




January 12, 2012

MEMORANDUM

TO: Lisa Vickers, Executive Director

FROM: Sharon Doredant, Inspector General 
Office of Inspector General

SUBJECT: Six-Month Update on Auditor General Report No. 2012-002, Information Technology Audit of the Florida Online Recipient Integrated Data Access (FLORIDA) System Child Support Enforcement (CSE) Component and Child Support Enforcement Automated Management System (CAMS)

As required by *section 20.55(5)(h), Florida Statutes*, attached is the Department's six-month status update for corrective actions taken in response to the Auditor General's Report No. 2012-002, Information Technology Audit of the Florida Online Recipient Integrated Data Access (FLORIDA) System Child Support Enforcement (CSE) Component and Child Support Enforcement Automated Management System (CAMS).

If you have any questions, please contact me at 617-8152, or Teresa Wood at 717-7598.

SD/bso

Attachment

cc: Marshall Stranburg, Deputy Executive Director
Blanca Bayó, Chief of Staff
Teresa Wood, Director of Auditing
Kathy DuBose, Coordinator, JLAC

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|----------------------------------|----------------------------------------|
| Status Date 12/31/11 | Report No. AG 2012-002 | Report Title CAMS IT Audit | | |
| Contact Person | Program/Process | | Phone No. | |
| Dan Kelly / Valerie Griner | Information Services (ISP), Child Support Enforcement (CSE) | | (850)717-6940 / (850)617-8176 | |
| Activity | Accountability | | Schedule | |
| Documentation of User Access Authorization | Responsible Unit | Coordinating Unit | Repeat Finding | Anticipated Completion Date |
| | ISP/ISM/CAMS Security, CSE/SSP/FLORIDA Security | | Y | 1/31/2012 |
| Finding | Authorization documentation for FLORIDA System CSE Component and CAMS access privileges for some users was missing, incomplete, or inaccurate. | | | |
| No. | 1 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | The Department should ensure that access authorization forms for the FLORIDA System CSE Component and CAMS are appropriately completed and maintained. | | | |
| Original Response | We concur. The Department will continue to periodically remind security officers and administrators for FLORIDA and CAMS of the requirements for accurate completion and retention of access request forms. | | | |
| Status Updates | 12/31/2011: The Department has created an electronic version of the CAMS access request form to be used with the implementation of the second phase of CAMS. The form has a built-in work flow for approvals and signatures, and the data will be retained electronically. This will eliminate the problem of a misplaced form. | | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| Status Date | Report No. | Report Title | | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|----------------------------------|--------------------------------|
| 12/31/11 | AG 2012-002 | CAMS IT Audit | | |
| Contact Person | Program/Process | | Phone No. | |
| Dan Kelly / Valerie Griner | Information Services, Child Support Enforcement | | (850)717-6940 / (850)617-8176 | |
| Activity | Accountability | | Schedule | |
| Appropriateness of Access Privileges | Responsible Unit | Coordinating Unit | Repeat Finding | Anticipated Completion Date |
| | ISP/ISM/CAMS Security, CSE/SSP/FLORIDA Security | | Y | 3/31/2012 |
| Finding | The access privileges of some FLORIDA System CSE Component and CAMS users were not appropriate for their job responsibilities. | | | |
| No. | 2 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | The Department should limit access privileges to the FLORIDA System CSE Component and CAMS resources to only what is needed to perform job responsibilities. Additionally, update access privileges assigned to IT staff for CAMS should be monitored as required by the Department's acceptance of risk forms. | | | |
| Original Response | We concur. As mentioned in response to finding 5, access privileges will continue to be reviewed annually by the user's supervisor during the employee's annual performance review, and at the time an employee's job duties are changed. The review will ensure the access privileges are in sync with employee job responsibilities. Additionally, the Department will research what is required to provide the capability to monitor IT staff with system update access privileges in CAMS production. | | | |
| Status Updates | <p>12/31/2011: The Department reviewed the existing CAMS security role assignments and role content in order to split them into more defined job duties. This was the basis for creating new security roles for existing CAMS functions for Phase 2. We assert this is complete.</p> <p>CAMS security roles have been redesigned to be more targeted to specific job duties. In Phase 2, users will have the capability to request more than one security role based on job duties. We assert this is complete.</p> <p>Because of the conversion from FLORIDA to CAMS, Department-authorized FLORIDA users now have view only access; therefore, there are no conflicts of duties between FLORIDA and CAMS security roles. We assert this is complete.</p> <p>The Department has implemented a process that allows supervisors look up access privileges for each CAMS user. CAMS and FLORIDA access privileges are reviewed with the employee as part of the employee's annual evaluation process and whenever the employee changes job duties. We assert this is complete.</p> <p>The final CAMS will have the capability to allow temporary assignment of extra privileges (Super-user Privilege Management - SPM). The Department has created procedures for granting temporary elevated privileges using a unique SPM account. When a user is granted a temporary SPM account, all user activity under that account is documented, including when access is granted and removed.</p> <p>User security role assignments will be posted online for periodic supervisor review. Any elevated privileges temporarily assigned for go live will be reviewed at least monthly; all elevated privileges should be removed by the end of the warrantee period.</p> | | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------------|
| Status Date | Report No. | Report Title | | |
| 12/31/11 | AG 2012-002 | CAMS IT Audit | | |
| Contact Person | Program/Process | | Phone No. | |
| Dan Kelly / Valerie Griner | Information Services, Child Support Enforcement | | (850)717-6940 / (850)617-8176 | |
| Activity | Accountability | | Schedule | |
| Access Privileges | Responsible Unit | Coordinating Unit | Repeat Finding | Anticipated Completion Date |
| | ISP/ISM/CAMS Security, CSE/SSP/FLORIDA Security | | Y | 1/31/2012 |
| Finding | | Some access privileges in the FLORIDA System CSE Component and CAMS did not enforce an appropriate separation of incompatible duties. | | |
| No. | 3 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | The Department should ensure that CAMS IT staff are not assigned access privileges that allow them to perform incompatible functions. The Department should also ensure that end users with access privileges to both the CSE Component and CAMS cannot create or assign payments and also update custodial family addresses. | | | |
| Original Response | We concur. The security officers and administrators for FLORIDA and CAMS verify that there is no separation of duty conflict for selected profiles when granting access to FLORIDA and CAMS. The FLORIDA forms used to approve access privileges were revised and require a signature confirming that the review was completed. CAMS Security staff will start annotating on the CAMS access form when the review is completed. | | | |
| Status Updates | 12/31/2011: A review of CAMS and FLORIDA privileges was completed, identifying all users that had Separation of Duties (SOD) issues between systems. Users having SOD issues were required to change roles in CAMS or profiles in FLORIDA to eliminate these conflicts, or have documented exceptions to policy. Production role assignments for Phase II go-live (January 2012) were analyzed for SOD issues and all SOD combinations were removed. SOD checks will be performed for each access request for two or more roles (individual roles have been tested and are free of SODs). The Department will conduct separation of duties verification on CAMS at least quarterly. | | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|----------------------------------|----------------------------------------|
| Status Date 12/31/11 | Report No. AG 2012-002 | Report Title CAMS IT Audit | | |
| Contact Person | Program/Process | | Phone No. | |
| Dan Kelly / Valerie Griner | Information Services, Child Support Enforcement | | (850)717-6940 / (850)617-8176 | |
| Activity | Accountability | | Schedule | |
| Timely Removal of Access Privileges | Responsible Unit | Coordinating Unit | Repeat Finding | Anticipated Completion Date |
| | ISP/ISM/CAMS Security, CSE/SSP/FLORIDA Security | | Y | 3/31/2012 |
| Finding | The Department did not timely remove FLORIDA System CSE Component and CAMS access privileges of some former employees and contractors. | | | |
| No. | 4 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | The Department should ensure that the access privileges of former Department and other entity employees and contractors are removed in a timely manner in order to minimize the risk of compromising CSE program data and IT resources. | | | |
| Original Response | We concur. The CSE contract managers are entering all contracted staff into the Department's electronic termination notification process. The entry should be completed by September 2011. A monthly termination monitoring process is in place to verify privileges for terminated state employees are properly removed. A weekly review of state employee terminations has also been implemented so that access removal is more timely. | | | |
| Status Updates | 12/31/2011: The CSE contract managers are entering all contracted staff into the Department's electronic termination notification process. Completion of entry has been delayed and anticipated completion date is now March 2012. | | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------|------------------------------------|
| Status Date | Report No. | Report Title | | |
| 12/31/11 | AG 2012-002 | CAMS IT Audit | | |
| Contact Person | Program/Process | | Phone No. | |
| Sharyn Thomas | Child Support Enforcement | | (850)617-8306 | |
| Activity | Accountability | | Schedule | |
| Access Privileges | Responsible Unit | Coordinating Unit | Repeat Finding | Anticipated Completion Date |
| | CSE/Data Safeguarding & Management | ISP/ISM/CAMS Security | Y | 12/31/2012 |
| Finding | | The Department's review of the appropriateness of CAMS user access privileges was not conducted on a sufficiently frequent basis. | | |
| No. | 5 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | The Department should reassess the frequency by which CAMS access privileges are reviewed and consider a more frequent review. | | | |
| Original Response | We partially concur. The Department agrees that access privileges must be reviewed periodically. Access privileges will continue to be reviewed annually by the user's supervisor during the employee's annual performance review and at the time an employee's job duties are changed. | | | |
| Status Updates | 12/31/2011: The Program reviewed the frequency of user reviews for CAMS access. Due to upcoming implementation of the final CAMS system, all users were reviewed in preparation for implementation. The program has implemented a requirement to review user access at initial hire, mid-point probationary review, annually thereafter and anytime their job duties change. The program will reassess the frequency and manner of the reviews mid-to-late 2012. | | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------|------------------------------------|
| Status Date | Report No. | Report Title | | |
| 12/31/11 | AG 2012-002 | CAMS IT Audit | | |
| Contact Person | Program/Process | | Phone No. | |
| Brunetta Pfaender | Information Services | | (850)717-7223 | |
| Activity | Accountability | | Schedule | |
| Vulnerability Scanning | Responsible Unit | Coordinating Unit | Repeat Finding | Anticipated Completion Date |
| | ISP/ISM/Policy & Monitoring | ISP/Project Management Office | Y | 3/31/2012 |
| Finding | | The Department did not document its evaluation of network vulnerability scans or subsequent actions to mitigate vulnerabilities. | | |
| No. | 6 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | The Department should continue its efforts to implement a process for documenting the results of vulnerability scanning evaluation and mitigation. | | | |
| Original Response | The Information Security Management (ISM) office has a deployed and documented vulnerability scanning and remediation process. The process was in use by April 2011 which includes tracking planned actions to be taken to mitigate vulnerabilities. The procedural document was completed on June 16, 2011. A verification process will be implemented and documented to ensure the planned mitigations were completed. | | | |
| Status Updates | 12/31/2011: Vulnerability scanning procedures have been documented and implemented. The process was put in use April 2011 and the procedural document completed June 2011. A verification process to validate the completion of mitigations was documented and implemented June 2011. | | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | The process has been identified and the procedures are being revised to refine mitigation process to include vetting the solution to ensure compatibility with Revenue systems and coordination with Primary Data Centers. | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|-----------------------------------|-----------------------------------------------------|
| Status Date 12/31/11 | Report No. AG 2012-002 | Report Title CAMS IT Audit | | |
| Contact Person Brunetta Pfaender | Program/Process Information Services | | Phone No. (850)717-7223 | |
| Activity Security Controls – User Authentication | Accountability | | Schedule | |
| | Responsible Unit ISP/Information Security Manager | Coordinating Unit CSE/CAMS Project Management, ISP/Basis | Repeat Finding Y | Anticipated Completion Date 6/30/2012 |
| Finding No. 7 Date 07/11/2011 | Certain Department security controls related to user authentication needed improvement. | | | |
| Recommendation | The Department should improve security controls related to user authentication to ensure the confidentiality, integrity, and availability of data and IT resources. | | | |
| Original Response | We concur. The deployment of CAMS Phase II scheduled for February 2012 will offer improved security controls for user authentication. | | | |
| Status Updates <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | 12/31/2011: The implementation of CAMS, now scheduled for January 2012, will offer improved user authentication security controls. | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|------------------------------------|
| Status Date | Report No. | Report Title | | |
| 12/31/11 | AG 2012-002 | CAMS IT Audit | | |
| Contact Person | Program/Process | | Phone No. | |
| Teresa Dozier | Child Support Enforcement | | (850)617-8263 | |
| Activity | Accountability | | Schedule | |
| CAMS Disaster Recovery Plan | Responsible Unit | Coordinating Unit | Repeat Finding | Anticipated Completion Date |
| | CSE/CAMS Operations & Maintenance | ISP/DR Manager | N | 12/31/2012 |
| Finding | | The Department's CAMS Disaster Recovery Plan was not complete and up to date and had not been thoroughly tested. | | |
| No. | 8 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | | The Department should ensure that its disaster recovery plan is complete and up to date. In addition, the Department should, at least annually, conduct a comprehensive test of the plan including all critical Department IT resources. | | |
| Original Response | | We concur. The Department is scheduled to update the CAMS Disaster Recovery Plan during August – September 2011. The plan will be updated to reflect a requirement for an annual test each calendar year. The next annual test will include CAMS II, batch processing, data changes, and selected interfaces. | | |
| Status Updates | | 12/31/2011 | | |
| <input type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input checked="" type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | Due to resource commitment to the CAMS project, ISP/BASIS resources are not available to make the necessary revision to the Disaster Recovery Plan (A301), respective to the Hardware/OS Migration and Contact List. Anticipated revisions have been recorded in the "Plan Update Recommendation Log." Update as of 01/12/2012 The situation with A301, Disaster Recovery Plan has changed - with the advanced Go Live date for CAMS II, the A301 is now obsolete. The B301, Disaster Recovery Plan is now in effect. We will be conducting a Disaster Recovery test of the CAMS system this year. OIG verified this corrective action is partially complete, the program has a Disaster Recovery Plan. | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------------|
| Status Date | | Report No. | Report Title | |
| 12/31/11 | | AG 2012-002 | CAMS IT Audit | |
| Contact Person | | Program/Process | | Phone No. |
| Sharon Keri | | Child Support Enforcement | | (850)617-8092 |
| Activity | | Accountability | | Schedule |
| Enforcement Overrides | | Responsible Unit | Coordinating Unit | Repeat Finding |
| | | Compliance | | Y |
| | | | | Anticipated Completion Date |
| | | | | 03/31/2012 |
| Finding | | Because of limitations in CAMS access control functionality, many CAMS users inappropriately had the ability to perform enforcement override transactions on cases. Additionally, the Department did not monitor enforcement override transactions to ensure that such users had not performed unauthorized overrides. | | |
| No. | 9 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | | The Department should enhance CAMS functionality to provide the capability to assign view-only access privileges for the enforcement override screens. Upon implementation of the enhancements, the Department should restrict the ability to perform enforcement override transactions to authorized and appropriate users. Until such functionality can be established in CAMS, the Department should closely monitor the system activities of users with access to the override screens to ensure that only authorized users are performing override transactions. | | |
| Original Response | | We concur. The Department will initiate a system enhancement to provide the capability to assign view-only access privileges after Phase II of CAMS is implemented. In the interim, the Department believes the risk of unauthorized override entry or update is mitigated through the current procedure which directs local offices to review a CAMS report to ensure appropriate entry of overrides. The Department revised the procedures in December 2010 to indicate the frequency of the review is quarterly. | | |
| Status Updates | | 12/31/2011 | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | The Department prioritized the overrides enhancement to occur after CAMS is implemented. The request will be further prioritized based on other identified CAMS changes. | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------|-----------------------------------|--------------------------------------------------|
| Status Date 12/31/11 | Report No. AG 2012-002 | Report Title CAMS IT Audit | | |
| Contact Person Sharyn Thomas | Program/Process Child Support Enforcement | | Phone No. (850)617-8306 | |
| Activity Ongoing Address Issues | Accountability | | Schedule | |
| | Responsible Unit CSE/Data Safeguarding & Management | Coordinating Unit | Repeat Finding Y | Anticipated Completion Date 03/31/2012 |
| Finding | | | | |
| No. | 10 | The Department had not resolved some issues with address information in CAMS. | | |
| Date | 07/11/2011 | | | |
| Recommendation | | | | |
| The Department should continue its efforts to identify and correct address issues within CAMS in order to promote the integrity of the data in CAMS and the FLORIDA System CSE Component and the effective and efficient operation of the CSE program. | | | | |
| Original Response | | | | |
| We concur. The Department is continuing to make improvements and corrections on the issues identified. The majority of issues will be resolved upon implementation of CAMS Phase II, scheduled for February 2012. | | | | |
| Status Updates | | | | |
| 12/31/2011 | | | | |
| The issues identified in the finding are related to residential addresses and the FLORIDA to CAMS interface should be resolved once CAMS is implemented. | | | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|------------------------------------|
| Status Date | Report No. | Report Title | | |
| 12/31/11 | AG 2012-002 | CAMS IT Audit | | |
| Contact Person | Program/Process | | Phone No. | |
| Sharon Keri | Child Support Enforcement | | (850)617-8092 | |
| Activity | Accountability | | Schedule | |
| Caseworker Task Monitoring Procedures | Responsible Unit | Coordinating Unit | Repeat Finding | Anticipated Completion Date |
| | Compliance | | Y | Completed |
| Finding | | Although the Department had an informal process in place, the Department did not have written procedures for supervisor monitoring and follow-up of unprocessed CAMS tasks. Furthermore, the Department did not maintain a record of the tasks reviewed or the related decisions made during the monitoring process. | | |
| No. | 11 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | The Department should provide staff with approved procedures for monitoring tasks in CAMS to ensure that unprocessed tasks are completed in a timely manner consistent with management's expectations. | | | |
| Original Response | We concur. Procedures addressing the frequency of review and the use of the Business Intelligence report by region management in monitoring tasks for their service sites were approved and signed by the director on March 25, 2011. These procedures were posted to the CSE Policy and Procedure intranet site on April 6, 2011. | | | |
| Status Updates | 12/31/2011 | | | |
| <input type="checkbox"/> Open | Procedures addressing the frequency of review and the use of the Business Warehouse report by region management in monitoring tasks for their service sites were approved and signed by the director on March 25, 2011. These procedures were posted to the CSE Policy and Procedure intranet site on April 6, 2011. | | | |
| <input type="checkbox"/> Management assumes risk | | | | |
| <input type="checkbox"/> Partially complete | | | | |
| <input type="checkbox"/> Complete pending verification by OIG | Recommend closure of this finding. | | | |
| <input checked="" type="checkbox"/> Complete | OIG reviewed – agree corrective action is completed. | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| | | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|--------------------------|-----------------------|------------------------------------|
| Status Date | Report No. | Report Title | | |
| 12/31/11 | AG 2012-002 | CAMS IT Audit | | |
| Contact Person | Program/Process | | Phone No. | |
| Joe Lockard | Information Services | | (850)717-7020 | |
| Activity | Accountability | | Schedule | |
| Service Level Agreement | Responsible Unit | Coordinating Unit | Repeat Finding | Anticipated Completion Date |
| | ISP/Supplier Management | NWRDC | N | 3/31/2012 |
| Finding | | | | |
| No. | 12 | | | |
| Date | 07/11/2011 | | | |
| The Department's service-level agreement with Northwest Regional Data Center(NWRDC) lacked certain provisions required in State law. | | | | |
| Recommendation | | | | |
| The Department should work with NWRDC to ensure that its service-level agreements include all provisions required by State law. | | | | |
| Original Response | | | | |
| We concur. The Service Level Agreement (SLA) with NWRDC is scheduled to go through an annual review and renewal process. During this year's review, State laws will be researched to identify additional provisions that should be included in the SLA with NWRDC. | | | | |
| Status Updates | | | | |
| 12/31/2011 | | | | |
| The Department is in the process of negotiating with the NWRDC about the missing provisions. | | | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | | | |

CORRECTIVE ACTION PLAN

Rev. 11/04

| Status Date | | Report No. | Report Title | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-----------------------------|
| 12/31/11 | | AG 2012-002 | CAMS IT Audit | |
| Contact Person | | Program/Process | | Phone No. |
| Brunetta Pfaender | | Information Services | | (850)717-7223 |
| Activity | | Accountability | | Schedule |
| Reporting of Security Incidents | | Responsible Unit | Coordinating Unit | Repeat Finding |
| | | ISP/Information Security Manager, Primary Data Centers (PDCs) | ISP/Service Desk, ISP/Problem Management | N |
| | | | | Anticipated Completion Date |
| | | | | 3/31/2012 |
| Finding | | Contrary to State law and rules, the Department did not timely notify the Agency for Enterprise Information Technology, Office of Information Security (AEIT) of an interruption in CAMS processing. | | |
| No. | 13 | | | |
| Date | 07/11/2011 | | | |
| Recommendation | | The Department should update its internal CSIRT procedures to ensure that AEIT is timely notified of future security incidents, should they occur. | | |
| Original Response | | We concur. Prior to August 2010, state agencies, including Revenue, did not typically report loss of service caused by a system error or malfunction. After this incident, the AEIT Office of Information Security (AEIT/OIS) communicated to the agency Information Security Managers (ISMs) that an availability incident that is classified as a Class 2 or 3 incident as defined in the AEIT CSIRT procedures that exceeds the agency's Service Level Agreement (SLA) should be reported to AEIT/OIS within 24 hours, and that the agencies and the Primary Data Center(s) (PDC) should work together to develop a process to report these incidents to AEIT/OIS. The Revenue ISM is working with SSRC, NWRDC and Department of Education ISMs to add language to each agency's CSIRT procedures that provides a process for PDC and the agency working together on the appropriate joint CSIRT activities and for developing and reporting either a joint report or separate reports to the AEIT/OIS that provide consistent information regarding the incident. This process will include providing an initial report of the incident, then a final report with more detail. | | |
| Status Updates | | <p>12/31/2011: The Department is now reporting significant CSIRT incidents to AEIT that fall outside of the SLA. The ISM is working with the Service Desk and Problem Management to determine a way to identify incidents so that notifications could possibly be automated.</p> <p>The Department is in the process of revising the CSIRT procedures to be current with the revised AEIT CSIRT procedures.</p> | | |
| <input checked="" type="checkbox"/> Open <input type="checkbox"/> Management assumes risk <input type="checkbox"/> Partially complete <input type="checkbox"/> Complete pending verification by OIG <input type="checkbox"/> Complete | | | | |