STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2016-199
June 2016

DEPARTMENT OF FINANCIAL SERVICES

Special Disability Trust Fund
Claims Manager 2004 System

Sherrill F. Norman, CPA
Auditor General

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 team leader was Andrew Denny, CISA, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

www.myflorida.com/audgen

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF FINANCIAL SERVICES

Special Disability Trust Fund Claims Manager 2004 System

SUMMARY

This operational audit of the Department of Financial Services (Department) focused on evaluating selected information technology (IT) controls applicable to the Special Disability Trust Fund (SDTF) Claims Manager 2004 System (SDTF System) and included a follow-up on the findings included in our report No. 2012-179. Our audit disclosed the following:

Finding 1: The Department did not timely deactivate the access privileges for a former employee to prevent the former employee or others from misusing the former employee's access privileges.

Finding 2: Certain security controls related to physical security, confidential and exempt data, and monitoring of the SDTF System and related IT resources continue to need improvement to ensure the confidentiality, integrity, and availability of SDTF System data and related IT resources.

BACKGROUND

The Special Disability Trust Fund (SDTF) was established pursuant to State law[1] for the purpose of encouraging the employment, reemployment, and accommodation of the physically disabled by reducing an employer's insurance premium for reemploying an injured worker, decreasing litigation between carriers on apportionment issues, and protecting employers from excess liability for compensation and medical expense when an injury to a physically disabled worker merges with, aggravates, or accelerates her or his preexisting permanent physical impairment to cause either a greater disability or permanent impairment, or an increase in expenditures for temporary compensation or medical benefits than would have resulted from the injury alone.

The State law[2] establishing the SDTF does not apply to any case in which the accident causing the subsequent injury or death or the disablement or death from a subsequent occupational disease occurred prior to July 1, 1955, or on or after January 1, 1998. While the SDTF is not liable for any case in which the accident causing the subsequent injury or death or the disablement or death from a subsequent occupational disease occurred on or after January 1, 1998, the SDTF continues to reimburse employers or carriers for subsequent injuries that occurred prior to January 1, 1998. As of June 30, 2015, the SDTF fund liability was $887 million and the number of outstanding claims was 4,770.

The Department of Financial Services (Department), Division of Workers' Compensation, Office of SDTF (SDTF Office) is responsible for administering the SDTF. The SDTF Office uses the SDTF Claims Manager 2004 System (SDTF System) for functions related to the SDTF, including the receipt, review, acceptance, and payment of SDTF claims. Monthly, the SDTF Office submits a batch payment file of

[1] Section 440.49(1) and (9)(a), Florida Statutes.

[2] Section 440.49(11), Florida Statutes.

approved claim reimbursement requests to the Florida Accounting Information Resource Subsystem (FLAIR) for payment issuance.

FINDINGS AND RECOMMENDATIONS

Finding 1: Timely Deactivation of Access Privileges

Agency for Enterprise Information Technology (AEIT) rules[3] require that access authorization be promptly removed when a user's employment is terminated or access to the information resource is no longer required. Prompt action is necessary to prevent the former employee or others from misusing the former employee's access privileges.

Our audit procedures disclosed that the Department did not timely deactivate all user accounts for a former employee who performed network administrative functions for the SDTF System. Specifically, we found that, as of January 21, 2016, a user account for a former network administrator remained active for 166 days after the network administrator separated from Department employment. The user account was assigned various administrator and user access privileges that included, among other things, update and read-only access privileges to development and production training databases, respectively. Also, the user account had the capability to connect to the Department's network remotely allowing functions to be performed related to the system administration of the Department's various file management, data exchange, and connectivity systems. Subsequent to our audit inquiry, Department management indicated that the user account access privileges had been deactivated except for access privileges to the Department's automated public records request process. This process required the user account to remain active to generate communication records in support of the process. However, a user that has terminated employment should not retain access privileges.

Without timely deactivation of former employee user accounts, the risk is increased that the user accounts may be misused by former employees or others.

Recommendation: We recommend that Department management ensure that user account access privileges of former employees are timely deactivated.

Finding 2: Security Controls – Physical Security, Confidential and Exempt Data, and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to physical security, confidential and exempt data, and monitoring of the SDTF System and related IT resources continued to need improvement. We are not disclosing specific details of the issues in this report to avoid the

[3] AEIT Rule 71A-1.007(6), Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records, property, administrative authority, and administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, of the AEIT to the AST. The AST adopted Rules 74-2.001 through 74-2.006, Florida Administrative Code, effective March 16, 2016, establishing the Florida Cybersecurity Standards. On June 5, 2016, Chapters 71A-1 and 71A-2, Florida Administrative Code, were repealed.

possibility of compromising SDTF System data and related IT resources. However, we have notified appropriate Department management of the specific issues.

Without appropriate security controls related to physical security, confidential and exempt data, and monitoring of the SDTF System and related IT resources, the risk is increased that the confidentiality, integrity, and availability of SDTF System data and related IT resources may be compromised. Similar issues were communicated to Department management in connection with our report No. 2012-179.

Recommendation: We recommend that Department management improve certain security controls related to physical security, confidential and exempt data, and monitoring of the SDTF System and related IT resources to ensure the confidentiality, integrity, and availability of SDTF System data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2012-179.

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 November 2015 through January 2016 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to the SDTF System during the period July 2015 through January 2016 and selected actions subsequent thereto. The audit included selected business process application controls over transaction data input, processing, and output applicable to the SDTF System that related to the deficiencies disclosed in our report No. 2012-179. The audit also included selected system-level and application-level general controls applicable to access controls and backup and recovery controls that related to the deficiencies disclosed in our report No. 2012-179. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls 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.
- To determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2012-179.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the SDTF System data and business process flows, including key sources of data input and interfaces; key application transactions and processes; and key types of application data output.
- Evaluated the effectiveness of selected transaction data input, processing, and output controls related to the SDTF System for ensuring the completeness, accuracy, validity, and confidentiality of SDTF data. Specifically, we reviewed:
    - Forty of 477 SDTF claim reimbursement requests submitted to the SDTF Office for processing during the period July 1, 2015, through December 9, 2015, to determine whether source documentation reconciled with SDTF System data.
    - Forty of 498 SDTF approved claim reimbursement requests submitted for payment issuance through FLAIR that were paid during the period July 1, 2015, through November 30, 2015, to determine whether SDTF System data reconciled with FLAIR data.
- Obtained an understanding of the IT computing platform for the SDTF System, including identification of the applicable hardware, operating system and version, database management system and version, and security software and version related to the SDTF System.
- Obtained an understanding of the account management processes for authorizing, creating, modifying, and revoking SDTF System accounts.

- Obtained an understanding of the process for periodically reviewing SDTF System access appropriateness.
- Evaluated the effectiveness of selected access controls related to the appropriateness of access privileges granted to selected SDTF System processes for selected employees' user accounts. Specifically, we reviewed 12 SDTF System processes with update access privileges associated with 20 employees as of December 16, 2015, to determine whether access privileges granted to the SDTF System processes were appropriate.
- Evaluated the effectiveness of selected access privileges related to sensitive IT resources associated with the SDTF System and performed additional procedures related to various user accounts of a former employee.
- Evaluated the effectiveness of selected controls applicable to the storage of sensitive SDTF System data and the physical SDTF System claim files.
- Evaluated the effectiveness of selected logging and monitoring controls related to the SDTF System.
- Evaluated the effectiveness of selected off-site backup controls related to the SDTF System.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. 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.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

June 9, 2016

Sherrill F. Norman
Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

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 Teresa Michael, Inspector General, at (850) 413-4960.

Sincerely,

Jeff Atwater FOR

JA:rlg

Enclosure

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

DEPARTMENT OF FINANCIAL SERVICES
SPECIAL DISABILITY TRUST FUND
CLAIMS MANAGER 2004 SYSTEM

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Timely Deactivation of Access Privileges

The Department did not timely deactivate the access privileges for a former employee to prevent the former employee or others from misusing the former employee's access privileges.

Recommendation: We recommend that Department management ensure that user account access privileges of former employees are timely deactivated.

Response: We concur. The Department has many effective processes in place to ensure timely termination of former employee accounts. The two accounts identified were an anomaly to these processes as the corresponding accesses required transition to new staff and others are tied to existing business processes preventing one of the accounts from being fully deactivated. The Department has restricted the functionality of the one remaining account to the extent possible without limiting our ability to comply with public records request requirements. Access to the account is appropriately restricted to designated staff who are authorized to perform these functions. The account will be required for this purpose until the Department procures and transitions all related records to another resource.

Expected Completion Date for Corrective Action: August 2017

Finding No. 2: Security Controls – Physical Security, Confidential and Exempt Data, and Monitoring

Certain security controls related to physical security, confidential and exempt data, and monitoring of the SDTF System and related IT resources continue to need improvement to ensure the confidentiality, integrity, and availability of SDTF System data and related IT resources.

Recommendation: We recommend that Department management improve certain security controls related to physical security, confidential and exempt data, and monitoring of the SDTF System and related IT resources to ensure the confidentiality, integrity, and availability of SDTF System data and related IT resources.

Response: We concur. The Department had made significant improvement in restricting physical security by building a restricted area. The physical security matter identified was resolved as of February 4, 2016. The additional business process concerns will be evaluated and, where appropriate, additional security controls will be implemented to further enhance security of system data and related resources.

Expected Completion Date for Corrective Action: March 2017