REPORT NO. 2015-181
APRIL 2015

DEPARTMENT OF FINANCIAL SERVICES

AUTOMATED INVESTIGATION MANAGEMENT SYSTEM (AIM)

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 Earl M. Butler, CISA, CFE, 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 can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF FINANCIAL SERVICES

Automated Investigation Management System (AIM)

SUMMARY

The mission of the Department of Financial Services (Department), Division of Public Assistance Fraud (Division) is to investigate fraud and abuse in State-administered public assistance programs. Section 414.411(1), Florida Statutes, provides the Department authority to conduct these investigations. The Division partners with several entities on the State and Federal levels to carry out its mission. The Division investigates fraud committed by recipients, employees administering the programs, and merchants or contractors. Division staff in field offices throughout the State utilize AIM to receive, track, and review referrals; store case background information; and assign and document investigations.

Our operational audit focused on evaluating selected information technology (IT) controls applicable to AIM. We also determined the status of corrective actions regarding audit findings included in our report No. 2014-103 that were applicable to the scope of this audit.

Our audit disclosed areas in which improvements in AIM IT controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: Some user access privileges to AIM data and related IT resources were not limited to only what was necessary in the performance of assigned job duties and did not promote an appropriate separation of duties or provide for individual accountability.

Finding No. 2: The Department had not conducted periodic reviews of the appropriateness of access privileges granted to AIM users.

Finding No. 3: Certain security controls related to user authentication, logging, and review for AIM and related IT resources needed improvement.

BACKGROUND

The State provides to eligible individuals and families various types of public assistance including food, prescription drugs, medical care, childcare, and cash assistance. Pursuant to Section 414.411(1), Florida Statutes, the Department of Financial Services (Department) shall investigate all public assistance provided to residents of the State or provided to others by the State. To perform the Department's duties, the Division of Public Assistance Fraud (Division) within the Department has access to a variety of data, including birth, employment, incarceration, and death records. Division staff utilize the Automated Investigation Management System (AIM) to receive, track, and review referrals; store case background information; and assign and document investigations. AIM electronically uploads referrals from systems maintained by various entities, such as the Department of Children and Families and the Department of Education, on a periodic basis, while Division staff manually enter referrals from other sources.

In connection with its statutorily assigned responsibilities for investigating public assistance fraud in Florida, the Division, as the designated State Law Enforcement Bureau (SLEB) for Supplemental Nutrition Assistance Program (SNAP) Electronic Benefits Transfer (EBT) card investigations, entered into an agreement with the United States Department of Agriculture Food and Nutrition Service. As the SLEB, the Division is responsible for maintaining secure controls over EBT cards used in investigations and is authorized to create, fund, issue, and control the use of EBT cards in investigations of potential SNAP fraud.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to only what is necessary in the performance of assigned job duties, promote an appropriate separation of duties, and provide for individual accountability. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, or destruction. Our audit disclosed that some inappropriate and unnecessary access privileges existed to the production AIM application, the production file transfer protocol (FTP) server, and the production public assistance fraud (PAF) File Exchange server. Specifically:

AIM Application

Our review of AIM access privileges disclosed that programming staff shared a test account that had access privileges to the production environment of AIM. Anyone with knowledge of the test account password had the capability to log on to AIM and inappropriately view the AIM data. Additionally, the use of the shared test account provided no method to enforce individual accountability.

FTP Server

Our review of the adequacy of the control of confidential data during transaction processing disclosed that programming staff were sharing an account with access privileges to the production FTP server to move entity files to the production PAF File Exchange server. This shared account resulted in inappropriate access to entity AIM data by programming staff that was contrary to an appropriate separation of duties. Furthermore, the use of the shared account provided no method to enforce individual accountability.

PAF File Exchange Server

Our review of the adequacy of the control of confidential data during transaction processing disclosed that programming staff had operating system accounts on the production PAF File Exchange server that provided read, write, and execute access privileges to certain production files that were unnecessary for their assigned job duties and were contrary to an appropriate separation of duties.

Inappropriate or unnecessary access to AIM data and related IT resources and the lack of individual accountability when accessing AIM data and related IT resources increase the risk of unauthorized disclosure, modification, or destruction of AIM data and related IT resources.

Recommendation: The Department should limit user access to AIM data and related IT resources to only access privileges that are necessary to perform assigned job duties, promote an appropriate separation of duties, and provide for individual accountability.

Finding No. 2: Periodic Review of Access Privileges

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights (privileges) periodically based on risk, access account change

[1] Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; pending issues and existing contracts; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, in effect as of November 15, 2010; trust funds; and unexpended balances of appropriations, allocations, and other funds of the AEIT to the AST.

activity, and error rate. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

Department *Administrative Policies and Procedures 4-05, Application Access Control Policy* (*AP&P 4-05*) requires business unit level reviews of application access privileges to be conducted quarterly at a minimum to ensure that the access privileges of users are consistent with the roles and responsibilities the users require in order to perform their assigned duties.

Our audit disclosed that, contrary to *AP&P 4-05*, the Department had not conducted periodic reviews of the appropriateness of access privileges granted to AIM users. The lack of periodic reviews of the appropriateness of access privileges granted to AIM users increases the risk that excessive or inappropriate access privileges may exist and not be timely detected or corrected.

Recommendation: The Department should ensure that reviews of the appropriateness of access privileges granted to AIM users are conducted as required by *AP&P 4-05* to ensure the continued appropriateness of user access privileges.

Finding No. 3: 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 related to user authentication, logging, and review for AIM and related IT resources that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising AIM data and related IT resources. However, we have notified appropriate Department management of the specific issues.

Without adequate security controls related to user authentication, logging, and review, the risk is increased that the confidentiality, integrity, and availability of AIM data and related IT resources may be compromised.

Recommendation: The Department should implement appropriate security controls related to user authentication, logging, and review to ensure the continued confidentiality, integrity, and availability of AIM data and related IT resources.

PRIOR AUDIT FOLLOW-UP

The Department had corrected one finding and partially corrected two findings included in our report No. 2014-103 that were applicable to the scope of this audit. The remaining three findings in our report No. 2014-103 were not applicable to the scope of this audit.

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 October 2014 through January 2015 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 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. An additional objective was to determine whether the Department had corrected, or was in the process of correcting, deficiencies disclosed in audit report No. 2014-103 that were applicable to the scope of this audit.

The scope of our audit focused on evaluating selected business process application controls over transaction data input, processing, and output applicable to AIM during the period July 2014 through January 2015 and selected actions through February 27, 2015. The audit also included selected application-level general controls over logical access to programs and data and configuration management.

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 the audit, the 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 our 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 our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our 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 our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the Department's IT computing platforms for the application, the procedures for security administration, and configuration management processes.
- Obtained an understanding of the data and business process flows for the application, the key sources of data input, key application transactions and processing, and key types of application data output related to the application.
- Evaluated the effectiveness of selected logical access controls including periodic reviews for AIM to ensure that user access privileges were authorized and appropriate. Specifically, we reviewed user access privileges as

of November 20, 2014, for 21 of 71 AIM user accounts to determine if the access privileges granted were authorized and appropriate.

- Reviewed and evaluated the adequacy of controls that protect the Department's sensitive system resources, including the adequacy of logging of system actions and the review and monitoring of system events.
- Reviewed and evaluated the effectiveness of selected user authentication controls. Specifically, we reviewed Department policies and other documentation regarding authentication settings. In addition, we reviewed authentication settings to determine if the settings were sufficient to appropriately restrict access.
- Evaluated the effectiveness of configuration management controls over AIM. Specifically, we reviewed 10 programs change requests that were moved into the production environment between July 1, 2014, and October 15, 2014, to determine whether selected AIM modifications were suitably requested, approved by IT management, user acceptance tested, and implemented.
- Evaluated the Department's data input, processing, and output controls that ensure the completeness, accuracy, validity, and confidentiality of AIM data, including transaction data processing related to the production FTP server and the production PAF File Exchange server.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing 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 those matters requiring corrective action.

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 April 10, 2015, 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

April 10, 2015

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

Dear Mr. Martin:

Pursuant to Section 11.45(3)(b), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's information technology (IT) operational audit of the Department of Financial Services, Automated Investigation Management System (AIMS).

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

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
AUTOMATED INVESTIGATION MANAGEMENT SYSTEM (AIM)
Information Technology Operational Audit

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Appropriateness of Access Privileges

Some user access privileges to AIM data and related IT resources were not limited to only what was necessary in the performance of assigned job duties and did not promote an appropriate separation of duties or provide for individual accountability.

Recommendation: The Department should limit user access to AIM data and related IT resources to only access privileges that are necessary to perform assigned job duties, promote an appropriate separation of duties, and provide for individual accountability.

Response: Concur. The Department will evaluate existing access and restrict it as appropriate to ensure separation of duties and accountability.

Expected Completion Date for Corrective Action: Ongoing

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
AUTOMATED INVESTIGATION MANAGEMENT SYSTEM (AIM)
Information Technology Operational Audit

Finding No. 2: Periodic Review of Access Privileges

The Department had not conducted periodic reviews of the appropriateness of access privileges granted to AIM users.

Recommendation: The Department should ensure that reviews of the appropriateness of access privileges granted to AIM users are conducted as required by AP&P 4-05 to ensure the continued appropriateness of user access privileges.

Response: Concur. Reviews of the appropriateness of access granted to AIM users will be conducted monthly and documented.

Expected Completion Date for Corrective Action: March 31, 2015

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
AUTOMATED INVESTIGATION MANAGEMENT SYSTEM (AIM)
Information Technology Operational Audit

Finding No. 3: Other Security Controls

Certain security controls related to user authentication, logging, and review for AIM and related IT resources needed improvement.

Recommendation: The Department should implement appropriate security controls related to user authentication, logging, and review to ensure the continued confidentiality, integrity, and availability of AIM data and related IT resources.

Response: The Department will continue to address security controls, as appropriate.

Expected Completion Date for Corrective Action: To be determined