



# AUDITOR GENERAL

## WILLIAM O. MONROE, CPA



### DEPARTMENT OF FINANCIAL SERVICES

## UNCLAIMED PROPERTY MANAGEMENT INFORMATION SYSTEM

### Information Technology Audit

#### SUMMARY

The Department of Financial Services (Department), Bureau of Unclaimed Property, 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 left inactive by its owner. Our audit focused on evaluating selected information technology (IT) controls applicable to UPMIS during the period September 2006 through January 2007.

The results of our audit are summarized below:

**Finding No. 1:** Our audit disclosed aspects of the Department's practices for managing access privileges that needed improvement. We also noted instances of excessive or inappropriate system access privileges.

**Finding No. 2:** We noted that Department staff could not provide a comprehensive and accurate listing of all terminated employees. In addition, we noted instances where Department staff did not remove access privileges of terminated employees in a timely manner.

**Finding No. 3:** Improvements were needed in certain physical security controls of the Bureau of Unclaimed Property and certain user authentication controls within UPMIS.

**Finding No. 4:** Improvements were needed in locator registration policies and procedures.

**Finding No. 5:** The UPMIS change management process needed strengthening.

**Finding No. 6:** The Department's reconciliation of cash disbursements and receipts between UPMIS and the Florida Accounting Information Resource Subsystem (FLAIR) needed

enhancement to provide more thorough follow-up on reconciling differences between the two systems.

**Finding No. 7:** UPMIS on-line screens and reports did not display holder refund cash disbursements, limiting the Department's ability to monitor holder refunds.

**Finding No. 8:** We noted instances of UPMIS training manuals not being finalized or not being updated for system changes.

#### BACKGROUND

Pursuant to Section 717.102, 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 is presumed to be unclaimed property. Section 717.103, Florida Statutes, provides that intangible property is subject to the custody of the 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 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, disposition of unclaimed property, depositing of funds and proceeds from the sale of unclaimed property, and making determinations of claims to unclaimed property.

Every person holding funds or other property, tangible or intangible, presumed unclaimed and subject to custody as unclaimed property shall report

the property to the Department. Florida law provides that the State has an obligation to make an effort to notify owners of unclaimed property in a cost-effective manner.

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 re-establish contact, then the asset is delivered to the Department as unclaimed property.

The Department is required to record the information provided by the holder, including the dollar amount, owner name, last known address, social security number, and any beneficiaries or joint owners. All receipts, except a \$15 million fund that is kept to pay claims, are deposited into the State School Fund, managed by the Department of Education. Each originally reported amount, however, is always available to the owner or his or her heirs since there is no statute of limitation on this property.

The Bureau of Unclaimed Property uses various methods in its attempt to notify apparent owners of the whereabouts of their unclaimed property. Historically, this was done through an annual publication of names in newspapers throughout Florida. In recent years, the Department has transitioned to a more proactive approach to notify owners, which includes searching credit bureau records, driver's license searches, radio and television programs, and by participating in home shows, state fairs, and other community events.

Section 717.1400, Florida Statutes, provides that private investigators holding a Class "C" individual license, Florida-certified public accountants, and attorneys licensed to practice in Florida must register with the Department in order to file claims as a claimant's representative, acquire ownership of or entitlement to unclaimed property, receive a

distribution of fees and costs from the Department, and obtain unclaimed property dollar amounts, numbers of reported shares of stock, and social security numbers held by the Department. Such individuals are categorized by the Department as "locators."

UPMIS was designed to collect, compile, and report unclaimed property data in Florida and to support statutory requirements for collecting and evaluating unclaimed property information from all Florida counties. UPMIS contains a searchable database, accessible from the Department's Unclaimed Property Web site - [www.fltreasurehunt.org](http://www.fltreasurehunt.org). This database contains nearly 3,000,000 names of apparent owners of unclaimed property, valued at \$25 and higher.

UPMIS was developed in-house by the Department of Financial Services, Division of Information Systems (DIS) staff with the assistance of development consultants. UPMIS was developed in a Web-based relational database environment, replacing a preexisting mainframe, non-relational database unclaimed property system. The Bureau of Unclaimed Property accepted the Unclaimed Property Management Information System Version 1.0 on January 1, 2005, with UPMIS being brought on-line on January 24, 2005.

---



---

#### **Finding No. 1:**

#### **Management of System Access Privileges**

---

An important aspect of IT security management is the establishment of system access privileges that restrict users to only those system functions necessary to perform their assigned duties. Properly configured access privileges help enforce an appropriate segregation of incompatible duties and minimize the risk of unauthorized system actions.

Sound practices for managing system access privileges include the following:

- Having the data or system owner initiate access requests and specify the nature and extent of access privileges to be given to each user.

- Developing standard security profiles that define the access requirements for groups of users and thereby simplify the process of setting up access.
- Documenting access requests and the approval thereof in a clear, standardized, retrievable manner.
- Monitoring security activity, such as changes to security profiles, through regular logging and review.

Access to UPMIS was controlled through a combination of Resource Access Control Facility (RACF), Database2 (DB2), and UPMIS application software. To access UPMIS, Department staff entered a RACF user ID into UPMIS, while locators entered an UPMIS ID. UPMIS application programs then retrieved a corresponding UPMIS security profile, through which UPMIS determined the RACF group ID to be used for accessing the DB2 database. The database security then determined which table privileges the user was granted by comparing the RACF group ID to individual database tables.

To grant users the ability to access UPMIS, the Department established access privileges in RACF, DB2, and UPMIS. Our audit disclosed aspects of the Department's practices for managing access privileges that needed improvement. Specifically:

- UPMIS access privileges were not documented in a manner that clearly demonstrated the level of access users had been granted to the various UPMIS functions. Access privileges were defined within the UPMIS application using a descriptor called a verb. Because the different components within UPMIS were designed differently and did not use standard verb definitions, a particular verb, such as "view," could represent different access capabilities in the different UPMIS components. Documentation was not available from the Department that described the access capabilities associated with the verb definitions in the various components. Therefore, we could not evaluate the appropriateness of UPMIS access privileges and it was not apparent how the Department could effectively monitor these access privileges.

- There was no documentation available that provided a detailed description of UPMIS access privileges associated with specific RACF groups. Therefore, as access requests are made, the extent of access privileges actually being granted to the new user may not be apparent to the individual who initiates the access request.
- UPMIS access requests and management's approval thereof were not documented on standard access request forms. User access requests were made through various means by submitting the new user's RACF ID and instructions to set the new user's privileges the same as those of an existing user. This process did not document that the specific access rights needed by the new user had been considered.
- Changes to security profiles were not automatically logged by the system. Instead, critical historical information, such as the user ID of the individual making the security change, had to be manually entered into the security tables, potentially limiting the Department's ability to pinpoint accountability for security changes, should the manual logging fail to occur.

Our audit also disclosed instances of excessive or inappropriate system access privileges within RACF, DB2, and UPMIS, as described in the following:

- The Department created a RACF group with direct access to the production database to facilitate UPMIS security updates. The four members in this RACF group were DIS staff with various security administration, supervisory, and system development responsibilities. The security administration capabilities appeared to be incompatible with the system development responsibilities of three members of the group in that they had not only the ability to modify application programs, but also the ability to modify data. Additionally, all members of this group had the ability to modify their own security profiles. This included the ability to give themselves (and others) update access privileges in production UPMIS without the approval of the Bureau of Unclaimed Property. As discussed above, such actions would not have been automatically logged by the system.

- Ten of eleven DIS staff with UPMIS security profiles had update access privileges in production UPMIS. We could not determine the complete extent of their update capabilities because of the lack of documentation of access privileges as described above. However, we determined that, because one of the ten individuals was assigned to all UPMIS groups, he had complete update access rights in the production system.
- Seven of the nine user IDs within a certain RACF group that had direct access to DB2 database tables, including the ability to view, add, modify, and delete information, did not appear to need the privileges to accomplish their job duties. One of the seven RACF user IDs was an ID used by the UPMIS application to allow access to the database by external users, all of whom sign on through UPMIS rather than RACF. The external users' access to database tables and views should have been limited. In response to our audit inquiries, Department staff indicated that one of the user IDs in question was removed from the group and another ID was planned to be removed. In addition, the Department indicated that the remaining five user IDs were intentionally left in the group so that the DIS staff could modify data when production problems arose. We question the necessity of these individuals having the unrestricted, ongoing ability to update production data, as the system users should be primarily responsible for updating data.
- Three of the four user IDs in another RACF group that had direct access to DB2 database tables, including view, add, and update capabilities, did not appear to need the access privileges for their jobs. In response to our audit inquiries, Department staff stated that the three user IDs in question did not need the access privileges and were removed from the group.
- Four RACF user IDs existed, including three that had been established for use by consultants, even though they were no longer needed. In response to our audit inquiries, Department staff indicated that they removed these RACF IDs.
- One DIS staff member was granted the SYSADM authority within the DB2 database, which grants access to all data within DB2 and nearly complete control of DB2, and was not needed for his job duties. In response to our audit inquiries, Department staff stated that the SYSADM authority had since been removed from this individual.
- During our review of the DB2 database, we noted seven RACF user IDs defined in the database that were not needed. These RACF IDs no longer existed in RACF. In response to our audit inquiries, Department staff indicated that six of the seven user IDs were deleted from the DB2 database and the remaining RACF user ID would be deleted at a later time.
- Twenty-two unneeded RACF group IDs existed. Users, mainly Bureau of Unclaimed Property employees, were assigned to some of the groups, but none of the groups were assigned access privileges and the groups were not used outside of UPMIS. In response to our audit inquiries, Department staff indicated that the group IDs were unnecessary and were subsequently deleted from RACF.
- Two locators each had two UPMIS user IDs for accessing UPMIS when only one ID appeared to be needed by each locator. In response to our audit inquiries, Department staff indicated that one of the user IDs for each locator in question was subsequently deactivated.

Weak security administration controls, such as poor documentation of access rights and authorizations, limited monitoring of security activity, and inappropriate or unneeded system access privileges, increase the risk of unauthorized disclosure, modification, or destruction of data and IT resources.

**Recommendation:** The Department should clearly define, standardize, and document all access capabilities associated with UPMIS to facilitate proper security administration. The Department should establish the means to automatically log security updates. Additionally, the Department should limit user and developer access privileges to UPMIS information to only what is needed in the course of their job duties. Specifically, DIS staff should be restricted from having ongoing update capability in production UPMIS. Should specific circumstances arise where DIS personnel need access to the UPMIS production application to assist users, access should be granted on a temporary basis, upon approval of the Bureau of Unclaimed Property, and then revoked immediately after the applicable work is completed.

#### **Finding No. 2:**

#### **Terminated Employee Access Capabilities**

Proper access controls include provisions to timely remove or adjust employee access privileges when employment terminations and job reassignments occur. Prompt action is necessary to ensure that a former or reassigned employee's access privileges are not misused by the employee or others.

As part of our audit, we requested from the Department a listing of all terminated employees for the period January 1, 2006, through September 30, 2006. In October 2006, the Department provided us three separate lists of employee terminations, each of which we found to be incomplete.

In response to our audit inquiries regarding this matter, Department staff stated that there was no automated mechanism in place for the Department to obtain a comprehensive and accurate listing from People First, the State's human resource management system, of employees who terminated from the Department. Similar issues with the reliability and accuracy of People First standard reports were noted in our report No. 2007-087. The Department of Management Services was aware of issues with the People First standard termination report and was working on a resolution as of the end of our current audit field work.

Department staff further indicated that the Department implemented a process through which staff manually tracked all separated employees. However, as of November 16, 2006, the manual process had not yet been tested for accuracy by the Department.

Notwithstanding the potential limitations of a manually-complied list, we compared the listings to employee access privileges in both UPMIS and RACF. Users had to be properly authorized in both to be granted access to the UPMIS application. Our comparison of 400 terminated employees disclosed the following:

- Department staff performed a review of users with access to the UPMIS application as part of the process of providing us with an UPMIS application access listing. Based on the Department's review, the UPMIS application access privileges of 12 individuals who had previously terminated from the Department were removed on October 6, 2006, which constituted periods between 21 and 231 days after their termination. In response to our audit inquiries, Department staff indicated that none of the access privileges had been used subsequent to the employee's termination. One of the 12 individuals retained RACF access privileges for 49 days after her termination date. Notwithstanding the Department's review, our audit disclosed an additional instance where one employee retained UPMIS access privileges for 90 days after her termination date. In response to our audit inquiries, Department staff indicated that her UPMIS access had since been removed, her RACF account was deleted at the time of her termination, and her UPMIS account had not been used subsequent to her termination. Because the RACF user IDs for the above-mentioned individuals unnecessarily remained on the DB2 database, the RACF user IDs retained the UPMIS access privileges in the database. This increased the risk that a new user who happened to be assigned the same RACF user ID would automatically inherit the same database access rights of the previous UPMIS user.

- Two employees retained RACF access privileges for periods between 108 and 185 days after their termination dates. Two of these employees continued to have access privileges as of the date of our testing. In response to our audit inquiries, Department staff indicated that these two individuals' access privileges had since been removed. Department staff further indicated that none of these accounts had been used subsequent to the employee's termination.

Notwithstanding the reporting issues with People First, the Department remains responsible for monitoring terminations and timely adjusting access privileges. The lack of a complete and accurate listing of employee terminations may have contributed to the above-noted inconsistencies in the removal of access capabilities for terminated employees. Without timely deletion of access of employees who terminate employment with the Department, the risk is increased that access privileges could be misused by the former employees or others.

---

**Recommendation:** Until the issue with the People First reporting functionality is resolved, the Department should continue to follow alternative procedures to ensure that accurate and complete records of all employee terminations are maintained. Additionally, the Department should ensure that the RACF and UPMIS access privileges of terminated employees are removed in a timely manner.

---

### Finding No. 3:

#### Other Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of data IT resources, and sensitive information. During our audit, we identified aspects of security controls in the areas of physical security and UPMIS user authentication that needed improvement. Specific details of these issues are not disclosed in the report to avoid the possibility of compromising the Department's information and resources. However, appropriate personnel have been notified of these issues.

Without adequate security controls, the integrity, confidentiality, and availability of data and resources may be compromised, increasing the risk that the Department's information and resources may be subject to improper disclosure, destruction, theft, or modification.

---

**Recommendation:** The Department should strengthen security controls in the areas noted above.

---

### Finding No. 4:

#### Locator Registration and Verification

As previously discussed, locators must, by law, register with the Department in order to file claims as a claimant's representative. Our review of the locator registration process noted the following deficiencies:

- The Department had not developed any written procedures for verifying the validity of the license at the time of the locator's application. Our testing of active locators noted nine locator licenses that were improperly recorded in the system. Specifically, for these locators, the actual license number did not correspond to the license number recorded in UPMIS.
- The Department had not implemented procedures to periodically reverify the licenses for registered locators. Our testing noted five registered locators who were listed within UPMIS even though their licenses were no longer valid. The five licenses were no longer valid due to the death of a locator, missing continuing education credits, licenses that were expired or suspended, and a license that was relinquished. These locators had not been licensed to practice for periods between 26 and 495 days. For three of the locators, we determined that they had not made use of their UPMIS access privileges subsequent to the date their license was no longer valid. For the remaining two, the Department was unable to demonstrate when their access privileges were last used.

Without adequate controls over the granting of locator privileges, individuals may inappropriately be granted and misuse the access rights of a locator, which could enable an individual to commit unauthorized or fraudulent actions.

---

**Recommendation:** The Department should implement procedures to ensure that license information is correctly recorded and supported by a valid professional license.

---

#### **Finding No. 5: Change Management Process**

Establishing controls over the modification of application programs helps to ensure that only authorized modifications are implemented. Effective system modification controls include procedures for a documented evaluation and acceptance of information system modifications by both user and IT management. State Technology Office (STO<sup>1</sup>) Rules 60 DD-2.004(1)(a) and 60 DD-2.004(2)(a), Florida Administrative Code, respectively, provide that unique identifiers and personal passwords are to be used to authenticate users. In addition, proper access controls limit system access privileges to only what is needed to perform assigned duties and restrict individuals from performing incompatible functions. Management's oversight of the use of access privileges is facilitated by assigning a unique system identifier (user ID) to all users for their sole use, thereby allowing all system activities to be traced to the responsible individual.

The Department used an Application System Request (ASR) to log which individual requested a program change, management's approval of the change, the assignment of the change to a programmer, and user's acceptance of the completed change. Our audit disclosed aspects of the Department's change management process for UPMIS that needed improvement. Specifically:

- The Department had not developed written policies and procedures governing systems development or certain job scheduling processes used for UPMIS. In response to our audit inquiries, Department staff indicated that the development of these procedures had been added to their 2007 work plan, with an anticipated completion date of June 29, 2007.
- Our review of 411 ASRs noted three instances where the user acceptance function was performed by a member of the programming team. In addition, we noted that program changes associated with ASRs did not normally undergo independent technical code reviews.
- Three programmers shared a single user ID and password for moving program changes to production. Additionally, the program change logs did not indicate which of the three individuals moved the programs. As a result, we were unable to determine whether any of the three individuals promoted their own program changes into production.
- There was no system-generated listing tying the movement of programs to production back to the original ASR. The Department's practice was to manually document this information in e-mail messages notifying the end users of the program move. However, this practice was not always followed. Our review of 98 program changes noted 13 program moves where the manually-created e-mail did not reference the program move to the ASR. Our testing additionally noted one program move that was not documented on an e-mail. In response to our audit inquiries, Department staff concurred that the 13 program moves did not reference the authorizing ASR; however, they also indicated that they were subsequently able to determine the originating ASRs for nine of the program changes. For the remaining four changes, Department staff indicated that these were infrastructure changes that did not require an ASR, although they had since begun requiring ASRs for changes of this type.

Without written policies and procedures for systems development and job scheduling, the risk is increased that staff will not perform their jobs in a consistent manner in accordance with management's intent. A lack of independent code review and adequate

---

<sup>1</sup> Effective July 1, 2005, the responsibilities of the STO were assimilated by the Department of Management Services.

documentation of program moves increases the risk of malicious or erroneous programs being implemented into production. Additionally, the sharing of a single user ID and password limits the ability to trace system activities to the responsible individual.

---

**Recommendation:** The Department should develop and implement UPMIS policies and procedures for the systems development and job scheduling processes. Department procedures should include provisions for an appropriate segregation of duties within the program change process, including appropriate supervisory and end user reviews and approvals. The Department should cease allowing programmers to share user IDs and each authorized individual should be assigned a unique user ID with a corresponding password. Finally, the Department should implement a process to ensure that program changes are accurately recorded and referenced to the originating ASR.

---

#### Finding No. 6:

##### Reconciling Procedures

Effective user controls include the reconciliation of processing results between interconnected systems. Sound reconciliation procedures include following up on and correcting or explaining reconciliation differences.

On a monthly basis, Department staff reconciled cash receipts and disbursement transactions between UPMIS and FLAIR, the State's accounting system, with differences being identified as reconciling items on a reconciliation spreadsheet. There were known reconciling items that occurred each month as a result of classification differences between UPMIS and FLAIR. In response to our audit inquiries, certain types of reconciling items requiring no further action, such as dividends and interest, were identified and explained by the Bureau of Unclaimed Property staff performing the reconciliations. However, during our testing, we noted additional reconciling differences, such as timing issues and corrections, identified on the reconciliation spreadsheets, indicating that follow-up might have been necessary. We determined that the Department had not followed up on exceptions from

the monthly reconciliations to ensure that no corrective action was required. For example, during the month of May 2006, differences between the systems equaled \$3,313,383. While the Department indicated that most of these differences were explainable, they could not provide documentation supporting how they reached those conclusions. The lack of appropriate follow-up on potential issues identified by the reconciliation process precluded the Department's ability to demonstrate the completeness of cash information in UPMIS.

---

**Recommendation:** The Department should establish procedures to analyze and follow-up on reconciling differences between UPMIS and FLAIR.

---

#### Finding No. 7:

##### System Functionality

Proper information system development methodologies help ensure, among other things, that adequate mechanisms exist for defining and documenting the output requirements for each information system development or modification project. An important objective of an information system development methodology is to provide reasonable assurance that systems function properly and meet user requirements.

Our audit disclosed that once holder refund transactions were input into UPMIS, the resulting holder refund cash disbursements were not displayed by the on-line application screens or output reports. In response to our audit inquiries, Department staff stated that this was due to the current system functionality for viewing cash disbursements requiring a claim number, which was not part of the holder refund record. This issue had been outstanding since early system implementation, as noted in a system change request submitted in April 2005. As of December 22, 2006, two ASRs regarding this issue remained outstanding.

The inability to view data once it has been input into a system limits the ability to monitor the information contained therein and increases the risk that errors and



irregularities may not be identified. Additionally, because the holder refund cash disbursement transactions are recorded in FLAIR but are excluded from the UPMIS reports used in the reconciliation process, the transactions become additional reconciling items between UPMIS and FLAIR.

---

**Recommendation:** The Department should implement the necessary system changes to ensure that holder refund cash disbursement transactions are included in applicable UPMIS on-line screens and reports. In future system modifications, the Department should ensure that all system requirements are taken into account, including appropriate output requirements, when making modifications to the UPMIS application.

---



---

**Finding No. 8:**  
**UPMIS Training Manuals**

---

Effective knowledge transfer is necessary to equip end users to effectively and efficiently use an application system to support business processes. Knowledge transfer includes the development of a training plan to address initial and ongoing training and skills development, training materials, user manuals, procedure manuals, and user documentation. These materials should be updated, as appropriate, whenever relevant system changes are implemented.

Our audit disclosed that training manuals were developed within the areas of Accounts Receivable (UPMIS Holder Reporting Training Manual, October 2004) and Accounts Payable (UPMIS Claims Training Manual, October 2004). However, within the Asset Management area, a draft training manual was never completed and none of the UPMIS training manuals had been updated for system changes.

On November 6, 2006, in response to our audit inquiries, we were provided an updated UPMIS Holder Reporting Training Manual, dated September 2006. In addition, the Department initiated the completion of the Asset Management Training Manual and update of the Claims Training Manual, with estimated completion dates of March 1, 2007, and May 1, 2007, respectively. Not providing staff with accurate, complete, and up-to-date guidance in using UPMIS to perform their assigned tasks increases the risk of errors and inefficiencies in business processes and may limit user confidence in the system.

---

**Recommendation:** The Department should complete the development and update of the Asset Management and Claims training manuals. Additionally, the Department should implement a process whereby the training manuals are reviewed on a periodic basis and modified when relevant business process or application system changes are implemented.

---



---

**OBJECTIVES, SCOPE, AND METHODOLOGY**

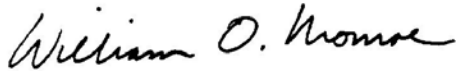
---

The objectives of this audit were to determine the effectiveness of selected general and application IT controls related to UPMIS. Our audit scope focused on evaluating selected IT controls applicable to UPMIS during the period September 2006, through January 2007.

In conducting this audit, we interviewed appropriate Department personnel, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to UPMIS.

**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 information technology audit.



William O. Monroe, CPA  
Auditor General

**MANAGEMENT RESPONSE**

In a letter dated May 15, 2007, the Chief Financial Officer provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. This audit was conducted by Shawn McCormick, and supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA\*, CISA, Audit Manager, via e-mail at [joningram@aud.state.fl.us](mailto:joningram@aud.state.fl.us) or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (<http://www.state.fl.us/audgen>); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

\*Regulated by State of Florida.

**APPENDIX A**  
**MANAGEMENT RESPONSE**



CHIEF FINANCIAL OFFICER  
STATE OF FLORIDA

ALEX SINK

May 15, 2007

Mr. William O. Monroe  
Auditor General  
State of Florida  
Claude Pepper Building  
111 West Madison Street  
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

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 preliminary report for the Information Technology Audit for the Unclaimed Property Management Information System (UPMIS), for the period September 2006, through January 2007.

If you have any questions or would like to discuss the matter further, please contact David Jenkins, Director of Internal Audit, at (850) 413-4962.

Sincerely,

Handwritten signature of Alex Sink in cursive.

Alex Sink

AS:Jc

Enclosure

**Florida Department of Financial Services**  
**Audit Response**  
**Information Technology Audit**  
**Unclaimed Property Management Information System**  
**Preliminary and Tentative Audit Findings**

---

**Finding No. 1:** Our audit disclosed aspects of the Department's practices for managing access privileges that needed improvement. We also noted instances of excessive or inappropriate system access privileges.

**Recommendation:** The Department should clearly define, standardize, and document all access capabilities associated with UPMIS to facilitate proper security administration. The Department should establish the means to automatically log security updates. Additionally, the Department should limit user and developer access privileges to UPMIS information to only what is needed in the course of their job duties. Specifically, DIS staff should be restricted from having ongoing update capability in production UPMIS. Should specific circumstances arise where DIS personnel need access to the UPMIS production application to assist users, access should be granted on a temporary basis, upon approval of the Bureau of Unclaimed Property, and then revoked immediately after the applicable work is completed.

**Response:** The Department concurs. The Bureau of Financial Applications (BFA) will work in conjunction with the Bureau of Unclaimed Property (BUP) to document the security access capabilities used within the Unclaimed Property Management Information System (UPMIS). BFA and BUP will also work to create a standardized method for requesting and documenting the groups and rights of each UPMIS user, along with improvements in the historical tracking of changes. The authorization of these changes will be tracked in the Application System Request (ASR) System. Additionally, the Department will include UPMIS in the Departmental employee services access process specified by DFS AP&P 4-06, Requests for Information Technology Resources, and DIS Operating Procedure, DIS-011 Help Desk Employee Services Access Procedures. To address the DIS staff access to the UPMIS production application, some DIS staff will continue to be in the UPSTAFF group in order to have read-only access to many sections of the system with BUP approval. This group was created to provide a basic level of access to UPMIS for viewing of data and filing claims. Filing claims is the only "update" capability this group provides, similar to the capabilities through the public website. Any additional access needed by DIS Personnel will be granted on a temporary basis, upon approval of the Bureau of Unclaimed Property, and then revoked immediately after the applicable work is completed, and will be tracked through the ASR System.

The Department anticipates that procedural changes will be implemented within 60 days and documentation of security administration will be completed by November 1, 2007.

**Finding No. 2:** We noted that Department staff could not provide a comprehensive and accurate listing of all terminated employees. In addition, we noted instances where

Department staff did not remove access privileges of terminated employees in a timely manner.

**Recommendation:** Until the issue with the People First reporting functionality is resolved, the Department should continue to follow alternative procedures to ensure that accurate and complete records of all employee terminations are maintained. Additionally, the Department should ensure that the RACF and UPMIS access privileges of terminated employees are removed in a timely manner.

**Response:** The Department concurs, and will continue to strengthen controls related to removal of access privileges when employees are reassigned or separate employment from the Department. The Department will include UPMIS in the Departmental employee services access process specified by DFS AP&P 4-06, Requests for Information Technology Resources, and DIS Operating Procedure, DIS-011 Help Desk Employee Services Access Procedures. BUP will also submit an update/terminate access request, via the existing ASR system, separate from the DFS process. Additionally, BUP management will review the UPMIS Security Matrix on a monthly basis, to ensure that no terminated/reassigned employee maintains unauthorized access to UPMIS. The Department anticipates that procedural changes will be implemented within 60 days.

**Finding No. 3: Improvements were needed in certain physical security controls of the Bureau of Unclaimed Property and certain user authentication controls within UPMIS.**

**Recommendation:** The Department should strengthen security controls in the areas noted above.

**Response:** The Department concurs, and has addressed and rectified certain physical controls of the Bureau of Unclaimed Property and will take immediate appropriate action to improve any remaining user authentication controls within UPMIS.

**Finding No. 4: Improvements were needed in locator registration policies and procedures.**

**Recommendation:** The Department should implement procedures to ensure that license information is correctly recorded and supported by a valid professional license.

**Response:** The Department concurs. BUP and BFA are taking steps to improve the procedures, policies and processes associated with locator verification, registration, recording and periodic review of individuals, firms, and licensees. BUP and BFA anticipate that procedural changes will be made within 60 days, and system changes will be implemented by November 1, 2007.

**Finding No. 5: The UPMIS change management process needed strengthening.**

**Recommendation:** The Department should develop and implement UPMIS policies and procedures for the systems development and job scheduling processes. Department procedures should include provisions for an appropriate segregation of duties within the program change process, including appropriate supervisory and end user reviews and approvals. The Department should cease allowing programmers to share user IDs and each authorized individual should be

assigned a unique user ID with a corresponding password. Finally, the Department should implement a process to ensure that program changes are accurately recorded and referenced to the originating ASR.

**Response:** The Department concurs. The Department is developing the policy and procedures for the Change Management process and will continue to strengthen controls related to systems development processes. Procedures are being implemented within the ASR system that ensure only authorized BUP staff can authorize, review, and accept changes to UPMIS. Additionally, the Department will require unique user IDs and passwords for authorized individuals during the UPMIS production build process. The Department will improve the procedures related to the movement of programs to production. The possibility of implementing a reporting system that ties production deployments to the associated ASRs will be researched. The Department anticipates that procedural changes will be implemented within 60 days.

**Finding No. 6: The Department's reconciliation of cash disbursements and receipts between UPMIS and the Florida Accounting Information Resource Subsystem (FLAIR) needed enhancement to provide more thorough follow-up on reconciling differences between the two systems.**

**Recommendation:** The Department should establish procedures to analyze and follow-up on reconciling differences between UPMIS and FLAIR.

**Response:** The Department concurs. BUP and BFA will work together to identify any UPMIS reports that need to be redesigned or changed as appropriate to aid in the reconciling between FLAIR and UPMIS cash disbursements and receipts. In conjunction with the system changes, BUP will establish and/or revise existing procedures regarding reconciliation of cash disbursements and receipts. BUP and BFA anticipate that both systems changes and the establishment of procedures can be completed by November 1, 2007.

**Finding No. 7: UPMIS on-line screens and reports did not display holder refund cash disbursements, limiting the Department's ability to monitor holder refunds.**

**Recommendation:** The Department should implement the necessary system changes to ensure that holder refund cash disbursement transactions are included in applicable UPMIS on-line screens and reports. In future system modifications, the Department should ensure that all system requirements are taken into account, including appropriate output requirements, when making modifications to the UPMIS application.

**Response:** The Department concurs. BUP and BFA will work together to prioritize and implement the changes necessary to ensure that holder refund cash disbursement transactions are included in the UPMIS on-line screens and reports where applicable.

**Finding No. 8: We noted instances of UPMIS training manuals not being finalized or not being updated for system changes.**

**Recommendation:** The Department should complete the development and update of the Asset Management and Claims training manuals. Additionally, the Department should implement a process whereby the training manuals are reviewed on a periodic basis and modified when relevant business process or application system changes are implemented.

**Response:** The Department concurs. BUP management has completed the development of the Asset Management and Tangible Property Management training manuals and has completed the update of the Claims training manual. BUP management, along with the assistance of BFA, will implement a process to review and revise UPMIS training manuals at six month intervals and when major UPMIS enhancements are implemented.

**THIS PAGE LEFT BLANK INTENTIONALLY**