CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

July 5, 2012

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

Dear Mr. Atwater:

As required by Section 20.055, Florida Statutes, I have enclosed the Department's six-month status report of corrective actions taken in response to Auditor General Report Number 2012-071, *Department of Financial Services STARS Information Technology Operational Audit* (published January 5, 2011).

If you have any questions, please do not hesitate to contact me.

Sincerely,

Ned Luczynski

NL:sll

Enclosure

cc: Robert Kneip, Chief of Staff
P.K. Jameson, General Counsel
R. J. Castellanos, Director, Division of Risk Management
Kathy DuBose, Coordinator, Joint Legislative Auditing Committee

FLORIDA DEPARTMENT OF FINANCIAL SERVICES
Ned Luczynski • Inspector General
200 E. Gaines St. • Tallahassee, FL 32399-0312 • Tel. 850-413-3112 • Fax 850-413-4973
Email • Ned.Luczynski@myfloridacfo.com

Department of Financial Services
Office of Inspector General

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012
Finding No. 1	The access privileges of some employees, contractors, and external users were not necessary for the users' assigned job responsibilities and did not enforce an appropriate separation of duties. Additionally, contrary to Department *Policy*, the Division lacked written procedures for controlling access to the STARS application.		
Recommendation	The Department should limit access privileges to STARS resources to only what is needed to perform job responsibilities. The Department should also evaluate employee job responsibilities relating to STARS and make appropriate changes to enforce an appropriate separation of incompatible duties such as, for example, updating the rolodex and generating payments. Additionally, the Department should develop written procedures for controlling access to the STARS application.		
Original Response	We concur. The Division of Risk Management is in the process of limiting access privileges to the STARS application to only those privileges necessary based on user job responsibility. Additionally, the Division of Risk Management will create access control procedures for controlling access to STARS. These procedures will identify the positions that should be granted access and the type of access to be granted based on the position's job responsibilities. In conjunction with the new procedures, the Division of Risk Management will implement quarterly reviews to ensure access privileges remain appropriate in accordance with Department Policy. The Division of Information Systems is in the process of identifying and limiting access privileges to the STARS application servers to only those positions necessary based on user job responsibilities.		
Six-month Follow-up:	July 5, 2012		
Responsible Divisions	Division of Risk Management Division of Information Systems		
Reported Status	The Division of Risk Management reviewed and limited user access privileges to the STARS application to only those privileges necessary based on user job responsibility. Additionally, the Division of Risk Management has created access control procedures for controlling access to STARS. These procedures identify the user access permissions which should not be combined and outline the process for requesting access to the system. In conjunction with the new procedures, the Division of Risk Management has implemented quarterly access reviews to ensure privileges remain appropriate in accordance with Department Policy. In January 2012, the Division of Information Systems completed identification and restriction of access privileges to the STARS application servers to only		

	those positions necessary based on user job responsibilities.
OIG Assessment	**PARTIALLY CLOSED.** It appears management has taken appropriate action to address the finding and recommendations. However, the OIG will continue to monitor this issue until such time as Division management approves the draft written procedures.

Department of Financial Services
Office of Inspector General

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012
Finding No. 2	Authorization documentation for STARS access privileges for some users was missing or incomplete.		
Recommendation	The Department should maintain complete documentation of management authorization for user access to STARS that specifies the security profiles assigned to the users.		
Original Response	We concur. The Division of Risk Management is in the process of revising its access authorization practices to ensure that user access authorizations are appropriately documented and specify the access privileges being requested for the users. The Division has already implemented a process for maintaining STARS access authorization documentation.		
Six-month Follow-up:	July 5, 2012		
Responsible Division	Division of Risk Management		
Reported Status	The Division of Risk Management revised its access authorization practices to ensure that user access authorizations are appropriately documented and specify the access privileges being requested for the users. The Division also implemented a process for maintaining STARS access authorization documentation.		
OIG Assessment	**PARTIALLY CLOSED.** It appears management has taken appropriate action. However, the OIG will continue to monitor this issue until such time as Division management approves the draft written procedures.		

Department of Financial Services
Office of Inspector General

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012

Finding No. 3	Department records of network access deactivation dates were manually prepared rather than system-generated, which may lessen management's assurance of the reliability and completeness of the records. In addition, contrary to Department *Policy*, the Department did not document the deactivation of access to the STARS application. We also noted that the Department did not timely deactivate the STARS server administrator access privileges of one former contractor.
Recommendation	The Department should comply with *AP&P 4-05* and also enhance its practices to ensure that the access privileges of all former employees and contractors are deactivated in a timely manner.
Original Response	We concur. The Department is actively working to enhance procedures to ensure timely disablement of network access privileges for separating employees, and the complete documentation of disablement tasks. The Division of Risk Management is exploring a revision of access control practices to eliminate the reissuance and reactivation of STARS user IDs to ensure that access control records for separated employees are appropriately maintained in STARS. Until the practice change has been adopted, the Division has implemented a process for preserving the access control records for separated employees outside of the application. The Division of Risk Management is working with the Division of Information Systems to ensure compliance with this requirement in the future Risk Management Information System (RMIS) procurement. The Division of Information Systems disabled the server administrator access ID for the former contractor. Additionally, the Division has already implemented a monitoring tool to more accurately record the actual date network privileges were disabled.

Six-month Follow-up:	July 5, 2012
Responsible Divisions	Division of Risk Management Division of Information Systems
Reported Status	The Department has enhanced procedures to ensure timely disablement of network access privileges for separating employees, and the complete documentation of disablement tasks. The Division of Risk Management has revised its access control practices to eliminate the reissuance and reactivation of STARS user IDs to ensure that access control records for separated employees are appropriately maintained in STARS. Additionally, the Division of Risk Management is working with the Division of Information Systems to ensure compliance with this requirement in

	the future Risk Management Information System (RMIS) procurement. In June 2011, the Department procured a monitoring tool to more accurately record the date network privileges are disabled. On July 13, 2011 the Division of Information Systems implemented this tool and since that time has been capturing these records.
OIG Assessment	**CLOSED.** It appears Department and Division management has enhanced practices in this area.

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012

Finding No. 4	Contrary to the State of Florida, *General Records Schedule* requirements for the retention of access control records, the Department did not retain complete access control records.
Recommendation	The Department should retain access control records as required by the *General Records Schedule*.
Original Response	We concur. The Division of Risk Management is exploring a revision of access control practices to eliminate the reissuance and reactivation of STARS user IDs to ensure that access control records for separated employees are appropriately maintained in STARS. The Division has, however, implemented a process for preserving the access control records outside of the application for both separated employees and employees whose access has been modified. The Division of Risk Management is working with the Division of Information Systems to ensure compliance with this requirement in the future Risk Management Information System (RMIS) procurement. The Division of Information Systems has already implemented a monitoring tool to more accurately record the actual date network access privileges of separating employees were disabled. These access control records will be retained in the system indefinitely.
Six-month Follow-up:	July 5, 2012
Responsible Divisions	Division of Risk Management Division of Information Systems
Reported Status	The Division of Risk Management has revised its access control practices to eliminate the reissuance and reactivation of STARS user IDs to ensure that access control records for separated employees are appropriately maintained in STARS. Additionally, in accordance with *General Records Schedule*, the Division implemented a process for preserving the access control records outside of the application for both separated employees and employees whose access has been modified. The Division of Risk Management is also working with the Division of Information Systems to ensure compliance with this requirement in the future Risk Management Information System (RMIS) procurement. In June 2011, the Department procured a monitoring tool to more accurately record the date network privileges are disabled. On July 13, 2011 the Division of Information Systems implemented this tool and since that time has been capturing these records.
OIG Assessment	**CLOSED.** It appears management has taken appropriate action.

Department of Financial Services
Office of Inspector General

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012
Finding No. 5	Contrary to Agency for Enterprise Information Technology (AEIT) Rules and Department *Policy*, some generic and shared user identification codes (IDs) existed with access privileges to STARS data and IT resources.		
Recommendation	The Department should assign unique user IDs to each individual who is authorized to access STARS data and IT resources as required by AEIT Rules and *AP&P 4-05*.		
Original Response	We concur. The Division of Risk Management has limited the use of generic user IDs within the STARS application by deactivating the three accounts that were no longer being utilized. Additionally, Division management has instructed staff on Department Policy prohibiting the sharing of network user ID's. The Division of Information Systems created individual STARS database administrative accounts for the Database Administrators.		
Six-month Follow-up:	July 5, 2012		
Responsible Divisions	Division of Risk Management Division of Information Systems		
Reported Status	The Division of Risk Management has limited the use of generic user IDs within the STARS application by deactivating the three accounts that were no longer being utilized. Additionally, Division management has instructed staff on Department Policy prohibiting the sharing of network user ID's. The Division of Information Systems created individual STARS database administrative accounts for the Database Administrators.		
OIG Assessment	**CLOSED.** As indicated in the original response, corrective action was taken in response to the finding and recommendation.		

Department of Financial Services
Office of Inspector General

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012
Finding No. 6	The Department's review of the appropriateness of STARS user access privileges was not conducted on a sufficiently frequent basis. Additionally, documentation of access reviews conducted was not retained and results of the reviews were not reported, contrary to Department *Policy*.		
Recommendation	The Department should ensure that STARS access privileges are reviewed quarterly as required by *AP&P 4-05*. Additionally, the Department should retain documentation of access reviews and report the results to the Division of Information Systems Compliance Office.		
Original Response	We concur. The Division of Risk Management is in the process of revising its practices to ensure that quarterly reviews of access privileges are conducted and that documentation of reviews is retained. The Division of Risk Management will work with the Division of Information Systems to ensure compliance with this requirement in future Risk Management Information System (RMIS) procurements.		
Six-month Follow-up:	July 5, 2012		
Responsible Division	Division of Risk Management		
Reported Status	The Division of Risk Management has revised its practices to ensure that quarterly reviews of access privileges are conducted and that documentation of reviews is retained. The Division of Risk Management is also working with the Division of Information Systems to ensure compliance with this requirement in the future Risk Management Information System (RMIS) procurement.		
OIG Assessment	**CLOSED.** It appears management has taken appropriate corrective action.		

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012

Finding No. 7	Certain Department security controls related to user authentication, session controls, and logging needed improvement.
Recommendation	The Department should implement appropriate security controls related to user authentication, session controls, and logging to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.
Original Response	We concur. The Department is working to enhance security controls in the areas noted in the report.
Six-month Follow-up:	July 5, 2012
Responsible Divisions	Division of Risk Management Division of Information Systems
Reported Status	The Department is working to enhance security controls in the areas noted in the report.
OIG Assessment	**OPEN.** The OIG will continue to monitor actions taken to enhance security controls.

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012
Finding No. 8	STARS application program change controls needed improvement and the Department had not established written procedures for managing changes to the STARS application.		
Recommendation	The Department should establish and follow written procedures for managing changes to the STARS application, including provisions for documenting key program change activities such as authorization and testing of program changes and user approval for changes to be moved into the production environment. The Department should also implement a process for monitoring the movement of program changes into production to ensure that unauthorized or erroneous changes, should they occur, are timely detected.		
Original Response	We concur. The Division of Risk Management will enhance its change management process to ensure that changes to STARS are appropriately authorized, documented, tested, and approved. Additionally, the Division of Risk Management will work with the Division of Information Systems to establish written procedures for managing changes to the application.		
Six-month Follow-up:	July 5, 2012		
Responsible Division	Division of Risk Management		
Reported Status	The Division of Risk Management has enhanced its change management process to ensure that changes to STARS are appropriately authorized, documented, tested, and approved. Additionally, the Division of Risk Management is drafting written procedures for managing changes to the application.		
OIG Assessment	**OPEN.** The OIG will continue to monitor this finding until such time as the Division adopts written procedures governing the change management process.		

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012

Finding No. 9	STARS lacked a data edit to disallow the payment of medical benefits incurred after the date of denial for controverted claims (initial claims that were denied). Additionally, no reporting was in place to allow claims supervisors to monitor the payment of benefits on controverted claims.
Recommendation	The Department should establish a data edit in STARS that prevents payments for medical benefits incurred after the date of denial on controverted claims. Until such a data edit can be established in STARS, the Department should implement exception reporting and monitoring to detect and follow-up on such payments, should they occur.
Original Response	We concur. The Division of Risk Management has determined that limitations prevent the implementation of this type of data edit and also prevent the production of an exception report. The Division of Risk Management will work with the Division of Information Systems to evaluate the feasibility of options for implementing exception reporting and monitoring outside of the application. The Division of Risk Management will work with the Division of Information Systems to ensure compliance with this requirement in future Risk Management Information System (RMIS) procurements.
Six-month Follow-up:	July 5, 2012
Responsible Divisions	Division of Risk Management Division of Information Systems
Reported Status	The Division of Risk Management determined that limitations prevent the implementation of this type of data edit and also prevent the production of an exception report. Due to these limitations, the Division of Risk Management has implemented a process to provide a Controverted Claims with Payments report to Claims staff for review on a monthly basis. Additionally, the Division of Risk Management is working with the Division of Information Systems to ensure compliance with this requirement in the future Risk Management Information System (RMIS) procurement.
OIG Assessment	**PARTIALLY CLOSED.** It appears management has taken steps to address the recommendation. However, the OIG will continue to monitor this issue until such time as the Division establishes formal exception reporting, monitoring and follow-up procedures.

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012

Finding No. 10	Confidential and exempt workers' compensation claims information such as Social Security numbers and medical information was not encrypted in some transmissions, contrary to AEIT Rules and Department *Policy.*
Recommendation	The Department should implement appropriate controls to ensure that the transmission of confidential and exempt information is secured as required by AEIT Rule 71A-1.006, Florida Administrative Code, and *AP&P 4-03.* The Department should also work with TPAs to ensure that confidential and exempt information is sent to the Department only in a secured manner.
Original Response	We concur. The Division of Information Systems has enhanced the Department's IT infrastructure to provide multiple technologies to facilitate the secure transmission of confidential and exempt information. Division of Risk Management staff has received guidance on the use of these technologies and are using them to transmit confidential and exempt information. Additionally, the Division of Risk Management is working with the Third Party Administrators to ensure that information sent to the Department is transmitted in a secure manner.
Six-month Follow-up:	July 5, 2012
Responsible Division	Division of Risk Management
Reported Status	The Division of Information Systems has enhanced the Department's IT infrastructure to provide multiple technologies to facilitate the secure transmission of confidential and exempt information. In March 2012, Division of Risk Management staff received guidance on the use of these technologies and are using them to transmit confidential and exempt information. Additionally, the Division of Risk Management continues to work with the Third Party Administrators to ensure that information exchanged with the Department is transmitted in a secure manner.
OIG Assessment	**CLOSED.** Our review showed that management has undertaken a number of initiatives in this area and continues to work with external entities to ensure the secure transmission of confidential and exempt information.

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012
Finding No. 11	The Department did not monitor payments for medical services to providers from the Genex billing process to ensure that claims were paid within 45 days of receipt, contrary to Section 440.20(6)(b), Florida Statutes.		
Recommendation	The Department should monitor billing claims for medical services to ensure that claims are paid within 45 days of receipt as required by State law.		
Original Response	We concur. The Division of Risk Management is working with Genex to identify and correct payment delay issues. Additionally, the Division of Risk Management will work with the Division of Information Systems to ensure compliance with this requirement in future Risk Management Information System (RMIS) procurements.		
Six-month Follow-up:	July 5, 2012		
Responsible Division	Division of Risk Management		
Reported Status	The Division of Risk Management has implemented a new process with Genex to identify and correct payment delay issues. The Division of Risk Management is also working with the Division of Information Systems to ensure compliance with this requirement in the future Risk Management Information System (RMIS) procurement.		
OIG Assessment	**PARTIALLY CLOSED.** It appears management has initiated action to address the recommendation. However, the OIG will continue to monitor efforts in this area.		

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012
Finding No. 12	Contrary to Department of Financial Services, Division of Workers' Compensation Rule 69L-56.3013(4)(a), Florida Administrative Code, sub-annual filings on open claims to the Division of Workers' Compensation were not always timely. Additionally, no reporting mechanism existed in STARS to allow Division staff to proactively ensure that filings were completed in a timely manner and filed with the Division of Workers' Compensation.		
Recommendation	The Department should ensure that the *Electronic Sub-Annual Claim Cost Reports* are filed with the Division of Workers' Compensation as required within the time frame specified. Additionally, the Department should review the *Missing SA Report* to ensure that past due reports are filed.		
Original Response	We concur. The Division of Risk Management has determined that STARS system configuration limitations prevent the implementation of a system trigger. The Division will implement a process for reviewing the *Missing SA Report*. Additionally, the Division of Risk Management will work with the Division of Information Systems to ensure compliance with this requirement in future Risk Management Information System (RMIS) procurements.		
Six-month Follow-up:	July 5, 2012		
Responsible Division	Division of Risk Management		
Reported Status	The Division of Risk Management is working to create an interim report to pull information from STARS data tables to ensure that reports are filed. Additionally, the Division of Risk Management is working with the Division of Information Systems to ensure compliance with this requirement in the future Risk Management Information System (RMIS) procurement.		
OIG Assessment	**OPEN.** The OIG will continue to monitor management's actions to correct the issues noted in this finding.		

SIX-MONTH FOLLOW-UP REPORT
STATUS OF CORRECTIVE ACTION

Reviewing Entity	Report No.	Report Title	Date Published
Auditor General	2012-071	***Department of Financial Services STARS Information Technology Operational Audit***	January 5, 2012
Finding No. 13	Data reconciliation procedures were lacking between STARS and the temporary total disability (TTD) database that was used to generate invoices to State agencies for reimbursement of the first ten weeks of TTD payments.		
Recommendation	The Department should implement the necessary controls to ensure that data transfers between STARS and the TTD database are complete and accurate. Additionally, the Department should implement procedures for reconciling the TTD benefit payment data transferred from STARS to the TTD database, including records written to the append file for manual review.		
Original Response	We concur. The Division of Risk Management has implemented a pay code to identify TTD payments which will be pulled into a report for the purpose of data exchange reconciliation. The Division of Risk Management is working with the Division of Information Systems to develop the report.		
Six-month Follow-up:	July 5, 2012		
Responsible Divisions	Division of Risk Management Division of Information Systems		
Reported Status	The Division of Risk Management is working with the Division of Information Systems to develop the TTD report.		
OIG Assessment	**OPEN.** The OIG will continue to monitor management's actions to implement the recommended controls and procedures.		