Once changes to the firewall have met the requirements of DIS' change control procedures network staff implement the required changes.

6 Month Response: The DIS Change Control Manager continues to provide oversight of and adherence to the change control procedures which includes changes to network firewalls.

Finding No. 5: We noted certain deficiencies in the Department's security control features, in addition to the matters described in Findings No. 1 through 4 above.

Recommendation: The Department should implement the appropriate security controls to ensure the continued integrity, confidentiality, and availability of FLAIR information resources.

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

6 Month Response: The Department has implemented the appropriate security controls.

Finding No. 6: Department staff did not follow established job scheduling procedures during a nightly production run, resulting in voucher processing errors.

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

Response: The Department concurs. DIS has reviewed the procedures with staff. Weekly meetings are held to review issues and communicate the issues to the supervisor for handling. The job control scheduling language has been modified so that if the voucher processing job must be rerun then a data refresh will be forced.

6 Month Response: DIS conducted weekly meetings until all issues had been resolved. A tracking sheet has been created for issues and the staff continues to meet on a monthly basis to discuss issues and the appropriate resolutions.

Finding No. 7: Department staff did not follow established procedures for change control, specifically documentation, testing, and approval procedures, when implementing a special data correction, resulting in discrepancies between data files.

Recommendation: The Department should follow its established procedures to ensure that data remains accurate during special data correction processes.

Response: The Department concurs. DIS has reviewed the procedures for change control with staff. Staff has been directed that procedures are to be followed for implementing data fixes.

6 Month Response: DIS management holds a quarterly quality control meeting to ensure that staff is following the procedures.

Finding No. 8: A system edit implemented to prevent prohibited contractual service expense disbursements from being paid from an expense category was not working properly in all scenarios throughout the application.

Recommendation: The Department should review edit controls and correct the specific edit problem noted above.

Response: The Department concurs. DIS staff has conducted research and testing to determine requirements for correcting the improperly functioning edit. DIS' research has revealed that additional refinements to the edits to include encumbrances and payables with this object code/category combination are required. Currently, DIS staff is running a report to monitor the system for any disbursement transactions that contain the object code/category combination in this scenario. If any are found, they will be treated as a production problem and corrected as quickly as possible. DIS and Accounting and Auditing are designing the additional edits and plan to have the new edits in place by 1-1-2008.

6 Month Response: On 11-1-2007, contractual service edits went into effect, preventing agencies from adding new encumbrance transactions, accounts payable transactions and encumbered payable transactions that a contractual service object code and expense category. On 1-1-2008 the edits were updated to include budgetary transactions. Agency Addressed Memorandum No.2, 2007-2008 was issued on 10-19-2007 to inform agencies of the new edits.

Finding No. 9: We noted a programming error in the salary refund calculation of net pay that resulted in inaccurate salary refunds for four employees.

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

Response: The Department concurs. DIS and Accounting and Auditing staff determined that in the case of net pay calculations for salary refunds, additional program edits were necessary to prevent future occurrences of salary refunds being processed when there are refund calculation errors. Code changes for the additional edits were implemented on 9-27-07.

6 Month Response: No errors have occurred since the edits were implemented on 9-27-2007.

Finding No. 10: Department staff did not have procedures in place to verify that the total State Active Duty (SAD) W-4 records sent from the Department of Military Affairs matched the records received on the Department's SAD W-4 control totals report produced during the processing of the SAD W-4 file.

Recommendation: Department staff should follow the newly implemented procedures to ensure that all records received are processed and corrected in a timely manner.

Response: The Department concurs. The Control Totals Report is a new tool to help BOSP expedite a notification to the Department of Military Affairs (DMA) payroll staff of incomplete or missing W-4 records on a SAD payroll. The Division of Accounting and Auditing will educate staff on the new tool and the procedures associated with the new tool by 10-31-2007.

6 Month Response: The BOSP staff has been following the new procedures that were put in place utilizing the Control Totals report for validation. For every SAD W-4 file received, the staff verifies the totals report to ensure that no issues have been found. Since implementing the procedure, there have been no discrepancies in the data received from the Department of Military Affairs.