REPORT NO. 2012-179
JUNE 2012

DEPARTMENT OF FINANCIAL SERVICES

SPECIAL DISABILITY TRUST FUND
CLAIMS MANAGER 2004 SYSTEM

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

DEPARTMENT OF FINANCIAL SERVICES

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 Faye Smith, 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) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF FINANCIAL SERVICES

Special Disability Trust Fund
Claims Manager 2004 System

SUMMARY

The Special Disability Trust Fund (SDTF) was established pursuant to Section 440.49(9)(a), Florida Statutes, to encourage the employment, reemployment, and accommodation of injured workers by, among other things, mitigating the potential liability to the employer from a subsequent accident or occupational disease that would not have occurred had a permanent physical impairment not existed. Specifically, SDTF reimburses employers or their insurance companies (carriers) for a percentage of the additional workers' compensation benefits they have provided to an employee with a preexisting impairment who is subsequently injured in a covered workers' compensation accident.

SDTF is the responsibility of the Office of SDTF (SDTF Office) in the Division of Workers' Compensation (Division) within the Department of Financial Services (Department). The SDTF Office uses the SDTF Claims Manager 2004 System (SDTF System) for functions related to SDTF, including the receipt, review, acceptance, and payment of SDTF claims.

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

SECURITY CONTROLS

Finding No. 1: The access privileges of some Department users were not necessary for their job responsibilities and did not enforce an appropriate separation of incompatible job duties.

Finding No. 2: The Department's review of SDTF System IT resource access privileges needed improvement.

Finding No. 3: Some confidential and exempt SDTF information was accessible by individuals who did not have a valid business purpose to access the information.

Finding No. 4: Certain Department security controls related to access privileges, default local administrator accounts, and local server security event logging needed improvement.

OTHER GENERAL CONTROLS

Finding No. 5: SDTF System database backups were not regularly being stored at an off-site location.

APPLICATION CONTROLS

Finding No. 6: We noted discrepancies in SDTF System data. Additionally, SDTF System input, processing, and related user controls were deficient.

Finding No. 7: The Department did not reconcile claim payment data in the SDTF System to the Florida Accounting Information Resource (FLAIR) Subsystem.

Finding No. 8: Department monitoring of SDTF System logs and reports needed improvement.

BACKGROUND

SDTF was created on July 1, 1955, pursuant to Section 440.49, Florida Statutes. SDTF reimburses insurance carriers and eligible self-insured employers for eligible expenses. Section 440.49, Florida Statutes, established the eligibility requirements that carriers and employers must meet to qualify for reimbursement from SDTF. Section 440.49(11), Florida Statutes, limits the reimbursement to injuries occurring on or after July 1, 1955, and prior to January 1, 1998, prospectively abolishing the SDTF. However, the SDTF Office continues to receive, review, accept, and reimburse

eligible claims with an accident date occurring within the stated period. As of June 30, 2011, the SDTF fund liability was $998 million and the number of outstanding claims was 5,439.

The SDTF System is a multi-document client-server application specifically developed to track SDTF claims. SDTF Office staff use the SDTF System to input and approve claim notices and proof of claims; document claim offers and acceptances; and input, review, submit for payment, and maintain claim and payment information. After the SDTF Office receives a claim notice and proof of claim on behalf of the carrier or employer, the SDTF Office audits the claim to ensure that it meets statutory and legal requirements for reimbursement from the SDTF. The SDTF Office then makes a written offer for the claims that have met the requirements. Since the SDTF Office is authorized by Section 440.49(10), Florida Statutes, to compromise or controvert (revalue) claims, many claims are accepted for reimbursement at less than the full statutory reimbursement level. A claim is eligible for reimbursement after the SDTF Office receives written acceptance of the claim offer from the carrier, employer, or legal representative.

Once the written claim offer acceptance has been received by the SDTF Office, the carrier, employer, or legal representative may submit claim reimbursement requests once every 12 months for authorized claim expenses. The reimbursement request is audited by the SDTF Office to ensure that the request is in agreement with the approved claim offer and that the requested reimbursement expenses are accurate and properly supported. The SDTF System assigns an invoice number to the approved claim reimbursement request. Twice a month, the SDTF Office generates and submits a batch of approved invoices to the Bureau of Financial and Support Services (BF&SS) for payment issuance through FLAIR. The SDTF System maintains the detailed claim reimbursement request information related to reimbursement payments and the detailed information is not entered into FLAIR.

FINDINGS AND RECOMMENDATIONS

The Department is highly dependent on the security, integrity, and proper functioning of the SDTF System to ensure the accurate valuation of current and future SDTF liabilities and payments in accordance with Section 440.49, Florida Statutes, as well as other applicable Federal and State laws. SDTF reimbursement payments submitted for processing to BF&SS by the SDTF Office during the 2010-11 fiscal year totaled approximately $74.18 million. Additionally, the SDTF System contains significant confidential information, including injured workers' names, dates of birth, social security numbers, and medical notes. Accordingly, effective IT controls over the SDTF System and its related IT resources are critical. Our audit disclosed instances where IT controls applicable to the SDTF System and database needed improvement as discussed in the following paragraphs.

Security Controls

Finding No. 1: Access Privileges and Separation of Duties

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) Rules 71A-1.007(3), 71A-1.002(47), and 71A-1.002(55), Florida Administrative Code, provide that workers, including employees and other individuals 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. Accordingly, an agency should take steps to ensure that incompatible combinations of functions cannot be performed by a single system user.

Our review of the 17 SDTF System users in one or more groups that had update access privileges to the SDTF System disclosed that some users had update access privileges that were not necessary for their job responsibilities and did not enforce an appropriate separation of duties. These conditions, as described below, increase the risk of errors, fraud, misuse, or other unauthorized modification of Department data.

- One user was assigned an incompatible combination of job duties and related access privileges that included entering reimbursement requests; preparing and submitting payment requests; and reviewing, posting, and mailing the related SDTF payments. In addition, this user performed the complete SDTF payment correction process with no management review. This user also had excessive update access privileges that were unnecessary to accomplish her assigned job duties.
- Three users who performed supervisory review functions had incompatible update access privileges to the SDTF System that were unnecessary for their assigned job duties and did not enforce an appropriate separation of duties.
- Seven users had update access privileges to certain fields on the SDTF System claim proof and reimbursement request screens that were unnecessary for their assigned job duties and did not enforce an appropriate separation of duties.

The excessive update access privileges resulted, in part, from the SDTF System lacking the functionality to assign inquiry-only access privileges to users who needed to view, but not update, SDTF System data. Consequently, SDTF System users with access privileges to an SDTF System screen had the ability to update all available fields on the screen.

Recommendation: The Department should limit access privileges to SDTF System resources to only those necessary to perform assigned job duties. The Department should also evaluate employee job responsibilities relating to the SDTF System and make applicable changes to enforce an appropriate separation of incompatible duties. Until an appropriate separation of incompatible duties can be established, the Department should implement effective compensating controls such as increased supervision and monitoring of users with incompatible duties and excessive access privileges.

Finding No. 2: Periodic Review of Access Privileges

Periodic review of user access privileges helps ensure that user access privileges remain appropriate. Department Administrative Policies and Procedures (AP&P) 4-05, *Application Access Control (AP&P 4-05)* requires an annual access control inspection by the Division of Information Systems (DIS) Compliance Office and quarterly business unit level reviews of application access privileges by the application owner with the results provided to the DIS Compliance Office. AEIT Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights periodically based on risk, access account change activity, and error rate.

Our audit disclosed that the annual access control inspection of SDTF System IT resource access privileges required by *AP&P 4-05* had not been performed and the quarterly business unit level reviews had only been performed annually. The lack of periodic reviews of access privileges increases the risk that inappropriate access privileges may not be timely detected or remediated.

Recommendation: The Department should comply with the provisions of *AP&P 4-05* regarding periodic reviews of access privileges for all SDTF System-related IT resources.

Finding No. 3: Protection of Confidential and Exempt SDTF Information

Confidentiality controls provide reasonable assurance that application data, reports, and other outputs are protected against unauthorized disclosure. Section 119.071(5)(a)5., Florida Statutes, provides that social security numbers held by an agency are confidential and exempt from public disclosure. Section 440.125, Florida Statutes, provides that any medical records and medical reports of an injured employee and any information identifying an injured employee in medical bills which are provided to the Department are confidential and exempt from public disclosure. In addition, Section 624.23(2), Florida Statutes, provides that personal financial and health information held by the Department relating to a consumer's complaint or inquiry regarding a matter or activity regulated under the Florida Insurance Code are confidential and exempt from public disclosure.

AEIT Rule 71A-1.006(1), Florida Administrative Code, provides, in part, that each agency shall exercise due diligence to protect confidential and exempt information by using appropriate administrative, technical, and physical controls and AEIT Rule 71A-1.018, Florida Administrative Code, provides that production confidential and exempt information shall not be used in the development (test) environment. Also, *AP&P 4-05* provides that access privileges to applications should be limited to individuals authorized to view, process, or maintain particular systems.

The SDTF System and related IT resources contained confidential and exempt information such as injured workers' names, dates of birth, social security numbers, medical, and financial information. Our audit disclosed that SDTF confidential and exempt injured workers' information was accessible by individuals who did not have a valid business purpose to access the information. These conditions, described in the following paragraphs, increased the risk of unauthorized disclosure of confidential and exempt information.

SDTF System Shared Folders

SDTF System injured workers' information, including confidential and exempt information such as injured workers' names, dates of birth, and social security numbers, was stored in two SDTF System shared folders. These folders were accessible not only to SDTF Office employees who had a valid business purpose to access this information, but also to individuals who were members of a Departmentwide access group. Approximately 3,000 members of the Departmentwide access group did not have a valid business purpose for the access privileges to the SDTF System shared folders. In response to audit inquiry, the access privileges were modified to remove the Departmentwide access group in November 2011.

SDTF System Test Environment

The Department used data from the SDTF System production database, including confidential and exempt information such as injured workers' names, dates of birth, social security numbers, and medical notes, to populate the SDTF System test database. By using production data to populate the test database, the Department inadvertently rendered confidential and exempt information accessible to Division and DIS employees who did not need the information for their assigned job duties.

Recommendation: The Department should improve controls protecting the confidentiality of SDTF confidential and exempt information by limiting access to only those individuals with a valid business purpose for accessing the information.

Finding No. 4: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain security controls relating to access privileges, default local administrator accounts, and local server security event logging for the SDTF System that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Department management and staff of the specific issues. Without adequate security controls related to access privileges, default local administrator accounts, and local server event logging, the risk is increased that the confidentiality, integrity, and availability of data and IT resources may be compromised.

Recommendation: The Department should improve its security controls relating to access privileges, default local administrator accounts, and local server security event logging to ensure the continued confidentiality, integrity, and availability of data and IT resources.

Other General Controls

Finding No. 5: SDTF System Backups

AEIT Rule 71A-1.012(1), Florida Administrative Code, provides that data that is essential to the continued operation of critical functions shall be mirrored to an off-site location or backed up regularly with a current copy stored at an off-site location. The Department backed up the SDTF System database on a regular basis but stored the backup copies on-site. Contrary to AEIT Rule, database backup copies were stored off-site only twice a year on June 30th and December 31st, rather than whenever the database was backed up. Under these conditions, the risk was increased that, in the event of a disaster at the Department's processing site, the Department would be unable to restore current information to the SDTF System database.

Recommendation: The Department should enhance procedures to ensure that a current copy of the SDTF System database is stored in a secure, off-site location.

Application Controls

Finding No. 6: SDTF System Input, Processing, and User Controls

Application controls include automated (application input, processing, and output) and manual (user) controls that are used to ensure the completeness and accuracy of system data. Effective input controls ensure that only correct data is entered and accepted by the system. These controls ensure input errors are recognized and that appropriate corrections are made in a manner that ensures the correction is verified, authorized, and reentered as part of normal processing and does not compromise the original transaction's authorization levels. Additionally, effective processing controls ensure that data located in a file or database remains complete and accurate and is only changed as a result of authorized processing or modification routines. User controls are manual processes performed by individuals interacting with information systems that, when combined with other application controls, help ensure data accuracy and completeness, thus achieving data integrity and reliability.

As previously discussed, claim reimbursement requests are submitted to the SDTF Office on behalf of insurance carriers or employers. The requests are entered into the SDTF System by the SDTF Office. Our audit disclosed

discrepancies in SDTF System data and SDTF System input, processing, and related user controls that needed improvement, as discussed in the following paragraphs.

SDTF System data did not always match the data on the claim reimbursement requests. We selected a sample of 47 of the 5,260 claim reimbursement requests for the period July 1, 2008, through September 30, 2011, that the SDTF Office had approved and submitted to BF&SS for payment processing. For the claim reimbursement requests included in our sample, we reviewed the related claim information provided to the SDTF Office to determine if the SDTF Office had accurately input the claim information into the SDTF System. Our review disclosed that, for 11 of the 47 claim reimbursement requests included in our sample, the data provided for input did not match the actual data input into the SDTF System. Specifically, a total of 16 data items from the 11 requests, including 1 payee's Federal identification number, 9 payees' Payable To name and address information, and 6 payees' or representatives' Mail To name and address information provided to the SDTF Office on claim reimbursement request forms, did not match the related information on the reimbursement request screens in the SDTF System.

Our review of the 5,260 SDTF claim reimbursement requests submitted to BF&SS for payment and the related FLAIR claim payments that were made during the period July 1, 2008, through September 30, 2011, disclosed 49 claim warrant payment transactions in which the SDTF vendor identification codes (IDs) did not match the related FLAIR vendor numbers, excluding differences resulting from vendor location changes. Department staff had corrected 46 of the SDTF vendor IDs as of October 25, 2011, prior to our review, and the remaining 3 SDTF vendor IDs were corrected on November 17, 2011, in response to audit inquiry.

SDTF payee information used to populate payment request batches submitted to BF&SS was not subject to review. Although the payee information on the reimbursement request screen was reviewed during request processing, the payee information that was exported to payment request batches was from another system table that was not subject to the review process. Additionally, SDTF Office procedures only required the review of the payee vendor number for the first claim reimbursement request for that vendor. The lack of sufficient review of SDTF payee information may have resulted in claim reimbursement requests being submitted to BF&SS for payment with inaccurate payee vendor numbers.

The payment correction process did not enforce established unique invoice numbering and review controls. When paid invoices were subsequently discovered by the SDTF Office or payee to contain errors, such as amount and payee errors, the SDTF Office made corrections by manually adding a payment to the payment request batch or by submitting a correction memorandum to BF&SS and making adjustments to the data in the SDTF System. Error corrections included voiding a payment, voiding and re-issuing a corrected payment, or making an additional payment. All correction payments were assigned the same invoice number as the original payment, resulting in each payment not having a unique invoice number. As previously discussed in Finding No. 1, a single user performed the complete payment correction process, independent of the SDTF System and the established review process.

Additionally, except for a limited number of fields, the data input fields in the SDTF System were not restricted from further update once claim data had been entered. Most data fields could be modified at any time by anyone with access privileges to the screens, and the modifications were not subject to independent review or approval. There was no mechanism in place to lock the fields and only allow data modifications with an appropriate system-required supervisory override.

As indicated by the data discrepancies described above, deficient SDTF System input, processing, and user controls increase the risk that erroneous, incomplete, or unauthorized modifications, should they occur, may not be timely detected.

Recommendation: The Department should implement appropriate input, processing, and user controls to enhance the integrity of the SDTF System data. Specifically, the Department should ensure that SDTF System data accurately reflects the claim data provided for input; payee vendor information submitted to BF&SS for payment is reviewed for accuracy; data error corrections do not circumvent the unique invoice numbering and review controls; and error corrections are subject to the same controls as the original transaction. In addition, after data has been entered, the claim data fields within the SDTF System should not be updatable without a supervisory override and review process.

Finding No. 7: Reconciliation of SDTF System and FLAIR Claim Payment Data

Interface controls consist of those controls over the timely, accurate, and complete processing of information that is exchanged 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. Such procedures typically include batch totals, reconciliations, and control totals.

Claim reimbursement requests reviewed and approved for payment by the SDTF Office are system selected for payment. Once a system-selected payment request batch is reviewed and approved by the SDTF Office, it is saved as a spreadsheet and e-mailed to BF&SS for payment processing. After the SDTF payments are processed in FLAIR, the resulting warrants and other payment information are delivered to the SDTF Office to be scanned, entered into the SDTF system, and mailed.

Our review of the 5,260 SDTF claim reimbursement requests submitted to BF&SS for payment and the related FLAIR claim payments that were made during the period July 1, 2008, through September 30, 2011, disclosed one SDTF duplicate payment in the amount of $28,744 paid in November 2009. The duplicate claim payment was the result of miscommunication between the SDTF Office and BF&SS staff. The duplicate payment had not been detected or corrected by the SDTF Office at the time of our review and the Department had not performed a reconciliation of the two systems. In response to audit inquiry, SDTF management requested and received a refund of the payment in September 2011.

Without an effective method to reconcile SDTF System claim payment data to the related FLAIR claim payment data, the risk is increased that SDTF System claim payments may not be processed or may be processed incorrectly or that duplicate payment errors could occur and not be detected or corrected timely.

Recommendation: The Department should implement the necessary reconciliation controls to ensure that SDTF claim payment data exchanged between the SDTF System and FLAIR is complete, valid, and accurate and that SDTF System claim payment requests are only submitted once for payment.

Finding No. 8: Monitoring of SDTF System Activity

Effective security controls include the logging and monitoring of significant system activity, including access to and modification of sensitive or critical system resources. For monitoring to be effective, managers should regularly review system logs for unusual or suspicious activity and take appropriate action. Supervision and review of personnel activities, reports, and queries help ensure that system activities are performed in accordance with prescribed procedures, errors are timely detected and corrected, and IT resources are only used for authorized purposes.

Our review of SDTF Office procedures disclosed that the SDTF Office had implemented history and event logs, reports, and database queries as tools to assist SDTF management, as needed, in the supervisory review processes; however, the logs and reports were not being routinely monitored by SDTF Office staff. The lack of monitoring increases the risk that system activity may not be performed in accordance with SDTF Office procedures and that erroneous or unauthorized transactions, should they occur, may not be timely detected.

Recommendation: The Department should ensure that SDTF System logs and reports are routinely monitored by SDTF Office staff for erroneous or unauthorized system activity.

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 during the period September 2011 through January 2012 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 the SDTF Claims Manager 2004 System in achieving management's control objectives 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 the SDTF System. The audit included selected general IT controls over system modification and backups; logical access to programs, data, and database files; and physical access. The audit also included selected application IT controls and selected user controls relevant to the SDTF System. Our audit included examinations of various Department records and transactions (as well as events and conditions) occurring from September 2011 through January 2012 and selected Department transactions from July 2008.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the SDTF System including the purpose and goals of the application; the network computing platform, software, user environment, and location of the SDTF System data; the logical access procedures used for granting access privileges to the SDTF System and IT resources; the access paths used to add, modify, or delete SDTF data; and the processes used to retrieve and provide SDTF data used to calculate the fund liability balances that are used on the annual Statewide Financial Statements.
- Observed and documented selected general, application, and user controls, including policies, procedures, hardware, software, organizational structure, and personnel relating to the SDTF System.
- Observed and evaluated the effectiveness of Department procedures for documenting and authorizing user access privileges to the SDTF System. Specifically, we reviewed the access request forms of all Division employees with update access privileges to the SDTF System application or database to determine whether the access authorization forms were on file and whether the access privileges requested matched the employees' current access privileges at the time of testing.

- Observed and tested the appropriateness of the 17 Division employees with user access privileges to the SDTF System application or database through membership into one or more SDTF access groups to determine if the access privileges granted were appropriate and enforced an appropriate separation of incompatible job duties.
- Observed and evaluated the effectiveness of Department logical access control procedures in preventing changes to SDTF data outside the SDTF System application processes.
- Observed and evaluated the effectiveness of selected logical access controls and password settings in ensuring that administrative access privileges to the Department's network, database, and servers were appropriately restricted and enforced an appropriate separation of duties, and that password control settings were effective in adequately protecting the confidentiality of administrator account passwords.
- Observed and tested the adequacy of SDTF System application on-line input edits in promoting data integrity, completeness, and accuracy.
- Observed and evaluated, on a sample basis, the effectiveness of selected application and user controls in promoting SDTF System data integrity. Specifically, we evaluated a sample of 47 claims selected from 5,260 claim reimbursement requests submitted for payment to determine if the input data was accurately reflected in the SDTF System.
- Observed and evaluated the controls surrounding the transfer of data between the SDTF System and FLAIR, including reconciliation procedures.
- Observed and evaluated the effectiveness of physical and logical access controls used to protect SDTF confidential and sensitive data stored in the SDTF System files, application test environment, database, and network shared folders.
- Observed and evaluated Department policies and procedures for timely deactivating SDTF System user access privileges of former and reassigned employees.
- Observed and evaluated Department policies and procedures relating to the SDTF System program change management process.
- Observed and evaluated Department policies and procedures for the backup and storage of SDTF System database information.
- 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 June 12, 2012, 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.

EXHIBIT A
MANAGEMENT'S RESPONSE

CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

June 12, 2012

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 Special Disability Trust Fund Claims Manager 2004 System.*

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

SPECIAL DISABILITY TRUST FUND
CLAIMS MANAGER 2004 SYSTEM
Information Technology Operational Audit

Security Controls

Finding No. 1: Access Privileges and Separation of Duties

The access privileges of some Department users were not necessary for their job responsibilities and did not enforce an appropriate separation of incompatible job duties.

Recommendation: The Department should limit access privileges to SDTF System resources to only those necessary to perform assigned job duties. The Department should also evaluate employee job responsibilities relating to the SDTF System and make applicable changes to enforce an appropriate separation of incompatible duties. Until an appropriate separation of incompatible duties can be established, the Department should implement effective compensating controls such as increased supervision and monitoring of users with incompatible duties and excessive access privileges.

Response:

We concur. Some of the excessive privileges resulted, in part, from the system's limited functionality in the assignment of inquiry-only privileges. Resolution of this issue would require a system program modification. The Division of Workers' Compensation will work to identify potential system modifications to resolve current system limitations. The Division's Office of the Special Disability Trust Fund will also review the job duties and associated access privileges for each staff member and make the changes necessary to minimize incompatible privileges.

Until the appropriate separation of duties can be established, the Division will implement increased supervision and monitoring of users.

Finding No. 2: Periodic Review of Access Privileges

The Department's review of SDTF System IT resource access privileges needed improvement.

Recommendation: The Department should comply with the provisions of *AP&P 4-05* regarding periodic reviews of access privileges for all SDTF System-related IT resources.

Response:

We concur. In September 2011, in accordance with *AP&P 4-05*, the Division of Workers' Compensation began performing quarterly business unit level reviews of Special Disability Trust Fund System access privileges.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

In May 2012, the Department revised *AP&P 4-05* from the requirement to perform an annual review of access control practices for each secure application to an annual requirement to review the access control practices of a sample of secure applications. The Division of Information Systems has implemented procedures to ensure compliance with the revised policy.

Finding No. 3: Protection of Confidential and Exempt SDTF Information

Some confidential and exempt SDTF information was accessible by individuals who did not have a valid business purpose to access the information.

Recommendation: The Department should improve controls protecting the confidentiality of SDTF confidential and exempt information by limiting access to only those individuals with a valid business purpose for accessing the information.

Response:

We concur. In November 2011, the Division of Information Systems restricted access permissions to the Special Disability Trust Fund System Shared Folders to limit access to only those individuals with a valid business purpose.

The Division of Workers' Compensation will work with the Division of Information Systems to identify a solution to resolve control issues with the test environment.

Finding No. 4: Other Security Controls

Certain Department security controls related to access privileges, default local administrator accounts, and local server security event logging needed improvement.

Recommendation: The Department should improve its security controls relating to access privileges, default local administrator accounts, and local server security event logging to ensure the continued confidentiality, integrity, and availability of data and IT resources.

Response:

We concur. The Department has implemented improvements in some areas, and is working to enhance security controls in other areas noted in the report.

Other General Controls

Finding No. 5: SDTF System Backups

SDTF System database backups were not regularly being stored at an off-site location.

Recommendation: The Department should enhance procedures to ensure that a current copy of the SDTF System database is stored in a secure, off-site location.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Response:

We concur. On February 20, 2012, the Division of Information Systems revised backup procedures to ensure that the Special Disabilities Trust Fund System database is backed up on a regular basis and that the back-up copies are stored at a secure off-site location.

Application Controls

Finding No. 6: SDTF System Input, Processing, and User Controls

We noted discrepancies in SDTF System data. Additionally, SDTF System input, processing, and related user controls were deficient.

Recommendation: The Department should implement appropriate input, processing, and user controls to enhance the integrity of the SDTF System data. Specifically, the Department should ensure that SDTF System data accurately reflects the claim data provided for input; payee vendor information submitted to BF&SS for payment is reviewed for accuracy; data error corrections do not circumvent the unique invoice numbering and review controls; and error corrections are subject to the same controls as the original transaction. In addition, after data has been entered, the claim data fields within the SDTF System should not be updatable without a supervisory override and review process.

Response:

We concur. The Department is aware that at times, human error causes some inaccurate information to be entered into the Special Disabilities Trust Fund System, despite redundant supervisory review. The Department will identify and implement additional input, processing, and user controls in an effort to enhance the integrity of system data. Some data input controls have already been implemented and others will be established through an automated Special Disabilities Trust Fund payment process.

Finding No. 7: Reconciliation of SDTF System and FLAIR Claim Payment Data

The Department did not reconcile claim payment data in the SDTF System to the Florida Accounting Information Resource (FLAIR) Subsystem.

Recommendation: The Department should implement the necessary reconciliation controls to ensure that SDTF claim payment data exchanged between the SDTF System and FLAIR is complete, valid, and accurate and that SDTF System claim payment requests are only submitted once for payment.

Response:

We concur. The Division of Workers' Compensation will work with the Division of Information Systems to identify and implement controls to ensure accurate reconciliation of the data exchanged between the Special Disabilities Trust Fund System and FLAIR.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 8: Monitoring of SDTF System Activity

Department monitoring of SDTF System logs and reports needed improvement.

Recommendation: The Department should ensure that SDTF System logs and reports are routinely monitored by SDTF Office staff for erroneous or unauthorized system activity.

Response:

We concur. The Special Disabilities Trust Fund System actively monitors and logs key changes to the database. It is the Division of Workers' Compensation's policy to periodically review the log for identification of erroneous or unauthorized system activity. The Division will establish a review schedule to further ensure routine monitoring.