REPORT NO. 2014-109
FEBRUARY 2014

DEPARTMENT OF FINANCIAL SERVICES

UNCLAIMED PROPERTY MANAGEMENT INFORMATION SYSTEM (UPMIS)

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 William Tuck, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Art 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

Unclaimed Property Management Information System (UPMIS)

SUMMARY

Pursuant to Section 717.102(1), Florida Statutes, all intangible property that is held, issued, or owing in the ordinary course of the holder's business and has remained unclaimed by the owner for more than five years after the property becomes payable or distributable, is presumed to be unclaimed property. Section 717.103, Florida Statutes, provides that intangible property is subject to the custody of the Department of Financial Services (Department) as unclaimed property if the conditions leading to a presumption that the property is unclaimed are satisfied and, among other things, if the last known address (as shown on the records of the holder) of the apparent owner is in this State. Chapter 717, Florida Statutes, gives the Department specific responsibilities with regard to locating apparent owners of unclaimed property, safeguarding unclaimed property, disposing of unclaimed property, depositing of funds and proceeds from the sale of unclaimed property, and making determinations of claims to unclaimed property. The Department utilizes the Unclaimed Property Management Information System (UPMIS) to support the functions required to provide unclaimed property services.

Our operational audit focused on evaluating selected information technology (IT) controls applicable to UPMIS. We also determined the status of corrective actions regarding audit findings included in our report No. 2007-186. Our audit disclosed areas in which enhancements in IT controls were needed. The results of our audit are summarized below:

Finding No. 1: The Department's reviewing and monitoring of program change requests needed improvement.

Finding No. 2: The Division of Accounting and Auditing, Bureau of Unclaimed Property did not have procedures to ensure that background checks were performed on employees selected to assist in the annual unclaimed property inventory process.

Finding No. 3: As similarly noted in our report No. 2007-186, improvements were needed in the Department's procedures for deactivating access privileges to the database used for UPMIS data.

Finding No. 4: Certain security controls related to user authentication needed improvement.

Finding No. 5: Access privileges of selected UPMIS IT programming staff were not appropriate for their job duties.

BACKGROUND

Within the Department, the Bureau of Unclaimed Property utilizes UPMIS to manage the collection and distribution of unclaimed property. Unclaimed property is a financial asset that has been left inactive by its owner. The most common types of unclaimed property are dormant bank accounts, undelivered insurance proceeds, stocks, dividends, uncashed payroll checks, and refunds. The Department also receives contents of safe deposit boxes from financial institutions. These unclaimed assets are held by the reporting entity ("holder") for a set period of time. If the holder is unable to locate the owner and reestablish contact, then the asset is delivered to the Department as unclaimed property. Currently, the Department holds unclaimed property accounts valued at over $1 billion. The Bureau of Unclaimed Property uses various methods in its attempt to notify apparent owners of the location of their unclaimed property, including searching credit bureau records; driver's license searches; advertising on radio and television programs; and participating in home shows, State fairs, and other community events.

UPMIS was designed to collect, compile, and report unclaimed property data in Florida. UPMIS contains a searchable database, accessible from the Department's Unclaimed Property Web site – www.fltreasurehunt.org. This database contains approximately 5.8 million claimable accounts of unclaimed property valued at $25 and higher.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Reviewing and Monitoring of Program Change Requests

Effective program change controls include procedures to review and monitor program change requests in a timely manner to ensure systems function as intended by management. The Division of Information Systems has established policies and procedures for the management of program change requests that sets forth the responsibilities and procedures to plan, prioritize, and assess the risk, impact, and benefit of program changes. However, we reviewed a report of outstanding program change requests for UPMIS as of October 7, 2013, and found that there were 374 UPMIS change requests dating as far back as July 16, 2012, of which 342 were still in a planning status. Through our inquiry, we determined that the Department had not implemented a procedure to review and monitor aging program change requests based on available resources.

The Department's lack of review and monitoring of aging program change requests increases the risk that necessary change requests may not be implemented in a timely manner to ensure that the system functions as intended by management.

Recommendation: The Department should establish a procedure for reviewing and monitoring aging program change requests based on available resources to ensure the system functions as intended by management.

Follow-Up to Management's Response

In written response to Finding No. 1, the Department indicated that it has policies and procedures regarding management-level monitoring of IT service requests and program change request processes. Although the policies and procedures address the initial submission, assignment, and processes for program change requests through their completion, the point of our finding was that the Department had not implemented effective processes for the periodic review of aging program change requests to ensure their timely and appropriate resolution as evidenced by the number of pending program change requests.

Finding No. 2: Background Checks for Unclaimed Property Inventory

Effective security controls include the performance of security background checks for new employees and the periodic reperformance of security background checks for existing employees who are in sensitive or special trust positions. The Bureau of Unclaimed Property requires security background checks on its employees. However, when performing the annual unclaimed property inventory process, employees were selected from other organizational areas outside of the Bureau of Unclaimed Property but within the Division of Accounting and Auditing to assist Bureau of Unclaimed Property employees in the inventory process. Through our inquiry, we determined that the Department had not performed background checks on some of the employees outside the Bureau of Unclaimed Property who participated in the annual unclaimed property inventory process. As a result, the risk is increased that the unclaimed property inventory could be compromised by employees who did not meet security background check criteria normally required by the Bureau of Unclaimed Property.

Recommendation: The Department should ensure background checks have been completed for all employees assisting with the annual unclaimed property inventory process.

Finding No. 3: Deactivating Access Privileges

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(6), Florida Administrative Code, provides that access authorization shall be promptly removed when a user's employment is terminated or access to the information is no longer required. Prompt action is necessary to ensure that a former employee, contractor, or others do not misuse the former employee's or contractor's access privileges.

Users needing access to UPMIS must have a user identification code (ID) that authenticates the user to UPMIS. Additionally, the same user ID is used to authenticate, through UPMIS, to the UPMIS database.

As similarly noted in our report No. 2007-186, we noted that access privileges to UPMIS are appropriately deactivated when an employee or contractor terminates or transfers from the Department. However, through our review, we determined that when access privileges were deactivated from UPMIS, the access privileges to the UPMIS database were not deactivated. Furthermore, if an UPMIS user ID is reactivated for a new user, the new user could inherit inappropriate access privileges to the UPMIS database previously assigned to the former user of that user ID. Allowing access privileges to remain active in the UPMIS database when corresponding access privileges to UPMIS have been deactivated increases the risk of unauthorized or erroneous changes to data.

Recommendation: The Department should ensure that access privileges to the UPMIS database are appropriately deactivated when corresponding access privileges to UPMIS are deactivated.

Finding No. 4: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. As similarly communicated to the Department in connection with our report No. 2007-186, our audit disclosed certain Department security controls related to user authentication 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, the risk is increased that the confidentiality, integrity, and availability of Department data and IT resources may be compromised.

Recommendation: The Department should improve user authentication controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Finding No. 5: 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 responsibilities and promote an appropriate separation of job duties. Appropriately

[1] During the 2012 Legislative Session, HB 5011 that abolished AEIT and reassigned the functions and duties of AEIT to a new State agency was passed by the Legislature and presented to the Governor for signature. The bill was vetoed by the Governor on April 20, 2012. However, AEIT underwent defacto dissolution as the 2012 General Appropriations Act made no appropriations for the funding of positions in AEIT. As of the completion of our audit, rulemaking authority and responsibility for promoting or enforcing compliance with existing AEIT rules had not been established.

restricted access privileges help protect data and IT resources from unauthorized and erroneous disclosure, modification, and destruction.

We determined that two members (one employee and one contractor) of the UPMIS IT programming staff had access to UPMIS that was inappropriate for their job duties. This access provided both members with inappropriate managerial update capabilities to UPMIS data in addition to the access to UPMIS programming code needed to perform their job duties.

UPMIS IT programming staff having inappropriate access to UPMIS managerial functions in addition to access to UPMIS programming code increases the risk of unauthorized or erroneous disclosure, modification, and destruction of UPMIS data being made without timely detection. In response to our inquiry, Department staff subsequently removed the inappropriate UPMIS access of both members.

Recommendation: The Department should continue to ensure that access to UPMIS is appropriate.

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. 2007-186.

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 August 2013 through November 2013 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 the extent to which the Department had corrected, or was in the process of correcting, deficiencies disclosed in audit report No. 2007-186.

The scope of our audit focused on evaluating selected IT controls applicable to UPMIS during the period July 2013 through October 2013. The audit included selected general IT controls over systems development and modification; systems software and the database; logical access to programs and data; selected application IT controls; and selected input, processing, and output controls relevant to UPMIS.

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 and IT controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective IT operational policies, procedures, or practices. The focus of this IT operational 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 vendors 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 UPMIS environment, including the computing platform and related software; the access paths by which UPMIS data can be viewed, modified, or deleted; the program change management process applicable to UPMIS, and the physical security controls over the unclaimed property vault and mailroom.
- Obtained an understanding of selected general, application, and user controls; the process flow within UPMIS, including all external interfaces; the authorization procedures for access to UPMIS; and the UPMIS input, processing, and output procedures, including exception reports, review logs, and monitoring of review logs.
- Obtained an understanding of the policies, procedures, organizational structure, and personnel relating to UPMIS.
- Evaluated the effectiveness of the UPMIS program change management process. Specifically, we reviewed 2 of 12 completed and closed CRQs (Change Requests) from July 1, 2013, through September 6, 2013, to determine whether program changes were authorized, tested, approved, and documented.
- Evaluated the appropriateness of access privileges to UPMIS databases and programs. Specifically, we evaluated 37 user IDs with update capabilities listed in the databases as of September 25, 2013, to determine the appropriateness of access privileges for accessing the UPMIS databases and programs.
- Evaluated the effectiveness of procedures for authorizing and granting access to UPMIS. Specifically, we reviewed 25 of 814 UPMIS user IDs as of September 17, 2013, to determine whether the access privileges granted to UPMIS were authorized and appropriate based on assigned job responsibilities.
- Evaluated the appropriateness of UPMIS access for 5 UPMIS users and all 41 DIS, Bureau of Enterprise Application employees as of September 17, 2013.
- Evaluated the effectiveness of procedures for deactivating the UPMIS user access privileges of 97 former Department employees and contractors who had terminated employment or contractual services from July 1, 2013, through September 16, 2013.

- Observed and evaluated the effectiveness of selected logical access controls and password settings in ensuring that administrative access privileges to the Department's network, application, and servers were appropriately restricted and enforced an appropriate separation of duties.
- 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 February 20, 2014, 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

February 20, 2014

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 operational audit of the *Department of Financial Services, Unclaimed Property Management Information System.*

If you have any questions concerning this response, please contact Teresa Michael, Interim Inspector General, at (850) 413-4970.

Sincerely,

Jeff Atwater

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
UNCLAIMED PROPERY MANAGEMENT INFORMATION SYSTEM
OPERATIONAL AUDIT

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Reviewing and Monitoring of Program Change Requests

The Department's reviewing and monitoring of program change requests needed improvement.

Recommendation:

The Department should establish a procedure for reviewing and monitoring aging program change requests based on available resources to ensure the system functions as intended by management.

Response: We non-concur. Department policy AP&P 4-06 Requests for IT Services specifies the requirement for management level monitoring of IT service requests. The Division of Information Systems also has a documented change management procedure which outlines the process and associated requirements for change requests. The Department has implemented the defined processes to ensure review and monitoring of aging program change requests for the system based on available resources. As part of our standard operating procedures, we will continue to evaluate processes and implement modifications, where appropriate.

Expected Completion Date for Corrective Action: N/A

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
UNCLAIMED PROPERY MANAGEMENT INFORMATION SYSTEM
OPERATIONAL AUDIT

Finding No. 2: Background Checks for Unclaimed Property Inventory

The Division of Accounting and Auditing, Bureau of Unclaimed Property did not have procedures to ensure that background checks were performed on employees selected to assist in the annual unclaimed property inventory process.

Recommendation:

The Department should ensure background checks have been completed for all employees assisting with the annual unclaimed property inventory process.

Response: The Department concurs. The Division of Accounting and Auditing's procedures related to the annual inventory process were updated to reflect that background checks must be completed on any employee assisting with the annual inventory.

Expected Completion Date for Corrective Action: Completed February 2014

2

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
UNCLAIMED PROPERY MANAGEMENT INFORMATION SYSTEM
OPERATIONAL AUDIT

Finding No. 3: Deactivating Access Privileges

As similarly noted in our Report No. 2007-186, improvements were needed in the Department's procedures for deactivating access privileges to the database used for UPMIS data.

Recommendation:

The Department should ensure that access privileges to the UPMIS database are appropriately deactivated when corresponding access privileges to UPMIS are deactivated.

Response: We concur. The Division previously revised the process for issuing access to the database which resolves the deactivation concern for access issued after the process was implemented. The Division is currently in the process of reviewing existing accounts to identify and resolve any additional access that may have been orphaned due to the former process.

Expected Completion Date for Corrective Action: August 2014

3

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
UNCLAIMED PROPERY MANAGEMENT INFORMATION SYSTEM
OPERATIONAL AUDIT

Finding No. 4: Security Controls – User Authentication

Certain security controls related to user authentication needed improvement.

Recommendation:

The Department should improve user authentication controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

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

Expected Completion Date for Corrective Action: Ongoing

4

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DEPARTMENT OF FINANCIAL SERVICES
UNCLAIMED PROPERY MANAGEMENT INFORMATION SYSTEM
OPERATIONAL AUDIT

Finding No. 5: Appropriateness of Access Privileges

Access privileges of selected UPMIS IT programming staff were not appropriate for their job duties.

Recommendation:

The Department should continue to ensure that access to UPMIS is appropriate.

Response: We concur. The Department will continue to review and ensure that access to UPMIS is appropriate.

Expected Completion Date for Corrective Action: Ongoing