**OFFICE OF**
**THE INSPECTOR GENERAL**

**SOCIAL SECURITY ADMINISTRATION**

**SINGLE AUDIT OF THE**
**STATE OF OHIO**
**FOR THE FISCAL YEAR ENDED**
**JUNE 30, 2008**

**June 2010** **A-77-10-00012**

# MANAGEMENT ADVISORY REPORT

## Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

## Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.
- Promote economy, effectiveness, and efficiency within the agency.
- Prevent and detect fraud, waste, and abuse in agency programs and operations.
- Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.
- Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.

To ensure objectivity, the IG Act empowers the IG with:

- Independence to determine what reviews to perform.
- Access to all information necessary for the reviews.
- Authority to publish findings and recommendations based on the reviews.

## Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

**MEMORANDUM**

Date: June 17, 2010

Refer To:

To: Candace Skurnik
Director
Audit Management and Liaison Staff

From: Inspector General

Subject: Management Advisory Report: Single Audit of the State of Ohio for the Fiscal Year Ended June 30, 2008 (A-77-10-00012)

This report presents the Social Security Administration's (SSA) portion of the single audit of the State of Ohio for the Fiscal Year ended June 30, 2008. Our objective was to report internal control weaknesses, noncompliance issues, and unallowable costs identified in the single audit to SSA for resolution action.

The Ohio State Auditor performed the audit. The results of the desk review conducted by the Department of Health and Human Services (HHS) concluded that the audit met Federal requirements. In reporting the results of the single audit, we relied entirely on the internal control and compliance work performed by the Ohio State Auditor and the reviews performed by HHS. We conducted our review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspections*.

For single audit purposes, the Office of Management and Budget assigns Federal programs a Catalog of Federal Domestic Assistance (CFDA) number. SSA's Disability Insurance (DI) and Supplemental Security Income (SSI) programs are identified by CFDA number 96. SSA is responsible for resolving single audit findings reported under this CFDA number.

The Ohio Bureau of Disability Determination (BDD) performs disability determinations under SSA's DI and SSI programs in accordance with Federal regulations. The BDD is reimbursed for 100 percent of allowable costs. The Ohio Rehabilitative Services Commission (ORSC) is the BDD's parent agency.

The single audit reported that ORSC:

- Could not provide documentation to support the calculation of Federal cash draws for SSA's disability program (Attachment A, Pages 1 and 2). The corrective action plan indicates the ORSC will adjust its Federal cash drawdown process to better document that funds are disbursed in accordance with Federal requirements (Attachment A, Page 2).

- Lacked internal control procedures to ensure payments for medical evidence were reviewed and approved prior to payment (Attachment A, Pages 3 and 4). The corrective action plan indicated that ORSC modified its process to require review and validation of medical evidence prior to payment (Attachment A, Page 4).

We recommend that SSA verify that ORSC:

1. Established appropriate controls to ensure cash draws for the SSA disability program are in accordance with Federal requirements.

2. Developed appropriate procedures to review and validate medical evidence payments prior to payment.

The single audit also disclosed the following findings that may impact BDD operations although they were not specifically identified to SSA. I am bringing these matters to your attention as they represent potentially serious service delivery and financial control problems for the Agency.

- Internal control weaknesses were identified related to the monitoring, security, and storage of programs and data in the State's computer system (Attachment B, Pages 1 through 6).

- Reconciliations were not performed between the detailed transactions and summary totals in the general ledger accounts (Attachment B, Pages 7 through.10).

- Controls were not sufficient to ensure the corruption of information systems was minimized and automated applications were performing as management intended (Attachment B, Pages11 through 13).

- Segregation of duties was not adequate over the purchasing of goods and services, and changes to the financial accounting structure (Attachment B, Pages 14 through 16).

- Documentation was not maintained to support interest earnings liability to the Federal Government (Attachment B, Pages 17 and 18).

Please send copies of the final Audit Clearance Document to Shannon Agee. If you have questions, contact Shannon Agee at (816) 221-0315, extension 1537.

Patrick P. O'Carroll, Jr.

Attachments

**1. VOCATIONAL REHABILITATION AND SOCIAL SECURITY DISABILITY INSURANCE – CASH MANAGEMENT**

| | |
|---|---|
| *Finding Number* | 2008-RSC01-053 |
| *CFDA Number and Title* | 84.126 – Vocational Rehabilitation<br>96.001 – Social Security Disability Insurance |
| *Federal Agency* | Department of Education<br>Department of Health and Human Services |
| *Compliance Requirement* | Cash Management |

NONCOMPLIANCE AND SIGNIFICANT DEFICIENCY

The Cash Management Improvement Act (CMIA) Agreement between the State of Ohio and the U.S. Department of Treasury states, in part:

> Section 6.1.4 – Estimate and Reconciliation of Estimates: Where estimated expenditures are used to determine the amount of the drawdown, the State will indicate in the terms of the State unique funding technique how the estimated amount is determined and when and how the State will reconcile the difference between the estimate and the State's actual expenditures.

The Vocational Rehabilitation and Social Security Disability Insurance programs' unique funding technique per the CMIA Agreement is pre-issuance.

> Section 6.2.1 – . . . Pre-Issuance: The State shall request funds such that they are deposited in a State account not more than three days prior to the day the State makes a disbursement. . . The amount of the request shall be the amount the State expects to disburse. . . .

During state fiscal year 2008, the Ohio Rehabilitation Services Commission utilized the pre-issuance funding technique and drew down approximately $125.8 million in federal funding for the Vocational Rehabilitation program and approximately $79.8 million in federal funding for the Social Security Disability Insurance program. Before completing a federal draw, the Fiscal Specialist prepares a cash forecast by obtaining the beginning cash balance for a particular fund from the Ohio Administrative Knowledge System (OAKS). Then the Fiscal Specialist will add any outstanding revenue deposits and deduct any payables and/or intra-state transfer voucher disbursements, deduct any estimated expenses for the next two days, deduct administrative payments, and deduct periodic expenses (e.g., rent, payroll, indirect costs, etc.,) from the beginning cash balance to determine the amount of the federal draw. After determining the cash balance for a particular fund, the Fiscal Specialist will compare the cash ledger from the OAKS commitment control to the summary voucher report from the Case Authorization Tracking System (CATS) to determine the amount of available funding after deducting any single payment vouchers approved and submitted to state accounting for processing. If there is not a sufficient amount of cash on hand, the Fiscal Specialist will prepare a federal draw down request.

The Commission was unable to provide any documentation to support their federal draw calculations and was unable to demonstrate how the estimated expenditures (determined via the process described above) were reconciled to the actual expenditures. Initially, procedures were performed to determine the clearance pattern of federal funds and determine whether or not the Commission was in compliance with the CMIA. However, the Commission did not retain documentation of the funds' daily cash balance and during testing expressed concerns that the cash balances in OAKS may not have been accurate. As a result, alternative procedures were performed by selecting a federal draw and two subsequent vouchers in order to determine whether or not the Commission was in compliance with the CMIA State-Treasury Agreement. The results of these procedures are noted below.

- For 25 of 28 (89%) vouchers subsequently selected from 14 Vocational Rehabilitation federal draws, we were unable to determine if the Commission disbursed the federal revenue within three business days, as required by the CMIA State-Treasury Agreement.

- For 37 of 38 (97%) vouchers subsequently selected from 19 Social Security Disability Insurance federal draws, we were unable to determine if the Commission disbursed the federal revenue within three business days, as required by the CMIA State-Treasury Agreement.

Without timely disbursement of funds by the Commission, interest penalties may be incurred by the State of Ohio for the funds drawn and not disbursed in accordance with federal requirements and the State-Treasury Agreement. According to the Commission's Finance Manager, tying a specific invoice to a specific deposit is not required by the CMIA and none of their internal systems can track this correlation. Management routinely runs low on federal funds and believes the CMIA speaks only in aggregate numbers and not specific invoices.

We recommend the Commission implement and/or strengthen controls to reasonably ensure all draw requests for the Vocational Rehabilitation and Social Security Disability Insurance programs are adequately documented and are drawn/disbursed in accordance with the CMIA State-Treasury Agreement pre-issuance methodology. We also recommend the Commission establish and document procedures to monitor cash balances and reconcile estimated expenditures to actual expenditures to reasonably ensure federal funds are drawn down consistently with the Commission's immediate cash needs.

**Official's Response and Corrective Action Plan**

*The process followed by ORSC for the drawdown of federal funds has not changed over the past seven audit periods, with no prior audit findings or management letter comments. The agency draws federal funds under the Vocational Rehabilitation program an average of two to three times per week. The State Accounting system, OAKS, will not process transactions for ORSC unless there are sufficient funds available (per budget checks in the system) to make payment on those transactions. Frequently, ORSC transactions have "bounced" or rejected in OAKS due to insufficient federal funds as the agency waited for federal funds to arrive in the State treasury as a result of our efforts to comply with the CMIA. Therefore, ORSC would contend that excess federal funds are not being drawn on a routine basis.*

*To address concerns raised by the Auditor of State, ORSC will adjust its federal drawdown process to better document the federal drawdown calculations and reconcile estimated expenditures to actual expenditures to ensure funds are disbursed in accordance with federal CMIA requirements. For example, ORSC is now processing its BDD Case Service file transfer only once per week. A report is available in CATS the morning the transfer will take place that gives the total of the transfer. A specific draw for that expenditure will be made and the CATS report attached to the draw request as support. This should satisfy both the need for documentation of the amount drawn as well as the reconciliation of expenditure to draw requirement. A similar process will be used to draw specific cash for VR Case Service file transfer expenditures which will soon begin to be done twice weekly. In addition, special draws will be done for large expenditures as they are vouchered, such as quarterly rent payments, bi-monthly payroll, bi-monthly BDD contract doctor payments, Indirect Cost assessments, and other large single or group payments as they occur. This should leave only 'routine' admin payments to be drawn from estimates and greatly reduce the amount of federal funds sitting in the state treasury based on expenditure estimates.*

**Anticipated Completion Date for Corrective Action**

*Action will be completed by September 30, 2009.*

**Contact Person Responsible for Corrective Action**

*Bill McFarland, Finance Manager, Ohio Rehabilitation Services Commission, 150 E. Campus View Blvd, Suite 150, Columbus, OH 43235, Phone: (614).433.8279, E-Mail: bill.mcfarland@rsc.state.oh.us*

## 2. SOCIAL SECURITY DISABILITY INSURANCE – DOCUMENTATION OF INTERNAL CONTROLS

| | |
|---|---|
| *Finding Number* | 2008-RSC02-054 |
| *CFDA Number and Title* | 96.001 – Social Security Disability Insurance |
| *Federal Agency* | Department of Health and Human Services |
| *Compliance Requirement* | Activities Allowed or Unallowed<br>Allowable Costs and Costs Principles |

SIGNIFICANT DEFICIENCY

An entity's internal control structure is placed in operation and maintained by management to prevent or detect misstatements in the accounting records; to help ensure compliance with laws and regulations, and to provide a basis for monitoring whether operations are achieving management's objectives. To be effective, the performance of internal control procedures must be evidenced in some manner to provide assurance the prescribed procedures are being followed.

During state fiscal year 2008, the Commission disbursed approximately $7.5 million of federal funds, or 10% of total program expenditures, for the request of Medical Evidence of Records (MER) for the Social Security Disability Insurance Program. The Commission is responsible for determining Social Security Disability Insurance claimants' disabilities and assuring determinations are adequately supported and evidenced. In order to perform the disability determinations, the Commission is authorized to purchase consultative medical examinations and medical evidence of record from the claimants' physicians or other treating sources. Once the medical evidence of record is received, the documentation supporting the service is scanned into the Levy Control System along with a Payment Authorization Form which services as the invoice. The documentation Authorization Form which serves as the invoice. The documentation is then forwarded to a Claim Adjudicator who performs a review to determine whether or not the services provided merits payment. However, the Claim Adjudicator does not evidence their review and, unless the payment is stopped by the Claim Adjudicator, the payment is automatically processed at the end of 20 days.

If internal control procedures are not performed and documented thoroughly and consistently, management is unable to provide reasonable assurance their objectives are being met and MER payments are recorded accurately. Additionally, since the Levy Control System automatically approves MER at the end of 20 days, there is an increased risk that unsubstantiated payments may be made using federal funding. Current and future funding received by the Commission could be affected as a result. The Commission's management indicated a similar issue had been brought to their attention and they have modified their process in fiscal year 2009 to begin the 20 day window once the Claim Adjudicator opens the claim for their review and not when the claim becomes available for review.

We recommend the Commission develop and implement control procedures over the review and approval of MER. These internal controls should reasonably ensure the transactions are accurately recorded and properly approved prior to payment, and be adequately documented to provide management with reasonable assurance they are performed timely and consistently. Additionally, the Commission should implement edit checks into the Levy Control System to ensure all payments are reviewed and approved by the Claim Adjudicator.

**Official's Response and Corrective Action Plan**

*Based on recommendations from the Auditor of State Performance Audit in 2008, the ORSC Bureau of Disability Determination requested modification of the Levy Control System such that payments for MER would no longer be automatically generated after 20 days from the date of receipt of bar-coded turnaround/invoice accompanying records.*

*The modification requires adjudicative staff to review and validate copies of medical evidence prior to the initiation of the payment cycle. The Levy Control System tracks this by utilizing an indicator on copies of medical evidence that are received. This indicator must be removed by adjudicative staff in order for the payment cycle to begin. During review and validation, if payment is unsubstantiated, adjudicative staff cancel the authorization for payment using specific indicators. This information is noted in the Levy Control System. Payment cannot be made without adjudicative action.*

**Anticipated Completion Date for Corrective Action**

*To address the recommendations of the prior Performance Audit, this modification to the Levy Control System was made in January of 2009.*

**Contact Person Responsible for Corrective Action**

*Kathleen Johnson, Director, Bureau of Disability Determination, Ohio Rehabilitation Services Commission, P.O. Box 359001, Columbus, OH 43235, Phone: (614).438.1501, E-Mail: Kathleen.johnson@ssa.gov*

## 1. INFORMATION TECHNOLOGY – OHIO ADMINISTRATIVE KNOWLEDGE SYSTEM (OAKS) IT SECURITY

| | |
|---|---|
| *Finding Number* | 2008-OAKS01-004 |
| *CFDA Number and Title* | All Programs Administered by the State |
| *Federal Agency* | All Federal Agencies |
| *Compliance Requirement* | Activities Allowed or Unallowed; Allowable Costs; Cash Management; Matching, Level of Effort, Earmarking; Period of Availability; Procurement and Suspension and Debarment; Program Income; and Reporting |

SIGNIFICANT DEFICIENCY – MATERIAL WEAKNESS

To help reduce the likelihood of unauthorized use of key computer resources, organizations restrict both logical and physical access to their computer systems, programs, and data. The level of access established must be commensurate to a specific user's current job responsibilities and needs, requested by an appropriate level of management, approved by system owners, implemented by designated security personnel, and periodically reviewed and validated by management. In a sound internal control environment, these security controls and restrictions would include, but not be limited to:

- Policies which identify the proper use of IDs and passwords and sanctions for misuse. Management must ensure employees are aware of the importance of maintaining individual IDs and the confidentiality of their passwords.
- Access rules which require passwords be a minimum number of characters in length, difficult to guess, contain no repeating characters, and changed periodically and provide for the suspension of user identification codes or the disability of the terminal, PC, or data entry device following a pre-defined number of unsuccessful attempts to access the system or applications.
- The use of a formalized access request form to document information about the employee and the access requested, and to provide a format for authorization by user and data processing management.
- Proper communication between departments when transferring or terminating employees and immediately upgrading or removing the electronic and physical access rights of users who have changed jobs or left the organization.
- Edit checks which promote the accuracy, completeness, and validity of data and provide for an appropriate separation of duties between incompatible functions.
- The use of security auditing tools to selectively record events for analysis and detection of security breaches. The audit data is typically recorded in log files and unique audit session ID called "audit tag" are generated and associated with the user's process.
- Environmental and physical control features (temperature controls, fire extinguishers/sprinklers, door locks, etc.) to protect the systems' hardware and data.

The State of Ohio implemented a new Enterprise Resource Planning (ERP) system called the Ohio Administrative Knowledge System (OAKS). This ERP system is used by the state to support administrative functions, such as finance (in the FIN module) and human resources (in the HCM module) for the state's agencies, boards, and commissions. The HCM module was implemented in January 2007 and the FIN module was implemented July 1, 2007. Functional responsibilities related to the OAKS HCM and FIN modules during the audit period were as follows:

- Accenture was the project contractor responsible for the administration, security, maintenance, and operations of the OAKS software.
- DAS provided the data processing center (with Internet services and utilities) that housed the OAKS production servers.
- OBM was responsible for the integrity of the FIN data and paying the State's obligations through OAKS via electronic fund transfers (EFT process).
- DAS was responsible for the integrity of the HCM data, the warrant writing facilities and related operations.

In state fiscal year 2008, as reported by the OAKS FIN general ledger, OAKS processed $58.9 billion in revenue and $50.1 billion in non-payroll expenditures, and HCM processed approximately $4.4 billion in payroll expenditures. These transactions included both state and federal funds for state agencies, departments, boards, commissions, and universities; 112 entities that processed revenue and 150 that processed expenditures. Although security features were built into the OAKS system, multiple control weaknesses that represented varying degrees of risk to the OAKS processing environment existed during fiscal year 2008. These weaknesses are presented below in two sections: material control deficiencies that pose the greatest risk to the security of the HCM and FIN processing environments; and other control deficiencies that, although individually pose less control risk, contribute significantly, in aggregate, to the overall risk of the OAKS security environment.

***MATERIAL CONTROL DEFICIENCIES***

- Password parameters were not set to OAKS standards for the UNIX servers that house the production OAKS programs and data for all 198 state and contractor user accounts as follows:

  - Accounts and passwords never expired.
  - Accounts did not lock out after a set number of invalid attempts.
  - Accounts were not disabled after a predetermined amount of terminal inactivity.
  - Passwords were not required to be reset after the account was re-opened.
  - Passwords were not required to be unique, which allowed previous passwords to be re-used.

- Of 60 tested FIN users sampled from a population of 13,740, five (projected to 1,145) were authorized by a CFO/Designee not listed on the authorized signatory listing. In addition, one of 60 users (projected to 229) had a form submitted with no CFO listed.

- There were 13 of 60 tested FIN users (projected to 3,000) who had additional roles not authorized on the User Security Access request form or the documentation which defined initial role assignments between OAKS and their home agencies.

- There were 72 unauthorized user accounts that could move FIN program code into production or could make changes directly to production program code.

- There were 22 unauthorized user accounts that could move HCM program code into production or could make changes directly into production code.

- Effective segregation of duties was not in place for 10 developer accounts that had access to make changes to the HCM production programs and also had access to move code into the HCM production environment.

- Three developer accounts had unauthorized access to the OAKS production databases.

- There were 95 user accounts with unauthorized access to one or more permission lists that allowed the ability to modify access roles in FIN. There was one system account that was erroneously shared by the security team with access to six permission lists in FIN. Additionally, there were 83 database administrators, six developers, and 14 contracted employees with access to add and modify user roles in FIN.

- 37 users either had UPDATE access instead of VIEW access to the FIN vendor database or had job duties that were questionable for requiring any logical access to the vendor database.

- One user had unauthorized access to post directly to the Actuals ledgers (production GL).

- Eight of 18 users had unauthorized access to update the FIN chartfields.

- Instead of being restricted to their own agency, 307 users had a security profile that allowed the user access to HCM data for *all* agencies within the State of Ohio. Fifteen of the 35 user accounts tested with this level of security did not have a corresponding security request form available for review and 23 had no authorizing signature.

- There is a corrections security privilege within the OAKS HCM module that allows modifications to existing employee payroll records and position data. There were 255 users with this privilege that no longer required that access.

- Five of 60 HCM users tested (projected to 278) were not included on the original approval spreadsheets for their agency submitted during the initial load and did not have an approved security access request form in place of the original approval. Of the 55 users who had access requests available, 50 (projected to 3,000) had access roles in HCM which were not authorized.

- Periodic access reviews of the user accounts with access to the HCM and/or FIN application modules in OAKS were not completed.

- Periodic access reviews of the Windows user accounts with access to the OAKS network were not completed.

- OAKS did not have formalized procedures that effectively addressed the termination of state or contracted personnel. Of the 5,810 employees terminated during the audit period, 381 had access roles in FIN that were not revoked and 23 had access roles in HCM that were not revoked.

***OTHER CONTROL DEFICIENCIES***

***<u>Security Management</u>***

- Eight of 30 (27%) employees tested did not have a signed non-disclosure agreement available and 12 (40%) did not have a signed acknowledgement of the OAKS workplace and IT policies.

- PeopleSoft security violation incident reports were not maintained to evidence that incidents were reviewed and addressed during the audit period.

- The login logs for the OAKS production servers did not track when users switched from using their own accounts to the OAKS superuser account. This information is important for monitoring use of the superuser account. The 16 logs tested from the four production servers were either not available or were missing various weeks of data.

***<u>Security Access Forms</u>***

- For four of the 60 HCM users tested, security access forms were not approved or completed properly. There was no pre-authorized list of supervisors authorized to submit access requests for each agency.

- There were multiple versions of the HCM access request form, and none contained a complete and accurate listing of assigned roles.

- 18 of the 30 Windows users tested did not have an IT access request form available to document authorization of access or the level of network access requested.

***Unauthorized Access***

- 48 users with access to the FIN development testing environment were unauthorized.

- 34 users with access to the FIN test production testing environment were unauthorized.

- 186 users with access to the HCM development testing environment were unauthorized.

- The OAKS QAS test environment was refreshed every two weeks with production data. This gave test personnel the ability to view production data that included personal employee information.

- One HCM developer with login access to three of the four production UNIX servers, and two FIN developers whose accounts were disabled, should have had their access removed.

- 11 user accounts had unauthorized access on the four OAKS production servers.

- There were 11 HCM accounts with the security administrator role that were loaded with the original PeopleSoft installation. Although the accounts were locked, users with the security administrator role (and SWAT2 role) had the capability to unlock the 11 accounts.

- Electronic access to the OAKS FIN, HCM, EPM (data warehouse environment), and CRM (Customer Relationship Management) data was controlled through the database servers. There were 35 users with access to the OAKS production databases that did not require the access as follows:

  - 17 users did not require access to the HCM production database.
  - 14 users did not require access to the FIN production database.
  - Three users did not require access to the EPM data warehouse.
  - One user did not require access to the CRM database.

- Logical access to the PeopleSoft automated batch scheduling software that scheduled all the batch jobs was administered through the batch administrator account. Eight OAKS batch team members (two state employees and six contractors) knew the password and used the batch administrator account. Additionally, the account had a password lifetime of 26 years and there was no evidence indicating the account password was changed during the audit period, even though employees with knowledge of the password were terminated during the audit period.

- When logged in to OAKS_HCM with a user who had row-level access for agency “A” and searching for an employee known to the application to work for agency “B”, OAKS did not allow the personal and job data for the employee at agency “B” to be accessed or modified. However, OAKS did allow changing the department in the position data screen to a department defined to agency “B” and subsequently allowed an employee from agency “A” to be assigned to a position at agency “B”.

- Combo codes indicate the account to be charged for various payroll expenditures (earnings, deductions, taxes, etc.) and multiple combo codes may be assigned for a given position. When attempting to manually enter a HCM combo code for agency “B” while logged in as an agency “A” user, the combo code was accepted.

***Physical Security***

We noted the following during testing of physical access controls at the main OAKS Project Management Office (PMO1):

- Of the 255 available access cards, 37 cards/slots did not match up from the key pad to the spreadsheet maintained to track the keycard access. Six cards were assigned to unauthorized users and two employees were assigned multiple cards.

- 12 of 25 users with access to the server room were unauthorized. In addition, because reports were unavailable, the ability to monitor server room access assignments was cumbersome and user access had to be reviewed one user at a time.

- A door leading into PMO1 from the State Library did not lock during business hours. Although a visitor sign-in sheet was maintained at the receptionist's desk, all visitors were not required to sign in to gain access to the building.

- Key network servers and hardware components were on the floor of the server room. In addition, humidity controls did not exist, resulting in severe mold on the wall and ceiling.

We noted the following during testing of physical access controls at the State of Ohio Computer Center (SOCC):

- OAKS production servers and tapes were not physically restricted from non-OAKS personnel. The OAKS servers were housed in cages, but the cages were not locked. In addition, OAKS data tapes were sitting against the wall unsecured.

- The computer room that houses the OAKS production servers also houses production servers owned and operated by other state agencies. Although a physical access reconciliation process was in place, 339 users had access cards to this computer room location.

- The DAS/OIT security department completed quarterly reconciliations with all participating agencies to validate physical access restrictions to the SOCC. No documentation in response to the reconciliation requests was available for three agencies (ODE, ODH, and DPS).

Sound IT security controls are imperative for ensuring only authorized personnel are processing OAKS FIN and HCM transactions. Without a combination of effective password and login controls in place, documented access authorities for all users, comprehensive and timely termination procedures, and regularly-scheduled reconciliations of defined user access rights, the risk could be significantly heightened that financial programs and data files would be purposely or accidently destroyed or corrupted. Misuse or misappropriation of material state and federal monies could occur as a result of unauthorized access to testing or production regions of OAKS.

In addition, a lack of adequate security violation and administrative account monitoring provides an even greater risk that fraudulent and accidental transactions could occur. Security breaches or unnecessary use of superuser accounts would also go undetected. Inadequate physical and environmental controls would contribute to the risk of unauthorized access to key hardware and software assets. Improper environmental controls could lead to the corruption of key data files and damage to equipment.

Several security weaknesses were the result of a lack of monitoring to ensure that control procedures were being consistently performed and the documentation evidencing performance of the control was maintained. Contributing factors include turnover and vacancies in several key OAKS management positions and heavy reliance on contract personnel. In addition, according to OAKS management, in some instances elevated access was granted to help ensure users had sufficient access to perform their jobs prior to and during the implementation phases of the OAKS system and was not subsequently reviewed and removed after OAKS was in production.

**Official's Response and Corrective Action Plan**

*There is no evidence provided that links these comments to potential material discrepancies in financial reporting. OAKS management began remediation efforts of all security comments as soon as they were known. At this point remediation has been completed on 19 of 21 security related SAS 70 comments.*

*We strongly disagree with the auditor's assertion that any material weakness existed with respect to this comment. The auditor has not disclosed testing to support findings of material weaknesses in the summarized comments. Without testing there is no basis for this determination.*

**Anticipated Completion Date for Corrective Action**

*Remediation has been completed on 19 comments and will be completed on the 2 (two) remaining comments by January 2010. OAKS management continues on a daily basis to monitor OAKS security.*

**Contact Person Responsible for Corrective Action**

*Darlene Wells, OAKS Program Manager, 30 W. Spring Street, Columbus, OH 43215, Phone: (614) 387-1891, E-Mail: darlene.wells@oaks.state.oh.us*

**Auditor of State's Conclusion**

We appreciate that OAKS management has begun remediation of 19 of the 21 comments described in the Auditor of State's SAS 70 report on OAKS, which we issued January 22, 2009. While we agree these deficiencies did not result in material misstatements, professional standards require us to categorize these deficiencies based on the *potential* for unauthorized transactions and/or program changes which could compromise the integrity of the financial reporting process.

The Official's statement above that "The auditor has not disclosed testing . . ." is incorrect. Our work papers include audit documentation to support all the statements we made above, which was part of the Auditor of State's SAS 70 report on the OAKS system. We can share our supporting evidence upon management's request.

## 2. INFORMATION TECHNOLOGY – OAKS RECONCILIATIONS

| | |
|---|---|
| *Finding Number* | 2008-OAKS02-005 |
| *CFDA Number and Title* | All Programs Administered by the State |
| *Federal Agency* | All Federal Agencies |
| *Compliance Requirement* | Activities Allowed or Unallowed; Allowable Costs; Cash Management; Matching, Level of Effort, Earmarking; Period of Availability; Procurement and Suspension and Debarment; Program Income; and Reporting |

SIGNIFICANT DEFICIENCY – MATERIAL WEAKNESS

When an effective automated accounting system processes transactions, controls are in place to help ensure these transactions are entered by authorized personnel. These detail transactions must be accepted, processed, validated, and posted in a controlled manner. The detail transactions must be completely and accurately processed and posted to a general ledger (GL) that fairly represents these detail transactions to allow accurate financial reporting to occur. Timely reconciliations of the control totals between the detail transactions and the summary totals in the GL provide an effective control to help ensure the integrity of the financial reporting from the GL.

During fiscal year 2008, the State of Ohio processed $58,914,962,687 in revenue and $54,487,730,121 in expenditures (comprised of $50,091,679,643 for non-payroll expenditures and $4,396,050,478 for payroll expenditures) using the Ohio Administrative Knowledge System (OAKS), which serves as the State's accounting system. However, controls were not in place in the OAKS software to reconcile the Financials (FIN) and Human Capital Management (HCM) module transaction totals to the totals reflected in the production GL, either on a monthly basis or at year end, nor was OAKS management aware if manual reconciliations were being performed by state personnel during the audit period between the GL and detail files. Although OBM management indicated they did perform cash reconciliations between the modules, GL and Treasurer of State, these procedures were not performed until after year end and were not part of our OAKS testing. Therefore, the auditor performed extensive manual reconciliation procedures and, after much difficulty and extensive investigation of many significant preliminary variances, determined there were no material variances between the GL and the detail transaction files.

While performing these procedures, we also noted the following issues that increased the likelihood of variances between the transactions and the GL. Although the amounts of the variances are not all significant, these issues identify areas were additional edits or other controls are warranted.

- The system allows transactions coded with expenditure account codes to be processed in the accounts receivable (AR) module and transactions coded with revenue account codes to be processed in the accounts payable (AP) module. Although AR transactions in the AP module would be acceptable if they were refunds, there was not an effective way to identify refund transactions. We identified 761 non-payroll expenditure transactions, totaling $28,554,770, in the AR module; and 286 revenue transactions totaling $827 in the AP module.
- The system does not have an edit to prevent identical journal IDs with different account codes from being used for corresponding transactions in the detail files and the GL journal tables. Such transactions were identified in the 2008 data (possibly the result of account code changes in the GL that were not also made to the original transaction).
- No edit is in place to require the agency (entered as Department ID) or fund be included in the data entered into the detail transaction in AR. Although such an edit is in place when transactions are posted to the GL, no corresponding adjustments are made to the AR transactions to include this missing information. We noted 85 AR transactions totaling $12 million that did not have an agency assigned to the transactions and 365,621 AR transactions totaling $55 billion with no fund. This did not impact the financial statements because the information was added at the GL level; however, the detail support did not reflect how this information was recorded.

- The system edits designed to prevent payroll and AP transactions from being entered without an agency were not functioning as intended. We noted 27,000 payroll transactions totaling $16 million and 181 AP transactions totaling $37,100 that did not have an agency assigned to the transaction.
- The miscellaneous revenue table in OAKS allowed transactions to have dollar amounts with three decimal places, causing rounding errors.
- Adjustments made to the GL for revenue, payroll and non-payroll expenditure Chartfields, were not retroactively changed in the original module (AR, AP, HCM). Because the GL adjustments were not linked to the original transaction, there was no way to determine if a transaction was modified or cancelled by looking at the transaction detail.
- Dates within OAKS were not always consistent; it was difficult to determine the appropriate date for a transaction, and there was not a formal guide to define the meaning and use of the available dates.

In addition to the OAKS FIN and HCM applications, the PeopleSoft Enterprise Performance Management (EPM) environment, referred to as the OAKS data warehouse, provided a repository of financial data extracted nightly from the OAKS production environment. This data warehouse was used by agency users and staff to query data and produce standard and customized financial reports for use by their respective agencies. Although not a mirror image of all the transactions in production, the data warehouse was designed to reflect a complete and accurate financial picture of the production GL and to provide for financial reporting from the data warehouse without disruption of the production environment's processes. However, no reconciliation of the production GL to the data warehouse totals and amounts occurred for fiscal year 2008 in order to ensure the integrity of the financial information from the EPM and the custom reports produced from it by the agency users.

If the integrity of the detail transaction data is compromised, the financial reporting that comes from the corresponding general ledgers is susceptible to error. Questionable general ledger data increases the risk that the State's financial condition may be misrepresented. This would impact the integrity of the State of Ohio's Comprehensive Annual Financial Report, a key document relied on by many external entities. In addition, the integrity of any financial reporting originating from the data warehouse could be jeopardized if the data warehouse control totals are not routinely reconciled to the production GL.

According to OAKS and OBM management, automated control procedures were not designed in PeopleSoft during fiscal year 2008 to reconcile the OAKS detail transaction control totals to the production GL control totals. Since management's emphasis was to meet the July 1, 2007 deadline to get FIN into production, these automated or any compensating manual controls were not a priority to design and implement. Production GL to data warehouse reconciliations were designed and implemented, but were inadequate and operated for only a part of the audit period. Management indicated it was not a priority to address these issues during the fiscal year.

The edits that required chartfields such as fund and department were not originally built into the purchased software. Although the edits were planned to be implemented into the customized software, OAKS management did not have time to design and implement them before FIN went into production. Subsequent coding corrections in the GL were not required to be automatically synchronized or manually changed in the respective OAKS modules. OAKS management could not explain why some journal entries entered in the GL had no corresponding entry in the OAKS modules. OBM management indicated the majority of these items related to corrections for errors made by state agencies as they were adapting to this new system.

We recommend OAKS management implement automated and/or manual controls to provide month-end and year-end reconciliations between the detail HCM and FIN transaction totals and the corresponding production GL summary totals. We also recommend timely reconciliation procedures be implemented to ensure the continual agreement of production GL totals to the corresponding data warehouse totals. Any significant variances identified as part of these reconciliation procedures should be investigated and any required adjustments resulting from this process thoroughly documented and approved by an appropriate level of management. Support documentation of the reconciliations should be maintained for at least one audit cycle.

In addition, to help eliminate potential variances in amounts between the detail transaction files and the GL, we recommend:

- Edits be enhanced to help ensure all OAKS agency transaction data is entered completely and accurately according to DAS and OBM specifications. This should include a control to ensure a required field, such as agency or fund, is not left blank.
- Transactions are only entered into the correct OAKS modules.
- Edits be implemented to ensure identical journal IDs in the transaction files and GL also have identical account codes.
- Adjustments made directly to the GL are also applied to the OAKS module where the transaction originated.
- Transaction amounts are accepted throughout OAKS with a consistent number of decimal places.
- All dates are consistently applied throughout OAKS and documentation to explain the various dates in OAKS is readily available.

**Official's Response and Corrective Action Plan**

*As mentioned in the Auditors report, The FIN module, which is the primary source of the State's financial transactions, was implemented on July 1, 2007 and was utilized in totality for the first time in preparing the fiscal year 2008 financial statements. Planning and development efforts for the new enterprise wide system began in 2001 under the Taft Administration and were finally implemented in 2007.*

*In FY 2009 OBM created the Data Integrity Group within State Accounting to address the reconciliation, validation and control requirements of the OAKS system. When fully staffed, the department will contain four individuals with the accounting, analysis, auditing and technical skills to develop and implement the appropriate validation methodologies.*

*Subsequent to go live, OBM also identified many of the same issues as the auditor and has initiated corrective actions, many of which, are complete or well under way. Although the discrepancies noted by the auditor are insignificant, OBM strongly supports data accuracy and integrity and has placed a priority on this effort. Below are specific responses to the individual items addressed in the auditors comment:*

- *For FY 2008 year end, reconciliations were performed as a manual control mitigating the risk of a lack of system controls that were not in place in the OAKS software throughout FY 2008. The mitigating control, cash reconciliation, included three sources of information drawn from (1) the OAKS general ledger, (2) detail queries for OAKS detail posted in the A/R and A/P sub-modules within OAKS and (3) the Treasurer of State published record of Revenue, Disbursements and Cash Balance. Monthly system balancing has been in effect since July 2009. As suggested by the auditor, this is a control balancing of OAKS detail transactions by source of origin to the General Ledger account balances for all balance sheet accounts and total revenue and expense account categories. This is a high level data integrity reconciliation of general ledger balances to sub module postings of A/R, A/P, HCM, and JRN (misc journal corrections) by journal entry and date.*

- *There are a finite number of non-payroll journal entries that bypass the sub ledgers and post directly to the OAKS general ledger. All of these are reviewed and posted by OBM. These occur for error corrections and reclassification of large subsidy payments where reversal and correction through the sub-modules is impractical. These are being logged and reviewed by OBM State Accounting. These are reviewed with the agency for root cause and corrective actions developed which will further limit this activity.*

- *A system edit is currently in test mode which restricts expenditure accounts in the A/R module and revenue accounts in the A/P module as appropriate.*

- *Identical journal ID's are used in the sub-modules and G/L in certain cases to provide a cross reference when corrections are made in the G/L. Although the ID is the same, the journals are unique by virtue of association with the system date and time stamp. This is delivered PeopleSoft functionality which would require a custom code update. We do not agree that this is necessary. We will communicate to users to append a letter to the original ID to create a more unique journal ID.*

- *An enhancement request to require business unit and fund when entering transactions in A/R was prepared shortly after go live. Since the change would require thousands of development hours it was shelved due to many competing priorities in the post go live environment. OBM has revisited this request and it is being costed out in the new managed services environment.*

- *HCM payroll entries are occasionally interfaced to OAKS without appropriate combo edit codes. This occurs because HCM went live prior to FIN and HCM was programmed initially to interface into CAS, a non PeopleSoft application. When the system integration is properly configured HCM and FIN share common chart field values so that interfacing entries are validated prior to entering the GL. The OAKS Quality Assurance team is working with Oracle to determine the size of this remediation effort. We anticipate having this completed prior to the close of FY10.*

- *Three decimal places is a standard delivered configuration of PeopleSoft. To change to the recommended two would require significant custom coding. OBM does not believe this is a prudent strategy or an effective use of limited resources.*

- *There are several dates within PeopleSoft for financial transactions. The Data Integrity Group is actively working to understand these in connection with their reconciliation activity in establishing cutoff dates between the modules and G/L. Once a firm understanding is confirmed it will be communicate throughout the OAKs community.*

**Anticipated Completion Date for Corrective Action**

*Various, all completed by end of FY 2010.*

**Contact Person Responsible for Corrective Action**

*Tom Holsinger, Deputy Director Accounting Administration, Office of Budget and Management, 30 E Broad St., Columbus, OH 43215, Phone: (614) 728-4734, e-mail: tom.holsinger@obm.state.oh.us*

### 3. INFORMATION TECHNOLOGY – LACK OF PROGRAM CHANGE CONTROLS IN OAKS

| | |
|---|---|
| *Finding Number* | 2008-OAKS03-006 |
| *CFDA Number and Title* | All Programs Administered by the State |
| *Federal Agency* | All Federal Agencies |
| *Compliance Requirement* | Activities Allowed or Unallowed, Allowable Costs, Reporting |

**SIGNIFICANT DEFICIENCY**

In order to minimize the corruption of information systems and help ensure automated applications are performing as management intended, strict controls must be in place to guide program modifications during the entire program change life cycle. In a sound internal control environment, these program change controls and restrictions would include, but not be limited to, the following control procedures:

- All program change requests are documented, initiated by authorized users, prioritized, assigned, and approved by the proper user and IT authorities during key control points of the program change life cycle. All key program change documentation is maintained according to published program change policies and standards.
- Documentation of all test plans and test results for program changes must be maintained along with evidence of user and IT acceptance of those results.
- Access to test regions must be restricted to authorized programmers and/or developers. A secure test region is designed and established to be representative of the planned operations environment relative to security, internal control, operational practices, data quality, and privacy requirements.
- Sensitive production data that must be used in the test environment is masked or sanitized to prevent IT personnel from unnecessarily viewing personal information. If sanitizing the test data prevents effective testing, the sensitive data must be sanitized or deleted immediately following successful testing and documentation.
- All tested programs must be approved before the final migration into the production environment. Documentation of that approval must be maintained.
- Program changes must be documented to be clear and meaningful to facilitate effective application modifications from subsequent programmers.

In state fiscal year 2008, as reported by the OAKS FIN general ledger, OAKS processed $58.9 billion in revenue and $50.1 billion in non-payroll expenditures, and HCM processed approximately $4.4 billion in payroll expenditures. The change process for the OAKS FIN and HCM application modules is largely controlled through automated change control software tools. Authorized programming staff members are required to formally indicate, through the use of these tools, when all tests, reviews, and approvals have been completed. After receipt of formal authorization, staff members independent of the programming staff move programs into production. As noted by the exceptions identified below, program change controls were not consistently performed:

- Six (15%) of the 39 tested HCM change requests and one (3%) of the tested 38 HCM System Investigation Requests (SIR) change requests were not authorized by OAKS management to complete the requested program change.
- 19 of the 39 (49%) HCM tested change requests did not have programmers assigned to the requests.
- Both testing and pre-migration approvals were not documented for four HCM maintenance packs prior to placing these changes in production.
- Test documentation was not available for any of the 23 FIN or 37 HCM changes tested.
- Eight of 23 selected FIN program changes and eight of 57 selected HCM program changes did not have corresponding updated technical documentation.

In addition, the OAKS test and development servers under the control of Accenture were housed at a Cincinnati area data center. These OAKS FIN and HCM testing environments were populated with live production data. The data contained sensitive information about all state employees, including salaries, social security numbers, bank account numbers, and dependent information. The personal information in the data was not sanitized or masked. The Mercury ITG software used by OAKS provided tracking and monitoring of application changes and a feature to mask and sanitize data used for the testing environment; however, this feature was not used. As a result, any user with access to the test environment could view employees' personal information.

If standardized procedures for modifying application programs, maintaining testing documentation, and migrating changed and approved programs into production are not followed, unauthorized, incomplete, or untested program changes could be placed in production. The lack of adequate test documentation and program change comment cross referencing may increase the cost and time burden to the State for future program modifications because an information systems professional who is unfamiliar with the programs would not have current information to obtain an understanding of the changes to applications. In addition, it may be impossible to duplicate or evaluate testing scenarios in the event that problems arise later that require subsequent review of the program changes. These control weaknesses could adversely affect the State's ability to effectively modify the programs that process state revenue and expenditure transactions.

Additionally, by using actual production data in the testing environment, any user with access to the testing environment could access sensitive data and use this information for fraudulent activities or personal gain.

According to OAKS management, because many of the project assignments were pre-determined, documenting these assignments was overlooked. Approvals of the program changes were completed; however, not all of the approval documentation could be located at the time of the audit. OAKS management also indicated the HCM maintenance pack changes with missing required testing and pre-migration approvals had e-mail notifications that testing was completed and approved; however, the related e-mails could not be located at the time of the audit. Management noted that all of the HCM and FIN program changes identified with missing change documentation were due to oversight by the programmers making the changes.

In addition, OAKS management said they were refreshing the test environments with live data so that developers would be able to test scenarios similar to production and that it would take a significant effort to mask the data; however, OAKS management has been looking into methods to mask sensitive data in the development and test environments. At this time, there were no plans to mask data in the QAS environments due to the need to perform root cause analysis.

We recommend OAKS management:

- Complete the change request forms in their entirety as program change work progresses from project submission to the final documentation and training stages. This includes ensuring all key user acceptance and IT approvals required on the form are documented.
- Follow established program change documentation standards to reasonably ensure all necessary test plans and corresponding results for all program changes are maintained.
- Follow established program change documentation standards to reasonably ensure technical and user documentation is provided and maintained.

Additionally, all production data used in the testing environment should be sanitized or masked, whenever possible, to prevent the compromise of sensitive employee information. If sanitizing the test data prevents effective testing, the sensitive data should be sanitized, masked, or deleted immediately following successful testing and documentation.

**Official's Response and Corrective Action Plan**

*There is no evidence provided that links these comments to potential material discrepancies in financial reporting. OAKS management began corrective planning and remediation efforts of all application and hardware control comments as soon as they were known. At this point remediation has been completed on 5 (five) of these comments and remediation of the remaining comment is projected to be completed by January 2010.*

*We strongly disagree with the auditor's assertion that any significant deficiency existed with respect to this comment. The auditor has not disclosed testing to support findings of material weaknesses in the summarized comments. Without testing there is no basis for this determination.*

**Anticipated Completion Date for Corrective Action**

*Remediation has been completed for 5 of the 6 comments contained in the SAS 70 audit. OAKS management continues to remediate the remaining item, with a projected completion date of January 2010.*

**Contact Person Responsible for Corrective Action**

*Darlene Wells, OAKS Program Manager, 30 W. Spring Street, Columbus, OH 43215, Phone: (614) 387-1891, E-Mail: darlene.wells@oaks.state.oh.us*

**Auditor of State's Conclusion**

We appreciate that OAKS management has begun remediation of the comments described above. While we agree these deficiencies did not result in material misstatements, professional standards require us to categorize these deficiencies based on the *potential* for unauthorized or inappropriate program changes which could compromise the integrity of the financial reporting process. The Official's statement above that "The auditor has not disclosed testing . . ." is incorrect. Our work papers include audit documentation to support all the statements we made above, which was part of the Auditor of State's SAS 70 report on the OAKS system, dated January 22, 2009. We can share our supporting evidence upon management's request.

## 4. INFORMATION TECHNOLOGY – OAKS REQUISITIONS & CHARTFIELD MAINTENANCE CONTROLS

| | |
|---|---|
| *Finding Number* | 2008-OAKS04-007 |
| *CFDA Number and Title* | All Programs Administered by the State |
| *Federal Agency* | All Federal Agencies |
| *Compliance Requirement* | Activities Allowed or Unallowed, Allowable Costs, Procurement, Reporting |

**SIGNIFICANT DEFICIENCY**

To reduce the risk of loss due to error or misuse of state and federal resources, controls over the purchasing process typically require approval for purchase of goods and services by someone independent of the person requesting the goods or services. Similarly, when changes must be made to important standing data that will impact multiple transactions, the changes must be approved by an authorized individual and documented.

The State of Ohio uses the OAKS FIN application module to process all revenue and expenditures for each state agency. During fiscal year 2008, the State of Ohio processed $58,914,962,687 in revenue and $50,091,679,643 in non-payroll expenditures using OAKS, which serves as the State's accounting system. The OAKS system uses a workflow process which allows for multiple levels of approval for electronic requisitions and subsequent purchase orders. A FIN user with both the ability to create and submit a requisition (requisitioner security role) and the final approver role (level 4) within OAKS security could create and approve their own requisition/purchase order. As of May 2008, 268 users were granted this access within OAKS FIN. In addition, there were 700 requisitions within the FIN module from 25 different agencies where the creator and approver of the requisition was the same user, for a total dollar amount of $180,192,618.

Also, OAKS General Ledger defines the financial structure of each organization by combining separate and distinct fields called Chartfields. OAKS uses Chartfields to classify the State's Chart of Accounts for financial reporting. OBM creates and/or modifies Chartfield accounts (department, program, grant/project, project, service location, reporting, agency use, and budget reference) based on Chartfield Change Request forms that are submitted by state agencies. OBM management was responsible for the maintenance of other Chartfields related to the Fund, Account, ALI, and ISTV XREF, and any changes were initiated by OBM personnel. There were 795 changes made to the Fund, Account, ALI, and ISTV XREF Chartfields during fiscal year 2008. However, documentation of these changes was not maintained during the audit period, and a full review of the Chartfields was not performed. In addition, OBM did not maintain a list of authorized agency approvers for the Chartfield Change Request forms. We tested a sample of 60 of 8,913 Chartfields that were added or modified based on agency requests during the audit period and noted the following:

- 24 of 60 changes (40%) did not have a change request form or other documentation available; therefore, we could not determine whether the changes were approved or accurately input into OAKS.
- Of the 36 change request forms available for testing, 16 (44%) were not approved by an authorized agency representative.
- For two of the 36 Chartfield changes input into OAKS, the data in the system was not supported by the available documentation. In one instance the user asked for the program value to be inactivated as of 7/1/08; however it was not actually inactivated until 7/28/08. In the second instance, the request to inactivate the program value was not made. According to OAKS personnel, the agency verbally requested the change request be disregarded, but did not send a formal retraction and no other documentation was maintained.

Without the proper segregation of duties within an organization, there is an increased risk that unauthorized or incorrect purchases are being made. This could result in the misuse of state and federal monies. Finally, if proper change control procedures are not practiced for Chartfield maintenance, there is an increased risk that unauthorized or incorrect Chartfield changes could be made and impact the classification of transactions entered into the OAKS FIN module.

DAS FIN management indicated the system was designed to prevent a user from approving a requisition they created and entered; however, it was not functioning properly during the audit period. OBM management indicated that many of the Chartfields were converted from CAS values when OAKS was developed and because this was a mass-change task, individual documentation was not maintained. If a modification was made to the description or short description, a form was not always completed due to the modification not affecting the Chartfield value. Additionally, due to time constraints, many modifications were requested via e-mail, and the e-mail documentation was not always maintained.

We recommend OAKS FIN management implement changes to ensure that users are restricted from creating and approving their own requisition/purchase order. When exceptions must occur, an additional subsequent approval should be required. Management should also ensure that proper segregation of duties is enforced throughout the FIN system. In addition, management should query all purchase orders and vouchers dispersed during the audit period to identify any expense transactions that were submitted and approved by the same individual. These transactions should then be given to the agencies and/or the State's Office of Internal Audit for review to ensure the amounts dispersed were authorized and allowable.

We also recommend OBM management ensure the Chartfield Change Request forms received from the agencies are completed in their entirety and any related support documentation is maintained prior to processing the requested change. A list of personnel authorized to submit the request forms should be established, periodically reconciled with the agencies, and readily available to all OBM maintenance personnel. Procedures should also be established and implemented for the documentation of changes to the Fund, Account, ALI, ISTV and XREF Chartfields made by OBM without the formal request of an agency. Lastly, a full review and confirmation of the current Chartfields should be performed to validate the existing values are correct and authorized by the user agencies.

**Official's Response and Corrective Action Plan**

*There is no evidence provided that links these comments to potential material discrepancies in financial reporting. OAKS management began corrective planning and remediation efforts of all requisitions and chartfield maintenance comments as soon as they were known. At this point remediation has been completed on both these comments.*

*We strongly disagree with the auditor's assertion that any significant deficiency existed with respect to this comment. The auditor has not disclosed testing to support findings of material weaknesses in the summarized comments. Without testing there is no basis for this determination.*

**Anticipated Completion Date for Corrective Action**

*Remediation efforts have been completed on this comment. OAKS management continues to monitor requisition and chartfield maintenance requirements.*

***Contact Person Responsible for Corrective Action***

*Darlene Wells, OAKS Program Manager, 30 W. Spring Street, Columbus, OH 43215, Phone: (614) 387-1891, E-Mail: darlene.wells@oaks.state.oh.us*

**Auditor of State's Conclusion**

We appreciate that OAKS management has begun remediation of the comments described above. While we agree these deficiencies did not result in material misstatements, professional standards require us to categorize these deficiencies based on the *potential* for unauthorized or inappropriate purchases or program changes which could compromise the integrity of the financial reporting process.

The Official's statement above that "The auditor has not disclosed testing . . ." is incorrect. Our work papers include audit documentation to support all the statements we made above, which was part of the Auditor of State's SAS 70 report on the OAKS system, dated January 22, 2009. We can share our supporting evidence upon management's request.

## 1. CASH MANAGEMENT – INTEREST DISTRIBUTION

| | |
|---|---|
| *Finding Number* | 2008-OBM01-008 |
| *CFDA Number and Title* | Various |
| *Federal Agency* | Various |
| *Compliance Requirement* | Cash Management |

<u>NONCOMPLIANCE AND SIGNIFICANT DEFICIENCY</u>

31 CFR 205.19 states, in part:

> (c) A State must calculate and report interest liabilities on the basis of its fiscal year. A state must ensure that its interest calculation is auditable and retain a record of the calculations.
>
> . . .

It is imperative management establish policies and procedures which provide reasonable assurance the interest calculation and distribution is accurate and complete and provide for the effective management of records to reasonably ensure appropriate supporting documentation is maintained for all amounts calculated, allocated, and disbursed, and to support the decisions made in all aspects of the process.

In order to determine the amount of interest to be distributed to each state fund, including those that have federal activity ("federal funds"), the Office of Budget and Management (OBM) prepares an interest distribution spreadsheet quarterly. After this determination, the State credits the state funds, including applicable federal funds, with their respective share of investment earnings. The earnings for the federal funds are then immediately transferred from each federal fund to the Cash Management Improvement Fund. Annually, the State reimburses the federal government with their share of the interest earnings on the federal funds from the Cash Management Improvement Fund. The State's interest earnings liability to the federal government for state fiscal year 2008 totaled $2,466,256. OBM was unable to provide support documentation for each of the federal funds' average daily cash balance from each quarter of SFY 2008 recorded in the interest distribution spreadsheet. Additionally, the amount of interest to be distributed to each federal fund was not identified in the spreadsheet. Therefore, we were unable to determine if the amount of interest distributed to the federal funds was complete and accurate. Costs were not questioned, however, because the disbursement of funds to the federal government based on this information did not occur until March 2009, subsequent to our audit period.

Without maintaining the proper support documentation, the State may not be able to fully support or ensure compliance with federal laws and regulations. Lack of compliance could result in questioned costs, fines, and/or penalties. Management indicated the individual responsible for preparing the fiscal year 2008 spreadsheet was no longer employed with the agency and the support documentation could not be located.

We recommend OBM management review current policies and procedures related to investment earnings. Policies and procedures should be updated/implemented as necessary to reasonably ensure appropriate documentation is maintained to support all interest calculations and distributions, and include procedures to ensure all appropriate documentation is obtained from departing employees. We recommend management communicate its policies and procedures to staff to ensure they are carried out as intended. In addition, management should perform periodic reviews of the investment earnings spreadsheet to ensure controls and record retention procedures are being followed by OBM personnel. With regard to the specific payment made in March 2009, we recommend OBM try to locate the documentation related to the calculations related to the interest distributions or otherwise substantiate the amounts to avoid a questioned cost in the fiscal year 2009 audit.

**Official's Response and Corrective Action Plan**

*The interest allocation process for FY2008 was based on a manually prepared spreadsheet. With regard to the specific payment made in March 2009, OBM has located the documentation related to the calculations related to the interest distributions or otherwise substantiate the payment amounts to avoid a questioned cost in the fiscal year 2009 audit.*

**Anticipated Completion Date for Corrective Action**

*Effective with FY 2009 beginning 7/1/08, a new OAKS base interest allocation module was implemented. This is an automated system based on daily fund balances contained in the OAKS system. The system calculates interest transfers and systematically prepares the journal entry posting. Once reviewed, the interest is posted.*

*We believe that the new system has the necessary controls and audit trail features.*

**Contact Person Responsible for Corrective Action**

*Tom Holsinger, Deputy Director Accounting Administration, Office of Budget and Management, 30 E Broad St., Columbus, OH 43215, Phone: (614) 728-4734, e-mail: tom.holsinger@obm.state.oh.us*

# Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

## Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

## Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

## Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

## Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

## Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.