AUDITOR GENERAL
DAVID W. MARTIN, CPA

DEPARTMENT OF REVENUE

CHILD SUPPORT ENFORCEMENT AUTOMATED MANAGEMENT SYSTEM (CAMS PHASE I)

Information Technology Audit

SUMMARY

Pursuant to Section 409.2557(1), Florida Statutes, the Department of Revenue (Department) is designated as the State agency responsible for the administration of Florida's Child Support Enforcement (CSE) Program under Title IV-D of the Federal Social Security Act. Pursuant to Title 45, Section 302.85(a), Code of Federal Regulations, states are required to have in effect a computerized child support enforcement system. The Florida On-Line Recipient Integrated Data Access (FLORIDA) System, operated and maintained by the Department of Children and Family Services, was the Title IV-D system that provided the daily information processing operations for the CSE Program.

The Department undertook the CSE Automated Management System (CAMS) initiative to eventually replace, in phases, the functionality of the CSE Component of the FLORIDA System. CAMS was being developed and implemented in two sequential functional increments. The first increment, CAMS Phase I, was implemented Statewide by April 2006 and provided Compliance Enforcement. The projected completion date for the second increment, CAMS Phase II, was February 2011.

Our audit focused on evaluating selected information technology (IT) controls applicable to CAMS Phase I during the period January 2007 through July 2007.

The results of our audit are summarized below:

Finding No. 1: The Department's error review and reporting process needed improvement.

Finding No. 2: The Department experienced ongoing problems with address information in CAMS.

Finding No. 3: Intended functionality for reporting and follow-up on a missing key data field in CAMS had not been implemented.

Finding No. 4: 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. 5: We noted instances where the Department did not timely remove the access privileges of terminated employees.

Finding No. 6: Improvements were needed in certain security control features related to CAMS Phase I and the supporting network environment at the Department, in addition to the matters discussed in Findings No. 4 and 5.

BACKGROUND

The Department has various statutory responsibilities in the administration of the CSE Program. The CSE Program executes child support processes that include: 1) identification and establishment of paternity, 2) location of non-custodial parents, 3) enforcement of support orders, and 4) distribution of child support remittances to custodial parents.

The Department began the CAMS initiative in October 2003 to replace the FLORIDA System, CSE Component, as the application system supporting Florida's CSE Program. The Department elected to use SAP Public Services, Inc. (SAP) software to develop CAMS.

According to the Department's CAMS operational work plan for 2006-07, CAMS is intended to be a state-of-the-art system to support Florida's CSE Program. The system is expected to automate much of the management of child support cases to more efficiently process cases from establishment through enforcement and collection of obligations through the life of the case. The operational work plan states that many of the activities associated with child support enforcement are manual and labor intensive and that CAMS is intended to use less paper and more automation, thereby freeing staff to be more responsive to the needs of Florida's children.

The Department contracted with Deloitte Consulting L.L.P. (Deloitte) to develop and implement the first increment, CAMS Phase I, providing Compliance Enforcement. CAMS Phase I primarily consisted of functions to determine compliance with support orders, the next appropriate enforcement actions to be taken, and the location of individuals related to the case. The contract with Deloitte for CAMS Phase I became effective on October 20, 2003, and was completed on January 10, 2007. Twenty-three contract amendments were executed that increased the base contract amount from $27,668,211 to $30,538,730. The total CAMS Phase I development cost, including the Deloitte contract amount, was $72,726,018.

The pilot for CAMS Phase I occurred in January 2006, with Wave 1 and Wave 2 rollouts of the system occurring in March and April 2006, respectively. After Statewide implementation was complete, CAMS Phase I moved into an operations and maintenance mode. The Department's CAMS Design and Support team assumed responsibility for the operations and maintenance, as well as additional functionality originally envisioned for CAMS Phase I but not implemented in 2006.

During the first phase of CAMS, the FLORIDA System and CAMS worked together as one child support enforcement system with necessary data duplicated on the two systems. After the initial load of data from the FLORIDA System to CAMS, the two systems exchanged information in a reciprocal fashion to maintain the synchronization of case and business partner (member) data. CAMS owned and maintained the business partner data which included all persons or organizations that impact a case, for example, case members (custodial parents, non-custodial parents, and child), employers, and financial institutions. The FLORIDA System continued to own and maintain case data and financial information for the business partners.

On October 31, 2006, the Department received proposals from vendors in response to an invitation to negotiate for the design, development, and implementation of CAMS Phase II, which will consist of the Case Management, Establishment, Payment Processing, and Fund Distribution functions and remaining compliance activities not included in Phase I. The vendor selection process was not complete as of the end of our audit field work.

Pursuant to Title 45, Section 307.15(b)(10), Code of Federal Regulations, states are required to acquire Independent Verification and Validation (IV&V) services throughout all system development phases and activities as a condition of Federal funding through the Federal Office of Child Support Enforcement (OCSE). This requirement provides for an entity independent of the Department to review all technical and managerial aspects of the project. With the deployment of CAMS Phase I, the Department allowed the previous IV&V services contract to expire as of June 30, 2007. The Department, in conjunction with OCSE, was in the process of drafting a procurement document for IV&V services for CAMS Phase II.

Finding No. 1: Error Review and Reporting

Proper IT controls are intended to ensure the integrity of information. For example, input controls provide for the complete and accurate recording of authorized transactions into a system through, among other things, the prompt detection, notification, and correction of input errors.

On a nightly basis, the FLORIDA System sent files to CAMS. During the CAMS load process, the records containing errors, such as invalid or missing data fields, were identified and subsequently separated into four error report files; the CAMS technical file, the FLORIDA technical file, the case file, and the case member file. These error reports were then distributed to individuals who were responsible for their review, correction, and follow-up. Additionally, the Department had a process in place whereby the case and case member error workers were to provide daily feedback to the appropriate staff on the status of each error being worked.

Our audit testing disclosed the following:

- The CAMS technical error report file and the FLORIDA technical error report file were distributed daily. However, due to higher priorities, the errors were not being reviewed by the assigned technical staff. During our audit field work, Department staff stated that, on an occasional basis, an individual who was not responsible for the technical error reports performed a limited review, eliminating known reported problems and errors included on the case and case member error reports.
- The case member error reports were also distributed daily. However, for 3 of 28 reports tested, daily feedback was not provided by the error workers in accordance with Department process.

When errors are not timely identified, reported, investigated, and corrected, the accuracy and completeness of the data in the system could be jeopardized, hindering the effectiveness of compliance enforcement activities.

Recommendation: The Department should ensure that all errors are timely reviewed, corrected, and reentered into the system.

Finding No. 2: Ongoing Address Issues

IT controls are intended to promote the integrity of data stored within an information system and exchanged between systems. CAMS utilized mailing software that corrected and standardized address components to increase mailing efficiency and cost-effectiveness. Additionally, the mailing software functioned to maintain a consistent address format within the system and apply that format to data received from various external agencies and the FLORIDA System. The mailing software was also used to facilitate communication between CAMS and the FLORIDA System by parsing (separating) the address information into discrete components, such as street, city, and postal code.

Address records in CAMS originated from one of four sources:

- The FLORIDA System as conversion records (these records represented the original address as entered into the FLORIDA System when a child support case was established);
- Manual entries in CAMS as a result of a change of address after the case was loaded into CAMS. After a case was converted to CAMS, all member address changes were made in CAMS rather than in the FLORIDA System;
- Change of address records entered into CAMS from external interfaces. For example, updates provided by the Department of Highway Safety and Motor Vehicles; and
- Change records submitted by the State Disbursement Unit (SDU)[1] through the FLORIDA System.

[1] Pursuant to Section 61.1826(1), Florida Statutes, the Department contracted with the Florida Association of Court Clerks to establish and operate an SDU, for the collection and disbursement of child support payments.

An IV&V report, dated March 14, 2007, indicated that CAMS had ongoing address problems. Our audit also disclosed inconsistencies with regard to the communication of address information between CAMS and the FLORIDA System. According to CAMS design, after a FLORIDA conversion record was processed by CAMS, an ECHO record (confirmation receipt) was to be sent back to the FLORIDA System to ensure that both systems were in agreement. Additionally, after an address change record was processed by CAMS, regardless of whether it originated as a CAMS manual entry, a CAMS external interface address record, or an SDU change record, a transaction record was to be sent back to the FLORIDA System to ensure that both systems were in agreement. Our audit disclosed instances where these communications did not occur. The Department acknowledged that it was aware of these problems, and had logged them in its maintenance tracking system.

For those ECHO records and transaction records that were sent back to the FLORIDA System from CAMS, our audit disclosed instances where:

- Address information stored in CAMS was not in agreement with address information stored in FLORIDA; and
- Correct address information in the FLORIDA System had been replaced with incorrect or undeliverable address information.

The primary cause for these address inconsistencies was that the ECHO records and transaction records were reformatted by the mailing software. Additionally, external interface and the FLORIDA System transaction errors reported by the mailing software had been ignored by CAMS and erroneous address information was loaded into the system. Although the Department used the mailing software in order to correct and standardize address information, its use instead resulted in address mismatches between the two systems.

Finally, our audit noted another source of ongoing address problems through the Department's practice of giving address information obtained from external interfaces a higher priority than address information provided by custodial parents. This practice sometimes resulted in previous address information replacing newly-provided address information.

Inaccurate address information increases the risk that checks will not be delivered to custodial parents in a timely manner. It also increases the risk that notices of noncompliance, as well as notices of enforcement actions, will not reach non-custodial parents.

Recommendation: The Department should ascertain and correct identified address problems with the CAMS application in order to promote the integrity of data in CAMS and the FLORIDA System and the effective and efficient operation of the child support enforcement program.

Finding No. 3: Monitoring of Data Completeness

Programmed validation and edit checks are, for the most part, the most critical and comprehensive set of controls in assuring that the initial recording of data into a system is accurate. Programmed validation and edit checks may also occur after data has entered the application system. Transactions detected with missing data need to be controlled to ensure that they are corrected in a timely manner.

When a service contract (support order) was converted from the FLORIDA System to CAMS, an edit took place within CAMS that determined whether the service contract header contained a depository number (derived from the court case number). When a depository number did not exist, CAMS generated a case worker task in the form of a follow-up activity that notified a case worker to update the depository number field in the FLORIDA System. This activity started a three-day wait period. Each day, through the completion of the wait period, CAMS determined whether the depository number had been updated through the FLORIDA System-CAMS interface. According to CAMS design, if the depository number had not been entered, the case worker task would be regenerated and an escalated task would be sent to the supervisor level as a follow-up activity.

Our audit disclosed that the case worker activity was generated one time when the service contract was converted to CAMS, but was not regenerated after the three-day wait period when the depository number was not updated. Additionally, the task was not escalated to the supervisor level. In response to our audit inquiries, the Department logged the issue in its maintenance tracking system.

The depository number was integral to the enforcement tool selection process, because at the conclusion of the process, notices of noncompliance and enforcement actions were to be printed and issued to the non-custodial parents. The depository number was required on the printed forms. If the depository number was missing, the forms could not print and would not be available for compliance enforcement activities.

Recommendation: The Department should implement the necessary system changes to ensure that the depository number field is monitored to provide for effective compliance enforcement. In future system development projects, the Department should ensure that all necessary system functionality is implemented as designed.

Finding No. 4: Management of 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. The effectiveness of system access controls is enhanced when access authorizations are approved by applicable management, documented, and maintained on file for management's periodic review.

Upon our audit request, the Department provided us a list of 2,403 active CAMS users as of March 26, 2007. Our testing of access privileges of 47 CAMS programmers, consultants, and end users disclosed the following:

- Documentation evidencing the authorization by applicable supervisors of access privileges for 14 of the 47 users could not be provided by Department staff.
- Through discussions with Department staff of the access rights granted to the 47 users, we determined that the access privileges of another 14 individuals were not appropriate given their current job functions. For 3 of these individuals, the access privileges allowed them to, contrary to an appropriate segregation of duties, perform a combination of security administration and system administration functions.

Additionally, through discussions with Department staff, we determined that Phase I CAMS security was not designed to allow inquiry only capability for activities. Access to CAMS functionality was granted in security roles by activity but did not distinguish between inquiry and update access capability. The inability to provide inquiry only access made it necessary for the Department to provide the CAMS Design and Support team with either full update access or no access, hindering them from being able to solve production problems. Consequently, Department management stated that they decided to accept the associated risk and grant the technical support staff update access to CAMS. Department staff indicated that existing monitoring reports were to be modified to monitor CAMS Design and Support staff updates of activities. In response to our audit inquiries, Department staff provided an estimated implementation date of December 31, 2007, for the revisions to the monitoring reports.

The lack of documentation of access authorizations and inappropriate or unneeded system access privileges increase the risk of unauthorized disclosure, modification, or destruction of data and IT resources. Additionally, the lack of a properly designed access control mechanism limited the Department's ability to restrict staff's access to only what was necessary to perform their jobs.

Recommendation: The Department should ensure that documentation is maintained of all access capabilities associated with CAMS to facilitate proper security administration. Additionally, the Department should ensure access privileges of personnel are commensurate with their job duties and appropriately segregated to prevent individuals from being able to subvert controls. Furthermore, the Department should ensure that future CAMS development efforts include an access control mechanism that allows for granting inquiry only capability when necessary to limit users to only what is needed to perform their job duties.

Finding No. 5: Terminated Employee Access Capabilities

Proper access controls include provisions to timely remove employee access privileges when employment terminations occur. Prompt action is necessary to ensure that a former employee's access privileges are not misused by the employee or others. Additionally, sound practices for managing system access privileges include maintaining an automated log of access modifications made by security personnel to determine how, when, and by whom specific actions were taken.

Upon our audit request, the Department provided us a list of 566 employees who terminated from the Department during the period July 1, 2006, through March 16, 2007. Our comparison of this list to users with access privileges to CAMS and the Department's IT network disclosed the following:

- CAMS access privileges of 54 employees were not timely deleted and remained in place for periods ranging from 2 to 188 days after their dates of termination. Our tests disclosed that 2 of the 54 employees still had access privileges as of March 26, 2007. Subsequently, in response to our audit inquiries, Department staff indicated that they had removed the CAMS access privileges of these 2 individuals. The CAMS access privileges of the 54 employees had not been used after the employees' termination.
- We noted 29 employees who, as of March 19, 2007, had network access accounts even though they had been terminated from the Department for periods ranging from 3 to 261 days. Subsequently, in response to our audit inquiries, Department staff indicated that they had removed the 29 network accounts.
- The Department did not maintain logs of network access modifications made by security personnel to evidence when terminated employees' access privileges were removed, or logs of last log-on dates to evidence whether access privileges were used subsequent to their termination date.

Without timely deletion of access privileges for employees who terminate employment with the Department, the risk is increased that access privileges could be misused by the former employees or others. Without logs of network access modifications, the Department may be unable to determine when a user's access was modified, and the Department's ability to pinpoint accountability for a breach of security, should it occur, may be hindered.

Recommendation: The Department should strengthen its controls to ensure that unneeded access privileges are promptly removed in order to minimize the risk of compromising the Department's data and information resources. Additionally, the Department should implement a logging function to capture modifications made to users' network access privileges.

Finding No. 6: Other Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of data and IT resources. During our audit, we identified certain deficiencies in the Department's security control features related to CAMS Phase I and the Department's IT network, in addition to the matters described in Findings No. 4 and 5. Specific details of theses deficiencies are not disclosed in this report to avoid the possibility of compromising the Department's information and resources. However, appropriate Department staff have been notified of the deficiencies.

Recommendation: The Department should implement the appropriate security controls to ensure the continued integrity, confidentiality, and availability of the Department's data and IT resources.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this audit were to determine the effectiveness of selected general and application IT controls related to CAMS Phase I. Our audit scope focused on evaluating selected IT controls applicable to CAMS Phase I during the period January 2007 through July 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 CAMS Phase I.

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.

David W. Martin, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated September 27, 2007, the Executive Director provided a response to our preliminary and tentative audit findings. The letter is included at the end of this report 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 Cathy Jones, CISA, 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 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.myflorida.com/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.

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.

David W. Martin, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated September 27, 2007, the Executive Director provided a response to our preliminary and tentative audit findings. The letter is included at the end of this report Appendix A.

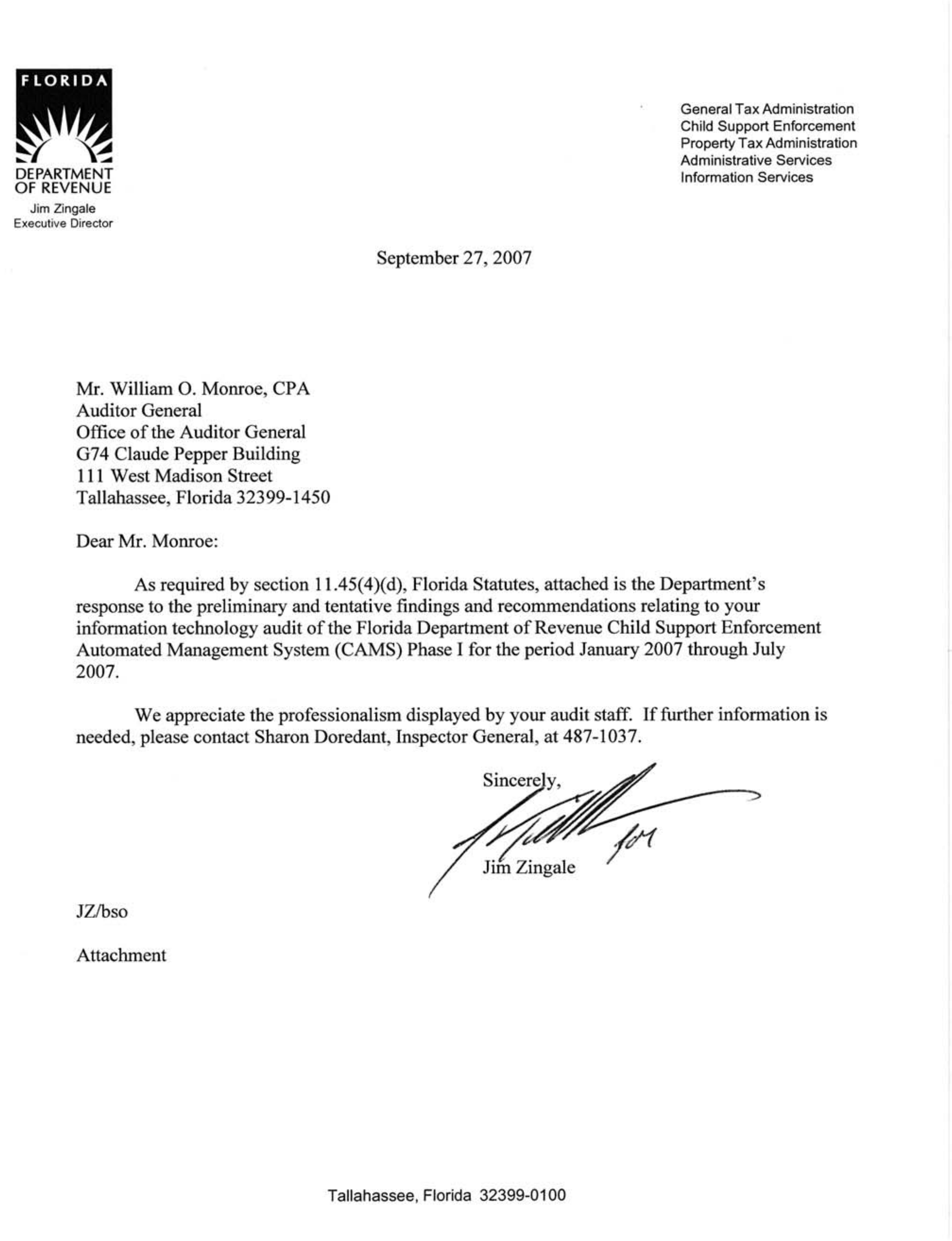
To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. This audit was conducted by Cathy Jones, CISA, 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 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



FLORIDA
DEPARTMENT
OF REVENUE
Jim Zingale
Executive Director

General Tax Administration
Child Support Enforcement
Property Tax Administration
Administrative Services
Information Services

September 27, 2007

Mr. William O. Monroe, CPA
Auditor General
Office of the Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

As required by section 11.45(4)(d), Florida Statutes, attached is the Department's response to the preliminary and tentative findings and recommendations relating to your information technology audit of the Florida Department of Revenue Child Support Enforcement Automated Management System (CAMS) Phase I for the period January 2007 through July 2007.

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact Sharon Doredant, Inspector General, at 487-1037.

Sincerely,

for

Jim Zingale

JZ/bso

Attachment

Tallahassee, Florida 32399-0100

Response to Preliminary and Tentative Audit Findings
Department of Revenue
Child Support Enforcement Automated Management System (CAMS) Phase I
For the Period January 2007 through July 2007
Information Technology Audit

Finding No. 1: The Department's error review and reporting process needed improvement.

Recommendation: The Department should ensure that all errors are timely reviewed, corrected, and reentered into the system.

Response: The Department has established a process to ensure errors are timely distributed, reviewed, and corrected in the FLORIDA System or CAMS.

The Department's process description is divided into the two (2) categories cited in the audit:

1. Audit: Technical errors were not being reviewed by assigned technical staff daily.

   The technical error staff review error files daily and notify the CAMS Data Resource Management (DRM) Team when they identify errors that require manual correction. Upon notification, the DRM Team distributes these errors to the case or case member error workers. If the technical error requires a system enhancement, either a HEAT ticket or ISSR is submitted.

2. Case member error workers do not provide daily feedback.

Case member error workers provide daily feedback to the DRM Team as lists are completed. However, the error workers are not solely dedicated to correcting the daily errors and feedback may be provided later than the day the original error list was distributed**.** Additionally, the DRM Team tracks daily lists and updates the status as completed. If the list is not completed within five (5) business days, the DRM Team asks the error team member for a status. Lists may be reassigned to other case or case member error workers to expedite the correction process when the DRM Team is notified of an error worker's increased workload.

Finding No. 2: The Department experienced ongoing problems with address information in CAMS.

Recommendation: The Department should ascertain and correct identified address problems with the CAMS application in order to promote the integrity of data in CAMS and the FLORIDA System and the effective and efficient operation of the child support enforcement program.

Response: While many of the address problems highlighted in the report have already been addressed, we concur with the finding. The Department continues to monitor address maintenance within CAMS and the FLORIDA; any problems identified and/or enhancements are analyzed in accordance with the CAMS defect resolution process or change management process.

Finding No. 3: Intended functionality for reporting and follow-up on a missing key data field in CAMS had not been implemented.

Recommendation: The Department should implement the necessary system changes to ensure that the depository number field is monitored to provide for effective compliance enforcement. In future system development projects, the Department should ensure that all necessary system functionality is implemented as designed.

Response: The Department agrees with this finding. As was noted in the formal preliminary and tentative findings letter to the Department, this condition has been recorded as a defect in the CAMS Incident Management system as a system defect (HEAT ticket #168027). This defect will be prioritized in accordance with the CAMS prioritization process and will be corrected. While this item has currently not received prioritization for resolution it is anticipated that within the next three (3) months this incident will gain prioritization and begin the process of realizing the change in the system.

Finding No. 4: 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 ensure that documentation is maintained of all access capabilities associated with CAMS to facilitate proper security administration. Additionally, the Department should ensure access privileges of personnel are commensurate with their job duties and appropriately segregated to prevent individuals from being able to subvert controls. Furthermore, the Department should ensure that future CAMS development efforts include an access control mechanism that allows for granting inquiry only capability when necessary to limit users to only what is needed to perform their job duties.

Response: The proper procedures were not in place during the time of the audit. This caused some documentation of user access privileges to be omitted. A procedure is now in place to eliminate future occurrences:

- User access privileges for CAMS are documented accurately and timely.
- Forms are in place for requesting training or specific security access privileges.

The three users who had expanded privileges are a part of the Basis team and these privileges have been deemed appropriate to their job function. The system currently records all changes. There is an agreement between Basis and Security that if a user access issue comes up after hours, they should document it and advise us immediately so we have it for our records.

CAMS Phase I was not designed to robustly allow "inquiry-only" access to certain activities. Changes to CAMS Phase I programming would be costly and at the present moment are a low priority due to the unavailability of resources from the development team. Security is researching authorization restrictions that weren't provided in the initial rollout and plans to revise the appropriate roles with more display capability. This will be accomplished by 12/31/2007. CAMS Phase II is in development and will support "inquiry–only" access.

Finding No. 5: We noted instances where the Department did not timely remove the access privileges of terminated employees.

Recommendation: The Department should strengthen its controls to ensure that unneeded access privileges are promptly removed in order to minimize the risk of compromising the Department's data and information resources. Additionally, the Department should implement a logging function to capture modifications made to users' network access privileges.

Response: The deficiency of terminated users' access privileges being retracted has been addressed and terminated employees and the revoked privileges are being tracked. The system currently records changes to users' network access privileges and end dates can be created ahead of time to retract access for users whose terminations have been reported to CAMS Security.

A new application, Personnel Action Separation System (PASS), is in development and will aid in providing a consistent, global notification of employee terminations from all Department of Revenue offices which should greatly reduce the number of users the Security team is not aware of prior to termination. The PASS application should be implemented by 12/31/2007.

Finding No. 6: Improvements were needed in certain security control features related to CAMS Phase I and the supporting network environment at the Department, in addition to the matters discussed in Findings No. 4 and 5.

Recommendation: The Department should implement the appropriate security controls to ensure the continued integrity, confidentiality, and availability of the Department's data and IT resources.

Response: Action is being taken on the security deficiencies that exist with CAMS Phase I and the Department's IT network. We will implement the recommended safeguards that will ensure the availability, confidentiality, and integrity of the Department's data and IT resources.