REPORT NO. 2012-071
JANUARY 2012

DEPARTMENT OF FINANCIAL SERVICES

STARS

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

CHIEF FINANCIAL OFFICER

Pursuant to Article IV, Sections 4.(c) and 5.(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Jeff Atwater served as Chief Financial Officer during the period of our audit.

The audit team leader was Brenda Shiner, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF FINANCIAL SERVICES

STARS

SUMMARY

The Department of Financial Services (Department), Division of Risk Management (Division) is responsible for providing technical assistance to participating State agencies in managing risk and providing workers' compensation, liability, federal civil rights, automobile liability, and property insurance coverage at reasonable rates. The Division provides self-insurance, purchase of insurance, and claims administration services. Within the Division, the Bureau of Claims Administration is responsible for the management of claims reported by or against State agencies for coverage under the self-insurance fund known as the State Risk Management Trust Fund.

STARS is a risk management information system owned and licensed by CS STARS, LLC, a wholly owned subsidiary of Marsh USA, Inc., and is used by the Division for claim administration functions related to the State Risk Management Trust Fund.

Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to STARS. The results of our audit are summarized below:

SECURITY CONTROLS

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.

Finding No. 2: Authorization documentation for STARS access privileges for some users was missing or incomplete.

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.

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.

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.

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*.

Finding No. 7: Certain Department security controls related to user authentication, session controls, and logging needed improvement.

PROGRAM CHANGE CONTROLS

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.

APPLICATION CONTROLS

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.

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*.

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.

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.

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.

BACKGROUND

The Division of Risk Management (Division) is composed of the Bureau of Loss Prevention and Bureau of Claims Administration. Bureau of Loss Prevention responsibilities include managing the State's property insurance program and administration of the Division's budget. The Bureau of Claims Administration is responsible for the investigation, resolution, and settlement of claims involving or against State agencies, universities, and injured State employees.

Within the Bureau of Claims Administration, the Workers' Compensation section is responsible for processing and paying workers' compensation benefits for injured State employees, including medical, indemnity (lost wages), and death benefits. Since January 1997, the Division has contracted with various third-party administrators (TPAs) for workers' compensation claims management. OptaComp is contracted with to manage claims with a date of injury of January 1, 2009, through December 31, 2013. Depending on the employee's date of injury, claims initiated prior to January 1, 2009, are serviced by various companies including CorVel Corporation and Genex Services, Inc. (Genex). Additionally, the Division contracts with Cypress Care for pharmacy benefits management for all claims.

Within the Department, the Division of Workers' Compensation is responsible for overseeing the Workers' Compensation Law as defined in Chapter 440, Florida Statutes. Within the Division of Workers' Compensation, the Bureau of Monitoring and Audit is responsible for carrier and claims-handling entity accountability and enforcement to ensure that the entities meet their obligations under Chapter 440, Florida Statutes, and administrative rules. The Bureau of Monitoring and Audit's responsibilities include, among other things, ensuring that medical bills are paid timely and all required claims data are accurately and timely filed with the Division of Workers' Compensation.

During the period of our audit, the Division of Risk Management managed security administration functions for STARS user accounts. The Division of Information Systems within the Department was responsible for managing and maintaining the STARS infrastructure. CS STARS, LLC, was the contractor responsible for the maintenance and support of STARS including the development and promotion of STARS program changes.

FINDINGS AND RECOMMENDATIONS

Security Controls

Finding No. 1: Appropriateness of Access Privileges

Effective security controls include logical (electronic) access controls that limit user access privileges to only what is needed in the performance of assigned job responsibilities and enforce an appropriate separation of incompatible duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

Agency for Enterprise Information Technology (AEIT) Rule 71A-1.007(3), Florida Administrative Code, provides that workers, including employees, contractors, and other persons whose conduct is under the direct supervision of an agency, shall be authorized access to agency IT resources based on the principles of "least privilege" (the principle that grants the minimum possible privileges to permit a legitimate action) and "need to know" (the principle that individuals are authorized to access only specific information needed to accomplish their individual job duties). AEIT Rule 71A-1.007(5), Florida Administrative Code, provides that, for functions susceptible to fraudulent or other unauthorized activity, an agency shall ensure separation of duties so no individual has the ability to control the entire process.

Our audit disclosed that some STARS users, including Department employees, contractors, and external users such as third-party administrators, had update access privileges that were not necessary for their job responsibilities and did not enforce an appropriate separation of duties. These conditions increased the risk of errors, fraud, misuse, or other unauthorized modification of Department data, as described in the following paragraphs.

There were 108 active STARS Division user accounts as of June 30, 2011. As a part of our audit, we reviewed the access privileges associated with all 22 STARS Division user accounts for the 10 users who had multiple accounts. We also reviewed the access privileges for a sample of 10 of the remaining 86 active user accounts. Our review disclosed user accounts that had update access privileges that were not necessary for their job responsibilities, did not enforce an appropriate separation of duties, and allowed access to internal claims (claims filed by Division employees), contrary to Division Policies and Procedures, *Administration of Claims Filed by Division of Risk Management Employees and Their Relatives 1.12 (Policy 1.12).* The results of our review are listed below in Table 1.

Table 1

Review of STARS Division User Accounts As of June 30, 2011	Multiple Accounts for Users	Single Accounts for Users	Total Active Division User Accounts
Active Accounts at 6-30-11	22	86	108
Accounts Reviewed by Auditor	22	10	32
Accounts with Unnecessary Update Access Privileges	16	2	18
Accounts with Privileges Allowing Incompatible Duties: (1)			
Update Claims, Update Rolodex (2), and Generate Payments	4	1	5
Update Claims and Update Rolodex	2	1	3
Update Rolodex and Generate Payments		1	1
Update Claims and Generate Payments	1		1
Fraud Investigator with Update Claims	2		2
Total Accounts with Privileges Allowing Incompatible Duties	9	3	12
Accounts That Could Access Internal Claims (3)	7	1	8

Notes (1): All 12 accounts were also among the 18 listed above that had unnecessary access privileges.
(2): Update access to the rolodex allows the user to create, modify, or delete vendor records.
(3): Five of these accounts were also among the 12 listed above with privileges allowing incompatible duties.

Because our sample described above disclosed some user accounts with access privileges that were contrary to an appropriate separation of duties, we expanded our testing and requested a listing of all users with active rolodex (vendor file) update access as of September 7, 2011. In response, the Department provided to us a manually compiled list of eight users; three of whom had already been evaluated as part of our review described above and five users who were not included in the above-described review. From our review of organizational charts and interviews with staff on job responsibilities, we were aware of additional Division employees who updated the rolodex but were not on the manual list that the Department provided. Because of ineffective access reporting functions in STARS, the Department lacked a way to effectively determine which users had critical access privileges and thus could not demonstrate the appropriateness of access. Notwithstanding the limitations of the manually compiled list, we reviewed the active user accounts of the five remaining users. Two of the five user accounts had update access privileges that were not necessary for their job responsibilities. Additionally, all five of the user accounts had access privileges that did not enforce an appropriate separation of incompatible duties. Specifically:

- Two of the user accounts were assigned access privileges that allowed the user to update claims, add to or update the rolodex, and generate payments on claims.
- Two of the user accounts were assigned access privileges that allowed the user to add to or update the rolodex and generate payments on claims.
- All five of the user accounts were also assigned access privileges to access internal claims, contrary to *Policy 1.12*.

Through additional audit procedures, we also noted three additional Division user accounts with access privileges to add payments on claims and print checks, contrary to an appropriate separation of duties.

Additionally, we tested eight active external user accounts as of June 30, 2011. All eight user accounts were assigned update access privileges that were not necessary for their job responsibilities.

The complexity of the design and assignment of STARS user access groups may have contributed to the difficulty in ensuring that assigned access privileges were appropriate for users. Also, from observations and interviews, we determined that access privileges were typically duplicated from existing user accounts without inspection of the privileges that were being duplicated, which in some cases promoted the perpetuation of inappropriate access to STARS. As a result, the access control administrator unknowingly issued access privileges that exceeded what was required by users.

We also evaluated access to the STARS application servers and determined that 169 users including employees, contractors, and external users had been assigned administrator privileges (unrestricted access) to the servers. Administrator privileges are typically restricted to IT staff responsible for maintaining the application; however, in this case, administrator privileges had been assigned to user accounts regardless of assigned job responsibilities.

Our audit further disclosed that the Division lacked written procedures for controlling access to the STARS application, contrary to the requirements of Department Administrative Policies and Procedures (AP&P) 4-05, *Application Access Control (AP&P 4-05)*. *AP&P 4-05* requires application owners to develop written procedures for controlling access to their applications. Specifically, these written procedures were to include all activities and resources associated with administering access and standards detailing how the business unit determined who should have access to its applications. The lack of written procedures for controlling access increases the risk that access controls may not be followed consistently and in a manner pursuant to management's expectations.

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.

Finding No. 2: STARS Access Authorization Documentation

AEIT Rule 71A-1.007(1), Florida Administrative Code, provides that information owners shall be responsible for authorizing access to information. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized. In STARS, users were assigned user accounts with security profiles that included specific access privileges.

We requested access authorization documentation for the 37 active STARS Division user accounts described above in Finding No. 1 (32 user accounts as of June 30, 2011, and 5 user accounts as of September 7, 2011) to determine if access granted to STARS was adequately documented and authorized. For 28 of the 37 user accounts, authorization documentation for the user access privileges did not exist. Our review of the nine access authorization documents that were on file in the Department's records disclosed that required information was absent from seven of the nine documents. Specifically, seven of the documents lacked the security profiles that had been assigned to the users. As indicated by the inappropriate access privileges described above in Finding No. 1, the lack of complete and specific documentation of management's authorization of user access privileges may limit the Department's ability to ensure that user access privileges granted to employees do not exceed what is necessary for the accomplishment of assigned job responsibilities.

Recommendation: The Department should maintain complete documentation of management authorization for user access to STARS that specifies the security profiles assigned to the users.

Finding No. 3: Timely Deactivation of STARS Access Privileges

Effective access controls include provisions for timely deactivating employee and contractor access privileges when employment or contract terminations occur. Prompt action is necessary to ensure that the former employee, contractor, or others do not misuse the former employee's or contractor's access privileges.

Access privileges to STARS are granted through the assignment of STARS user logons. Additionally, a user must successfully log on to the Department's network in order to gain access to STARS. As discussed further in Finding No. 4 below, the Department did not retain complete STARS and network access control records, including the dates that access privileges were deactivated.

AP&P 4-05 requires the use of a Remedy ticket for the purpose of tracking the progress of access deactivation tasks for former employees or contractors. However, the Remedy tickets were manually entered by Department staff and were not system-generated records, which may lessen management's assurance of the reliability and completeness of the records. Additionally, the Department prepared Remedy tickets for the deactivation of network, but not STARS application, access privileges, contrary to *AP&P 4-05*. Because of the limitations in the Department's records of access deactivation tasks, the Department could not demonstrate upon audit request that former employee or contractor access privileges had been timely deactivated.

Notwithstanding the limitations of the Department's records, we noted that one former contractor retained administrator access privileges to the STARS server after the termination of his contractual services on July 25, 2007. Although the former contractor's network access privileges had been deactivated timely, his server administrator access ID was still active as of August 5, 2011. Under these conditions, the risk was increased that the former contractor's access privileges may be misused by a valid network user.

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.

Finding No. 4: Access Control Records Retention

The State of Florida, *General Records Schedule GS-1-SL for State and Local Government Agencies (General Records Schedule)*, revised by the Department of State effective August 2010, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment.

Contrary to *General Records Schedule* requirements, the Department did not retain complete STARS access control records. The Department reactivated and reissued to new employees the user IDs and accounts of former employees with access to STARS. Once accounts were reissued, the record of the former employees' access to STARS no longer existed, including the dates that the access privileges were removed.

Additionally, in some instances, former employee access privileges had been used subsequent to employee terminations to generate reports developed by the former employees, causing the dates of access removal for the accounts to be overwritten with the dates the accounts were subsequently used to access STARS. Also, when modifications were made to existing employee access privileges in STARS, the unneeded access privileges were removed and records of the previous access privileges were deleted.

Without the adequate retention of access control records, the risk is increased that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur. Additionally, the Department is not in compliance with the State's record retention requirements. A similar finding with regard to the retention of network access control records was noted in our report No. 2012-016, IT Operational Audit of the Department of Financial Services, Florida Accounting Information Resource (FLAIR) Subsystem, dated October 2011.

Recommendation: The Department should retain access control records as required by the *General Records Schedule*.

Finding No. 5: User Identification

The effectiveness of access controls is dependent, in part, on the ability to uniquely identify system users. Unique identification of individual users assists in the assignment of specific access privileges and provides a mechanism for attributing system actions to a responsible user. AEIT Rule 71A-1.019(11), Florida Administrative Code, provides that agency computer users shall have unique user accounts. AEIT Rule 71A-1.019(16), Florida Administrative Code, further provides that agency workers shall not share, among other things, their agency accounts, personal identification numbers, or other devices used for identification or authentication purposes. Additionally, *AP&P 4-05* states that, to ensure accountability, users shall be assigned a unique user ID and users shall not share their unique user ID.

Our audit disclosed that, contrary to AEIT Rules and *AP&P 4-05*, some generic and shared user IDs existed with access privileges to STARS data and IT resources. Specifically:

- Five generic user IDs with update access privileges to STARS existed. According to the access control administrator, three of these accounts were no longer being utilized but had not been deactivated. The remaining two accounts were being utilized by the software provider for the purpose of system maintenance.
- A user ID for the administration of the STARS database servers was being shared among five Division of Information Systems employees who were responsible for managing the STARS servers.
- A user ID for the administration of the STARS database was being shared among four Division of Information Systems employees who were responsible for managing the STARS database.
- Two Division of Risk Management employees shared a network user ID for the purpose of downloading workers' compensation claim files.

Without uniquely identified system users, the Department's ability to establish accountability for system actions may be limited.

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*.

Finding No. 6: Periodic Review of STARS Access Privileges

Periodic reviews of user access privileges help ensure that user access privileges remain appropriate. Additionally, according to *AP&P 4-05*, business unit level reviews shall be conducted quarterly at a minimum and results reported to the Division of Information Systems Compliance Office. *AP&P 4-05* provides that accounts must be reviewed to ensure that access privileges are consistent with the roles and responsibilities that users require in order to perform their assigned duties and that privileges of former users have been removed within established time frames.

According to Division staff, STARS user access listings were reviewed as time permitted to verify that the access privileges were appropriate. However, documentation of prior access reviews was not retained and results of the reviews were not reported to the Division of Information Systems Compliance Office. The complexity of the design and assignment of STARS user access groups, coupled with the absence of authorization documentation as noted in Finding No. 2, may have limited the effectiveness of the Department's review of user access privileges. The importance of STARS to the Workers' Compensation Program and the existence of excessive STARS access privileges as described in Finding No. 1 indicate the need for the Department to review STARS access privileges at least quarterly pursuant to *AP&P 4-05*.

The lack of periodic reviews of access privileges was contrary to *AP&P 4-05* and increased the risk that excessive or inappropriate access privileges will not be timely detected or deactivated. Under such conditions, the risk is increased that unauthorized disclosure, modification, and destruction of STARS data and IT resources will occur and not be detected.

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.

Finding No. 7: Security Controls – User Authentication, Session Controls, and Logging

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls related to user authentication, session controls, and logging that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate security controls related to user authentication, session controls, and logging, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

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.

Program Change Controls

Finding No. 8: Program Change Management

Effective controls over modification of application programs help ensure that only authorized, tested, and approved changes are implemented. The effectiveness of program change controls is enhanced when management's expectations for the control of program changes are documented in the form of written procedures.

STARS application program changes were made by the STARS software provider, CS STARS, LLC. Additionally, the software provider was responsible for moving completed program changes into the production environment. The software provider maintained a log of STARS action items that included, among other things, change requests for the STARS application. However, the Division did not maintain documentation of change request authorizations, testing of program changes, or user approvals for changes to be moved into the production environment. Additionally, no reporting existed to allow the Division to monitor the movement of program changes made by the software provider

into the production environment. Under these conditions, the risk was increased that unauthorized changes that impact the proper functioning of STARS could occur without timely detection.

Also, the Division had not established written procedures for managing changes to the STARS application, including procedures for authorization, testing, and approval of program changes made by the software provider, contrary to Department AP&P 1-02, *Internal Controls Policy (AP&P 1-02)*. *AP&P 1-02* required the divisions to establish and maintain a system of internal controls, including procedures to provide reasonable assurance that division objectives were met. The lack of written program change control procedures increases the risk that program change controls may not be followed consistently and in a manner pursuant to management's expectations.

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.

Application Controls

Finding No. 9: STARS Data Edit

Application controls include data edits and validation checks against data being processed to ensure that only valid transactions are processed. Additional controls include exception reporting and monitoring procedures to ensure that errors and irregularities are detected.

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. Without a data edit in STARS to prevent or report the payment of medical services incurred after the date of denial on a controverted claim, the risk is increased that medical benefits may be paid on controverted claims and not be timely detected.

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.

Finding No. 10: Protection of Confidential and Exempt Medical Claims Information

Confidentiality controls provide reasonable assurance that application data, reports, and other outputs are protected against unauthorized disclosure. Pursuant to Section 284.40(2), Florida Statutes, the claims files maintained by the Division of Risk Management shall be confidential and exempt from public inspection.

AEIT Rule 71A-1.006, Florida Administrative Code, provides, in part, that each agency shall encrypt confidential and exempt information sent by e-mail and encrypt electronic transmission of such information when the transport medium is not owned or managed by the agency. The Rule further provides that procedures shall be in place to ensure proper security of confidential information shared or stored with entities outside the agency. Department AP&P 4-03, *Information Technology Security Policy* (*AP&P 4-03*) also provides that confidential information must be encrypted when transmitted over the network and when sent by e-mail.

STARS contained confidential and exempt workers' compensation claims information such as claimant name, date of birth, Social Security number, and medical claims information. Our audit disclosed that confidential and exempt STARS information was not encrypted in some transmissions, contrary to AEIT Rules and *AP&P 4-03*. Specifically:

- The Division sent reports on denied workers' compensation claims that contained names and Social Security numbers to third-party administrators (TPAs) via unsecured e-mail.
- The Division sent vendor file information that contained names, addresses, and Social Security numbers to TPAs via unsecured e-mail.
- On a daily basis, the Division sent an unencrypted file of workers' compensation claim information, including name, date of birth, Social Security number, and medical information, to a contractor via an unsecured transmission.

We also noted that the Division received some unsecured e-mails from TPAs that contained name, date of birth, Social Security number, and medical information. Exchange of confidential and exempt claims information between the Department and TPAs in an unsecured form increases the risk that such information in transit may be disclosed to unauthorized persons.

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.

Finding No. 11: Timeliness of Payments to Medical Providers

Section 440.20(6)(b), Florida Statutes, provides that, for medical services provided on or after January 1, 2004, medical, hospital, pharmacy, or dental bills properly submitted by the provider, except for bills that are disallowed or denied, are to be timely paid within 45 days after receipt of the bill. Penalties for late payments that are below a minimum 95-percent timely performance standard shall be paid by the carrier to the Workers' Compensation Administration Trust Fund.

From 525 medical billing claims received from June 1, 2011, through August 10, 2011, with an initial date of injury from December 17, 1986, through December 31, 1996 (Genex-managed claims), we reviewed a sample of 25 medical billing claims to determine if the claims were paid within 45 days of receipt by the Division. For 3 of the 25 medical billing claims reviewed, the Division did not pay the provider within 45 days of receipt of the medical bill. The number of days the payment was late ranged from 3 to 26 days. Although the number of days for the exceptions in our sample resulted in a timeliness performance standard of only 88 percent, a determination of the overall performance standard would require an evaluation of all payments to determine if the Department was subject to penalties. Also, no reporting or alert functionality existed in STARS to facilitate Division monitoring to ensure that bills for medical services for the Genex-managed claims were processing timely. Without effective monitoring of the payment-reimbursement process, the Division may not meet the timeliness requirements for payment to providers as detailed in 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.

Finding No. 12: Timeliness of Claims Reporting

IT output controls ensure that reporting is accurate, complete, and timely and that output reports are in compliance with applicable laws and regulations. Pursuant to Department of Financial Services, Division of Workers' Compensation Rule 69L-56.3013(4)(a), Florida Administrative Code, claim administrators are to file an *Electronic Sub-Annual Claim Cost Report* every six months after the date of injury until the claim is closed.

According to Division staff, no reporting mechanism existed in STARS that could be used by the Division to proactively ensure that the *Electronic Sub-Annual Claim Cost Reports* were completed and filed with the Division of Workers' Compensation in a timely manner. The Division of Workers' Compensation's *Missing SA Report* dated August 15, 2011, subsequently identified that the Division had 2,347 claims that were past due for filing. However, Division staff did not review the Division of Workers' Compensation *Missing SA Report* to follow up on the overdue filings to ensure that the *Electronic Sub-Annual Claim Cost Reports* were subsequently completed. Without effective reporting to ensure sub-annual filings are completed and sent to the Division of Workers' Compensation in a timely manner, the Division is not in compliance with Department of Financial Services, Division of Workers' Compensation Rule 69L-56.3013(4)(a) Florida Administrative Code.

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.

Finding No. 13: Reconciliation of Data Exchanges

Interface controls assist in the timely, accurate, and complete processing of information between applications. Interface controls include procedures that are intended to provide reasonable assurance that all inputs into the target application have been accepted for processing and accounted for and that any missing or unaccounted for input records are identified and investigated. Such procedures include batch totals, reconciliations, and control totals.

Pursuant to Section 284.44(2) and (3), Florida Statutes, State agencies covered by the State risk management program must reimburse the Division for the first ten weeks of temporary total disability (TTD) benefits paid to an employee. The Division generates and sends monthly invoices to the State agencies to recoup the cost of the first ten weeks of TTD benefits paid on a claim. The ten weeks do not have to be consecutive but can occur over the life of the claim.

On a monthly basis, TTD benefit payments made in STARS for the prior month were exported from STARS and imported into a TTD database for further processing and invoice generation for the applicable State agency. Control totals were not generated for the export file generated from STARS, and the Department did not perform reconciliations to ensure that all the records exported from STARS were completely imported into the TTD database.

During the import process to the TTD database, some of the records were written to an exception (append) file for manual review. Record counts were produced for the append file. The exceptions were reviewed, corrected, and appended to the TTD database for invoice billing as necessary. On August 9, 2011, we observed Department staff manually reviewing exception records and appending corrections to the database and noted that record counts indicated that eight records had been inadvertently deleted from the append file. These eight records had not been reviewed by Department staff and Department staff was unable to determine which records had been deleted from the append file.

Without an effective method to reconcile the data transfer between STARS and the TTD access database, the risk is increased that records exported from STARS may not be completely and accurately imported to the TTD database and that TTD benefit costs for the first ten weeks of TTD benefits paid on claims may not be billed to State agencies, contrary to Section 284.44(2) and (3), Florida Statutes.

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.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from June 2011 through September 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to STARS in achieving management's control objectives in in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.

The scope of our audit focused on evaluating selected IT controls applicable to STARS. The audit included selected general IT controls over logical access to programs, data, and database and application change management. The audit also included data exchange controls between STARS and other significant systems and other selected STARS application IT controls and selected user controls relevant to STARS.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of STARS including the purpose of the application and identification of the users; processing location, hardware, software, and user environments; the application data flow, interfaces, and applicable manual reconciliation procedures; the access authorization process for STARS; and the application change management process.
- Evaluated the effectiveness of the procedures for documenting and authorizing user access privileges to STARS for Division employees. Specifically, we reviewed 37 Division employee STARS user accounts to determine whether the access authorization forms were on file and whether the forms specified the access privileges being requested.
- Evaluated the appropriateness of user access privileges granted to STARS for the 37 Division employee STARS user accounts included in our review described above.
- Observed and evaluated the timeliness of Genex bill reimbursements. Specifically, we reviewed a sample of 25 medical billing claims to determine if the claims were paid within 45 days of receipt by the Division.

- Evaluated the appropriateness of user access privileges granted to STARS for 15 State agency user accounts included in our sample.
- Observed and evaluated the timeliness of controverted claims reporting to third-party administrators. Specifically, we reviewed a sample of four weekly controverted claim reports to determine whether the reports were timely communicated to the current third-party administrators.
- Evaluated the appropriateness of user access privileges granted to STARS for external user accounts. Specifically, we tested all eight external user accounts to determine the appropriateness of user access privileges granted to STARS.
- Tested the appropriateness of logical access privileges to STARS system resources (application servers, database servers, and database).
- Tested the timeliness of disabling STARS user access privileges of former Division employees.
- Observed and evaluated the effectiveness of the process and manual follow-up activities related to STARS processing of temporary total disability data exports and invoicing.
- Observed and evaluated the claims reporting process, including STARS file exports.
- Observed and tested the adequacy of controls protecting the confidentiality of passwords for the STARS application, database, and network.
- Tested the effectiveness of program change management procedures followed by the Division for the STARS application.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated December 29, 2011, the Chief Financial Officer provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE

CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

December 29, 2011

Mr. David W. Martin
Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's information technology operational audit of the *Department of Financial Services, STARS.*

If you have any questions concerning this response, please contact Ned Luczynski, Inspector General, at (850) 413-4960.

Sincerely,

Jeff Atwater

JA:sll

Enclosure

DEPARTMENT OF FINANCIAL SERVICES
THE CAPITOL, TALLAHASSEE, FLORIDA 32399-0301 • (850) 413-2850 FAX (850) 413-2950

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES

STARS
Information Technology Operational Audit

Security Controls

Finding No. 1: Appropriateness of Access Privileges

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.

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.

Finding No. 2: STARS Access Authorization Documentation

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.

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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 3: Timely Deactivation of STARS Access Privileges

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.

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 will work with the Division of Information Systems to ensure compliance with this requirement in future Risk Management Information System (RMIS) procurements.

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.

Finding No. 4: Access Control Records Retention

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*.

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 will work with the Division of Information Systems to ensure compliance with this requirement in future Risk Management Information System (RMIS) procurements.

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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 5: User Identification

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*.

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.

Finding No. 6: Periodic Review of STARS Access Privileges

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.

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.

Finding No. 7: Security Controls—User Authentication, Session Controls, and Logging

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.

Response: We concur. The Department is working to enhance security controls in the areas noted in the report.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Program Change Controls

Finding No. 8: Program Change Management

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.

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.

Application Controls

Finding No. 9: STARS Data Edit

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.

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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 10: Protection of Confidential and Exempt Medical Claims Information

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.

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.

Finding No. 11: Timeliness of Payments to Medical Providers

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.

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.

Finding No. 12: Timeliness of Claims Reporting

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 was 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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

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.

Finding No. 13: Reconciliation of Data Exchanges

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.

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.