STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-210
June 2018

DEPARTMENT OF FINANCIAL SERVICES

Unclaimed Property Management Information System (UPMIS)

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 Jimmy Patronis served as Chief Financial Officer during the period of our audit.

The team leader was Wayne Revell, CISA, and the audit was supervised by Hilda Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

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

FLAuditor.gov

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

Unclaimed Property Management Information System (UPMIS)

SUMMARY

This operational audit of the Department of Financial Services (Department) focused on evaluating selected information technology (IT) controls applicable to the Unclaimed Property Management Information System (UPMIS) and included a follow-up on the findings included in our report No. 2014-109. Our audit disclosed the following:

Finding 1: The Department did not conduct an annual inventory audit of the unclaimed property vault during 2017 and could not demonstrate that the required background screenings had been performed for two employees who participated in the 2016 annual inventory audit.

Finding 2: Certain security controls related to user authentication need improvement to ensure the confidentiality, integrity, and availability of UPMIS data and Department IT resources.

BACKGROUND

Within the Department of Financial Services (Department), the Division of Unclaimed Property (Division)[1] utilizes the Unclaimed Property Management Information System (UPMIS) to manage the collection and distribution of unclaimed property. Unclaimed property is a financial asset that has been lost, left inactive, or is unknown to its owner. Common types of unclaimed property are dormant bank accounts, unclaimed or undelivered insurance proceeds, stocks, dividends, uncashed checks, refunds, credit balances, and contents of abandoned safe deposit boxes at financial institutions. These unclaimed assets are held by the reporting entity (holder) for a set period. If the holder does not reestablish contact with the owner and reactivate the account according to the owner's affirmed, documented wishes, or deliver the asset to the owner, the holder reports and remits the asset to the Department as unclaimed property.

The Department uses various methods to proactively attempt to notify apparent owners of their unclaimed property. Apparent owners are individuals who are reported by the holders and whose names are listed in the unclaimed property database as the owner of an account. The methods used by the Department include the services of various official and private databases, direct mail, media coverage and media-related activities, and participation in community events, seminars, and various association gatherings. As of March 2018, the Department held unclaimed property valued at more than $1.52 billion.

UPMIS is a custom-built, interactive, Web-based application designed to collect, compile, store, and report unclaimed property data in Florida. UPMIS contains a searchable database, accessible from the Department's Unclaimed Property Web site (www.FLTreasureHunt.gov). As of March 2018, the database contained 9.9 million claimable accounts valued at $25 or more. The Department is responsible

[1] Effective July 1, 2016, Chapter 2016-165, Laws of Florida, reorganized the Department designating the Bureau of Unclaimed Property as the Division of Unclaimed Property.

for the operation and maintenance of UPMIS. Within the Department, the Office of Information Technology (OIT), formerly the Division of Information Systems, operates the Chief Financial Officer's Data Center that maintains UPMIS.

State law[2] provides that the Department may allow an apparent owner to electronically submit a claim for unclaimed property to the Department. If a claim is submitted electronically for $1,000 or less, the Department may use a method of identity verification other than a copy of a valid driver license, other government-issued photographic identification, or a sworn notarized statement. The electronic claims (e-claims) process allowing electronic submittal of selected unclaimed property claims was implemented on September 19, 2015.

FINDINGS AND RECOMMENDATIONS

Finding 1: Annual Inventory Audit and Background Screenings

Effective security controls include the performance of security background screenings for personnel who are in sensitive or special trust positions. The Department's *Unclaimed Property Vault Annual Inventory Audit Guide* (*Guide*) provides that an audit of the unclaimed property vault should be conducted annually in September and that all team members conducting the unclaimed property vault annual inventory audit must have satisfied a complete background screening, including fingerprinting, within the preceding 6 months.

In response to our audit inquiry, Department management indicated that, due to the unavailability of volunteers from the Division of Accounting and Auditing, the annual inventory audit of the unclaimed property vault was not conducted in September 2017 as required in the *Guide.* Department management also indicated that the last annual inventory audit of the vault was performed in October 2016.

As part of our audit, we requested records of background screenings for the 16 Division of Accounting and Auditing team members who participated in the October 2016 inventory audit of the unclaimed property vault. Department staff were unable to provide documentation demonstrating that the required background screenings for 2 of the 16 team members had been performed within the 6 months preceding the start date of the inventory audit. Although the audit assignment sheet indicated that 2 of the team members had received background screenings, Department staff were unable to provide documentation that 1 team member had ever received a background screening and documentation for the other team member, who served as the inventory audit team leader, indicated a background screening date of February 24, 2016, which was not within the required 6 months preceding the date of the inventory audit.

Timely completion of the annual inventory audit of the unclaimed property vault would enhance Department management's assurances related to the completeness and accuracy of the inventory of assets in the vault. Additionally, timely background screenings, including fingerprinting, for the team members conducting the annual inventory audit, within 6 months preceding the audit, would provide Department management greater assurance that the vault inventory will not be compromised during the inventory audit. A similar finding was noted in our report No. 2014-109.

[2] Section 717.124(7), Florida Statutes.

Recommendation: We recommend that Department management ensure that the annual inventory audit of the unclaimed property vault is timely performed and that all team members conducting the audit have received the required background screening, including fingerprinting, within the preceding 6 months of the inventory audit.

Finding 2: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain UPMIS security controls related to user authentication need improvement. We are not disclosing specific details of the issue in this report to avoid the possibility of compromising UPMIS data and Department IT resources. However, we have notified appropriate Department management of the specific issue.

Without appropriate UPMIS security controls related to user authentication, the risk is increased that the confidentiality, integrity, and availability of UPMIS data and IT resources may be compromised. A similar finding related to user authentication was communicated to Department management in connection with our report No. 2014-109.

Recommendation: We recommend that Department management improve certain UPMIS security controls related to user authentication to ensure the confidentiality, integrity, and availability of UPMIS data and Department IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the applicable findings included in our report No. 2014-109.

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 2017 through March 2018 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 UPMIS during the period July 2017 through February 2018 and selected actions subsequent thereto. The audit included selected business process application controls over transaction data input, processing, and output; selected application-level general controls over logical access, security controls, change management, and background screening related to UPMIS; and audit findings disclosed in audit report No. 2014-109. The overall objectives of the audit were:

- To evaluate 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. 2014-109.
- 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 and reviewed UPMIS-related documentation to obtain an understanding of:
  - UPMIS background information including the system's purpose or goals involving financial, operations, and compliance requirements.
  - UPMIS data and business process flows, including key sources of data input (including interfaces), key application transactions and processes, and key types of application data output.
  - UPMIS computing platform, including applicable hardware, operating system, database management system, and security software.

- Evaluated UPMIS business process application controls related to input, interfaces, processing, and output. Specifically, we:
  - Obtained an understanding of the UPMIS e-claims process implemented on September 19, 2015, allowing for filing unclaimed property claims electronically in certain situations for certain types of accounts, including the requirements for filing e-claims.
  - Evaluated the effectiveness of 28 key input edits specifically related to the unclaimed property e-claims process as of December 20, 2017, to determine whether the UPMIS e-claims function has online edits to adequately prevent erroneous data from being entered.
  - Inquired with Division staff and reviewed Department documentation to obtain an understanding of the services provided by LexisNexis, the third-party processing provider for claimant input into UPMIS, to determine its role in the e-claims process.
  - Inspected examples of output Crystal Reports, including the *Electronic Claims Diagnostic Report* and the *Unclaimed Property Voucher Report*, that are used to reasonably assure the integrity of production data and transaction processing.
  - Inspected an access listing of authorized users on March 8, 2018, and evaluated access controls to Crystal Reports related to the e-claims process to determine whether access to output reports was based on business need and appropriately limited to authorized users.
- Evaluated the administrative procedures for, and controls over, logical access privileges to the UPMIS application and database. Specifically, we evaluated:
  - Division procedures and Department access forms and instructions to obtain an understanding of, and verify the Division had adequate procedures in place for, controlling access to the UPMIS application and database.
  - The appropriateness of access privileges for 16 of the 156 active Department employee user accounts with UPMIS application access as of December 6, 2017.
  - The appropriateness of access privileges for all 194 OIT employees listed on the People First roster as of December 8, 2017, to determine whether OIT employees were appropriately restricted from accessing the UPMIS application.
  - The appropriateness of access privileges for 20 unique UPMIS database user accounts as of November 15, 2017, to determine whether access privileges to the UPMIS database were appropriate.
- Evaluated UPMIS authentication and identification controls. Specifically, we evaluated:
  - Division procedures and Department policy regarding password requirements to obtain an understanding of, and verify the Division had adequate procedures in place related to, UPMIS authentication and identification controls.
  - UPMIS authentication and identification controls as of November 21, 2017.
- Evaluated controls for the protection of confidential data related to UPMIS. Specifically, we:
  - Obtained an understanding of controls and reviewed Department policy and procedures related to the protection of confidential UPMIS data.
  - Evaluated documentation related to the Department's e-mail encryption process.
- Evaluated UPMIS application configuration management controls. Specifically, we:
  - Reviewed Department policy and OIT procedures to determine whether policies and procedures are designed to reasonably assure that aging UPMIS program change requests are reviewed and monitored, changes to application functionality in production are authorized and appropriate, and unauthorized changes are detected and reported promptly.

- Observed a demonstration on February 8, 2018, of the monitoring process for UPMIS program change requests, reviewed documentation related to the process, and evaluated controls for monitoring outstanding program change requests.
- Evaluated the effectiveness of change controls for 5 of the 49 closed change requests implemented during the period July 1, 2017, through November 1, 2017.

- Evaluated the effectiveness of security awareness and other security-related personnel policies related to employee background screenings. Specifically, we:
  - Inspected the Department's draft *Background Screening Policy* and evaluated the Department's Bureau of Human Resource Management, *Internal Policy & Procedure No. 23, Fingerprint Procedure* to determine whether a procedure had been established related to employee background screenings.
  - Examined Department records for 16 of the 156 Department employees with UPMIS access privileges as of December 6, 2017, to assess whether UPMIS users had received the required background screening for personnel who are in sensitive or special trust positions.
  - Inquired with Division of Unclaimed Property staff regarding performance of the annual inventory audit of the unclaimed property vault during 2017.
  - Examined the Department records related to the background screenings for the 16 Division of Accounting and Auditing team members assigned to the annual inventory audit of the unclaimed property vault conducted in October 2016 to evaluate the timeliness of the screenings obtained and whether the background screening results were properly evaluated before employees were assigned to the inventory audit.
- 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
JIMMY PATRONIS
STATE OF FLORIDA

May 23, 2018

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 *Unclaimed Property Management Information System (UPMIS)*.

If you have any questions concerning this response, please contact Leah Gardner, Director of Audit, at (850) 413-3112.

Sincerely,

Jimmy Patronis

JP/rlg
Enclosure

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

Unclaimed Property Management Information System (UPMIS)

DEPARTMENT OF FINANCIAL SERVICES' RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Annual Inventory Audit and Background Screenings

The Department did not conduct an annual inventory audit of the unclaimed property vault during 2017 and could not demonstrate that the required background screenings had been performed for two employees who participated in the 2016 annual inventory audit.

Recommendation: We recommend that Department management ensure that the annual inventory audit of the unclaimed property vault is timely performed and that all team members conducting the audit have received the required background screening, including fingerprinting, within the preceding 6 months of the inventory audit.

Response: The Department concurs. The Division of Unclaimed Property's procedures have been updated to include obtaining assistance with the annual inventory audit from other divisions and, if needed, from the Department's Office of Inspector General.

The annual inventory in previous years had been performed by individuals not associated with the Division. The Division of Accounting and Auditing provided staff to conduct the inventory in those years. In 2017, that assistance was unable to be arranged. It will be in 2018. The Division will ensure the inventory is completed in all future years.

The Division's procedures have been updated to require supporting documentation for background screenings and finger-printing for the required time period, for any employee involved in the annual inventory audit.

In addition to the annual inventory audit, a monthly "random box audit" of a randomly-selected bin's contents has been performed each month for several years by the Division. All monthly random box audits are conducted by staff who are independent of the unclaimed property vault. The randomly computer-selected bin's contents are inventoried and reconciled to the data for that bin in the unclaimed property database.

Procedures also require vault staff to perform a reconciliation of bin contents each time it has been opened and closed, and again each time it has been reviewed by the contracted personal property descriptor/appraiser. All items are reconciled to UPMIS.

Expected Completion Date for Corrective Action: May 31, 2018

Unclaimed Property Management Information System (UPMIS)

Finding No. 2: Security Controls – User Authentication

Certain security controls related to user authentication need improvement to ensure the confidentiality, integrity, and availability of UPMIS data and Department IT resources.

Recommendation: We recommend that Department management improve certain UPMIS security controls related to user authentication to ensure the confidentiality, integrity, and availability of UPMIS data and Department IT resources.

Response: Responsible staff has been made aware of this finding. Impact to the current process is considered low. This control will be addressed and meet the auditor's recommendation.

Expected Completion Date for Corrective Action: October 1, 2018