

**GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL**

DISTRICT OF COLUMBIA

**MEMORANDUM OF
RECOMMENDATIONS
FISCAL YEAR 2008**



**CHARLES J. WILLOUGHBY
INSPECTOR GENERAL**

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



April 9, 2009

The Honorable Adrian M. Fenty
Mayor
District of Columbia
John A. Wilson Building
Mayor's Correspondence Unit, Suite 316
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

The Honorable Vincent C. Gray
Chairman
Council of the District of Columbia
John A. Wilson Building
1350 Pennsylvania Avenue, N.W., Suite 504
Washington, D.C. 20004

Natwar M. Gandhi, PhD.
Chief Financial Officer
Office of the Chief Financial Officer
John A. Wilson Building
1350 Pennsylvania Avenue, N.W., Suite 203
Washington, D.C. 20004

Dear Mayor Fenty, Chairman Gray, and Dr. Gandhi:

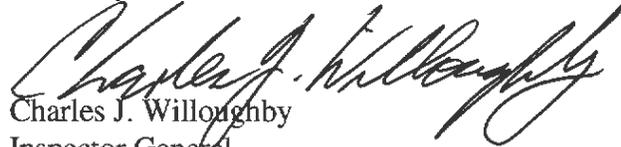
In connection with the audit of the District of Columbia's general purpose financial statements for fiscal year (FY) 2008, BDO Seidman, LLP (BDO) submitted the enclosed final Memorandum of Recommendations, in previous years known as the Management Letter. This report details certain control deficiencies that require continued management attention. In this regard, BDO Seidman, LLP set forth suggestions for improving existing internal controls. BDO did not consider these matters to be significant deficiencies or material weaknesses. Furthermore, these matters did not affect the fair presentation of the financial statements.

Mayor Fenty, Chairman Gray, and Dr. Gandhi
Issuance of FY 2008 Memorandum of Recommendations
OIG No. 09-1-22MA – Final Report
April 9, 2009
Page 2 of 4

While the Office of the Inspector General will continue to assess the District's implementation of recommendations, it is the responsibility of District government management to ensure that agencies correct the deficiencies noted in audit reports. This Office will work with managers, as appropriate, to help them monitor the implementation of recommendations.

If you have questions or need additional information, please contact William J. DiVello, Assistant Inspector General for Audit, or me at (202) 727-2540.

Sincerely,



Charles J. Willoughby
Inspector General

Enclosure

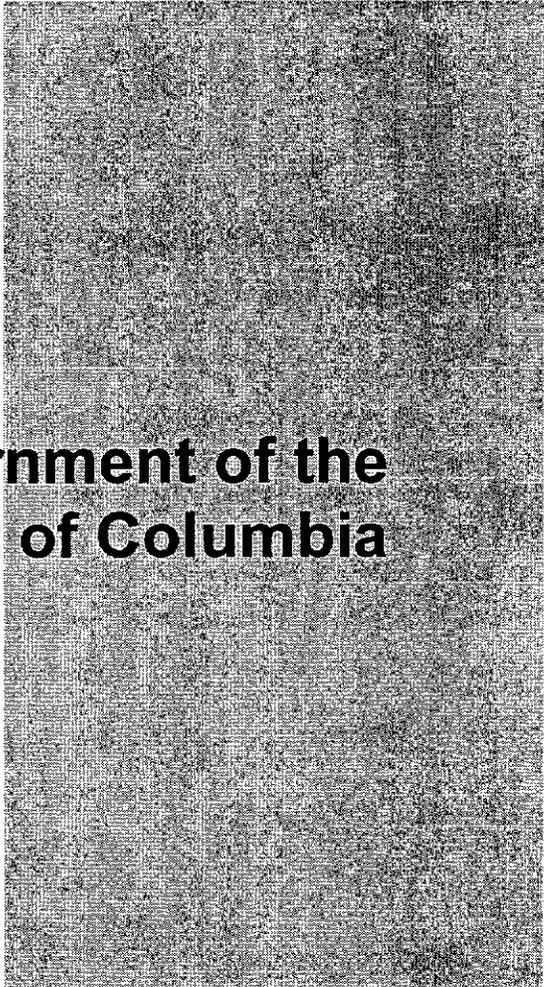
CJW/ad

cc: See Distribution List

DISTRIBUTION:

Mr. Daniel M. Tangherlini, City Administrator and Deputy Mayor, District of Columbia (1 copy)
Mr. Neil O. Albert, Deputy Mayor for Planning and Economic Development (1 copy)
The Honorable Vincent C. Gray, Chairman, Council of the District of Columbia (1 copy)
The Honorable Mary M. Cheh, Chairperson, Committee on Government Operations and the Environment, Council of the District of Columbia (1 copy)
Mr. Andrew T. Richardson, III, General Counsel to the Mayor (1 copy)
Ms. Carrie Kohns, Chief of Staff, Office of the Mayor (1 copy)
Ms. Bridget Davis, Director, Office of Policy and Legislative Affairs (1 copy)
Ms. Mafara Hobson, Director, Office of Communications (1 copy)
Mr. William Singer, Chief of Budget Execution, Office of the City Administrator (1 copy)
Ms. Cynthia Brock-Smith, Secretary to the Council (13 copies)
Mr. Peter Nickles, Attorney General for the District of Columbia (1 copy)
Dr. Natwar M. Gandhi, Chief Financial Officer (4 copies)
Mr. Robert Andary, Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (1 copy)
Ms. Deborah K. Nichols, D.C. Auditor (1 copy)
Ms. Kelly Valentine, Director and Chief Risk Officer, Office of Risk Management (1 copy)
Ms. Jeanette M. Franzel, Managing Director, FMA, GAO, Attention: Sandra Silzer (1 copy)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives, Attention: Bradley Truding (1 copy)
The Honorable Edolphus Towns, Chairman, House Committee on Oversight and Government Reform, Attention: Ron Stroman (1 copy)
The Honorable Darrell Issa, Ranking Member, House Committee on Oversight and Government Reform (1 copy)
The Honorable Stephen F. Lynch, Chairman, House Subcommittee on the Federal Workforce, Postal Service, and the District of Columbia, Attention: William Miles (1 copy)
The Honorable Jason Chaffetz, Ranking Member, House Subcommittee on the Federal Workforce, Postal Service, and the District of Columbia (1 copy)
The Honorable Joseph Lieberman, Chairman, Senate Committee on Homeland Security and Governmental Affairs, Attention: Holly Idelson (1 copy)
The Honorable Susan Collins, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs (1 copy)
The Honorable Daniel K. Akaka, Chairman, Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (1 copy)
The Honorable George Voinovich, Acting Ranking Member, Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (1 copy)

The Honorable David Obey, Chairman, House Committee on Appropriations,
Attention: Beverly Pheto (1 copy)
The Honorable Jerry Lewis, Ranking Member, House Committee on Appropriations (1 copy)
The Honorable José E. Serrano, Chairman, House Subcommittee on Financial Services and
General Government, Attention: Dale Oak (1 copy)
The Honorable Jo Ann Emerson, Ranking Member, House Subcommittee on Financial
Services and General Government (1 copy)
The Honorable Daniel K. Inouye, Chairman, Senate Committee on Appropriations,
Attention: Charles Houy (1 copy)
The Honorable Thad Cochran, Ranking Member, Senate Committee on Appropriations (1 copy)
The Honorable Richard Durbin, Chairman, Senate Subcommittee on Financial Services and
General Government (1 copy)
The Honorable Sam Brownback, Ranking Member, Senate Subcommittee on Financial
Services and General Government (1 copy)
Mr. William D. Eisig, CPA, Partner (Assurance), BDO Seidman, LLP (1 copy)



**Government of the
District of Columbia**

**Memorandum of Recommendations
Year Ended September 30, 2008**

Government of the District of Columbia

Contents

Introductory Letter	1
City Wide Observations	
<i>Processes</i>	
General District Administration	3
Cash and Investments	5
Revenue Generation and Collection	9
Compensation	17
Management of Grants	30
Disbursements	33
Management of the Disability Compensation Program	40
Fixed Assets	45
Management of the Postretirement Health and Life Insurance Trust	49
Management of the Medicaid Program	51
Health Care Safety Net	53
Budget and Planning	55
Inventory	58
Journal Entries	59
<i>Information Technology Environment</i>	
General Controls	60
Treasury Functions	72
Revenue Generation and Collection	78
Status of Prior Year Observations	80



March 31, 2009

To the Mayor and the Council of the Government of the District of Columbia, Inspector
General of the Government of the District of Columbia, and Management of the
Government of the District of Columbia

During the course of our audit of the financial statements of the **Government of the District of Columbia** (the District) for the year ended September 30, 2008, we observed the District's significant accounting policies and procedures and certain business, financial, and administrative practices.

In planning and performing our audit of the financial statements of the District as of and for the year ended September 30, 2008, in accordance with auditing standards generally accepted in the United States of America, we considered the District's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the District's internal control. Accordingly, we do not express an opinion on the effectiveness of the District's internal control.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the District's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the District's financial statements that is more than inconsequential will not be prevented or detected by the District's internal control. A material weakness is a significant deficiency or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the District's internal control.

Our consideration of internal control was for the limited purpose described in the second paragraph of this letter and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses.

We have prepared the following suggestions for improving existing internal controls. We did not consider these matters to be significant deficiencies or material weaknesses. Furthermore, they did not affect the fair presentation of the financial statements.

This report does not extend to the following entities or funds as their financial statements were audited separately:

- District of Columbia 529 College Savings Program.
- District of Columbia Housing Finance Agency.
- District of Columbia Police Officers and Firefighters' Retirement Fund.
- District of Columbia Teachers' Retirement Fund.
- District of Columbia Nursing Homes.
- District of Columbia Water and Sewer Authority.

The following entities or funds each receive separate reports; therefore, observations involving these entities or funds are also not included in this document.



- District of Columbia Tobacco Settlement Financing Corporation.
- University of the District of Columbia.
- Washington Convention Center Authority.
- District of Columbia Public Schools.
- District of Columbia Lottery and Charitable Games Control Board.
- District of Columbia Unemployment Compensation Fund.
- Sports and Entertainment Commission.
- Home Purchase Assistance Program.

Deficiencies in internal control that we considered to be significant deficiencies or material weaknesses, as defined above, are discussed in a separate report. We refer the Mayor, Council, and Inspector General to the *Independent Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with Government Auditing Standards*. This report, dated January 30, 2009, describes in greater detail the following material weaknesses, significant deficiencies, and material noncompliance with laws and regulations as noted for the year ended September 30, 2008:

Material Weaknesses

- Treasury Functions.
- Management of Medicaid Program.

Significant Deficiencies

- Compensation.
- Office of Tax & Revenue.
- District of Columbia Public Schools.
- Management of the Postretirement Health and Life Insurance Trust.

Material Noncompliance with Laws and Regulations

- Noncompliance with Procurement Regulations.
- Noncompliance with the Quick Payment Act.
- Noncompliance with the Financial Institutions Deposit and Investment Amendment Act.
- Expenditures in Excess of Budgetary Authority.

This report is intended solely for the information and use of the Mayor, the Council, the Inspector General of the District, management of the District, and others within the District government and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

BDO Seidman, LLP

BDO SEIDMAN, LLP

City Wide Observations

Process: General District Administration

Policies and Procedures Manual

We noted that the existing accounting procedures manual in use has not been updated for several years. This can lead to misunderstandings, errors, inefficient or wasted effort, duplicated or omitted procedures, and other situations that can result in inaccurate or untimely accounting records.

While management has begun the process of updating its manual, it has not yet been completed. A well-devised accounting manual can help to ensure that similar transactions are treated consistently, that accounting principles used are proper, and that records are produced in the form desired by management. A good accounting manual also aids in the training of new employees and possibly allows for delegation to other employees of some of accounting functions management performs.

All changes in the accounting procedures manual, as well as existing internal controls, should be documented and communicated on a regular basis to all concerned persons. Internal controls cannot work unless employees are aware of them. Further, a policy should be established for the manual's regularly scheduled review and update.

Management's Response:

The Office of the Chief Financial Officer (OCFO) has reconstituted the Financial Policies and Procedures Division within the Office of Financial Operations and Systems. The new Director of this division has already gathered the necessary information to assess the current status of the financial policies and procedures on a District-wide basis and has identified the level of work needed to develop, enhance, update and revise the District-Wide Financial Policies and Procedures Manuals. Through group discussions and one-on-one meetings with District staff, the Director gained an understanding of the current process in place and has begun an effective and efficient approach to develop more comprehensive financial policies and procedures manuals for the District of Columbia Government.

In establishing this comprehensive approach to policies and procedures development, the Financial Policies and Procedures Director established a matrix which identified the sectional/modular breakdown for the new comprehensive financial policies and procedures manuals; formed project teams (cross section of OCFO Central, Associate Chief Financial Officer (ACFO) Clusters, and Agency personnel) directed by the Financial Policies and Procedures Division; gathered an inventory of tasks with the required documentation to facilitate the development of new procedures and update existing ones; and defined the primary and secondary levels of responsibility for the preparation and review of the enhanced, updated, and revised comprehensive financial policies and procedures manuals.

This comprehensive approach will target the following three principal areas: (1) District-Wide – Central Offices; (2) Across-the-Board Operations (Associate Chief Financial Officers (ACFO) and Operations Clusters); and (3) Agency Operations - Specific policies and procedures. The implementation of this approach will not only strengthen the District's internal controls over financial operations and significantly minimize or eliminate Yellow Book findings and Management Letter Comments, but will also serve as an effective tool in current and new employee orientation, training, and cross-training.

Vendor Codes

The District uses a system of codes to identify various vendors with which it does business. These vendor codes are useful in managing payment transactions with internal agencies and with third party vendors. We noted that the vendor codification of the District has not been updated. We found several vendors listed in the database with whom there had been no transactions in months and years.

Process: General District Administration

The District should implement a policy of reviewing old and redundant vendor codes. Vendors with whom transactions have not been conducted in several years should be removed from the system, as deemed necessary. This would help minimize the risk of incorrect or fraudulent transactions with vendors who may not even be in existence.

Management's Response:

Management does not concur with this finding. When vendors are created in the District's Vendor Table, a vendor code is assigned to that vendor as their unique identifying number. These assigned vendor codes are never changed, unless the legal status/structure of the vendor changes.

Management will review the potentially redundant vendor codes provided and evaluate our policies for managing the District's Vendor Table.

* * * *

Process: Cash and Investments

Unclaimed Properties

Based on interviews with personnel and review of corroborating evidence to support our understanding of the process over unclaimed properties, we noted significant differences between management's understanding of the day-to-day responsibilities and the actual procedures performed by the Office of Finance and Treasury's (OFT) Unclaimed Property Unit.

Policies and procedures ensure that proper accounting principles are being applied, that similar transactions are treated consistently, and that financial information is produced in a form desired by management. We recommend that the District update and communicate comprehensive policies and procedures for unclaimed properties considering a review of the existing accounting system; this would offer management the opportunity to eliminate or improve procedures and thereby, create a more efficient and effective process.

Management's Response:

OFT is in the process of updating the policies and procedures for the Unclaimed Property Unit. We will incorporate the specific recommendations that were noted.

Cash Receipts

During our test work over cash receipts, we noted several instances where the actual procedures performed by the District differed from the set process. Deviations noted included the following:

- 1) Standard deposit tickets were not prepared by the agencies;
- 2) Office of Tax and Revenue (OTR) did not submit SOAR documentation;
- 3) Deposit slips were not submitted by the agencies to Office of Finance and Treasury (OFT);
- 4) Inconsistent enforcement of the requirement to include the change fund report in the documentation provided to OFT; and
- 5) Lack of sign-offs on register tapes.

In each instance, we did note that compensating controls were in place to support the integrity of the information processed. However, management should update its policies to ensure accuracy and to account for special instances where the official procedures cannot be followed. This would offer management the opportunity to eliminate or improve procedures and thereby, create a more efficient and effective process.

Management's Response:

Regarding the standard deposit tickets comment, there are different requirements for different transaction types. Transactions taken to Treasury cashier sites require the standard deposit ticket; the others do not. The Office of Tax and Revenue manages its own SOAR process. As indicated in the finding, the integrity of the information processed is supported by controls currently in place. Per the recommendation, management will review the policies and procedures and will incorporate appropriate updates into the process narrative.

Process: Cash and Investments

Cash Advances

For cash advances, Financial Management and Control Order No. 98-25, among other requirements, dictates the following:

Office of Finance and Treasury (OFT) shall review the documentation supporting all Cash Advance requests to ensure that it is consistent with what Office of Pay and Retirement Services (OPRS) and OFT have agreed is appropriate and required, and will ensure that it has been approved by the Director or Deputy Director of OPRS. If both the Director and Deputy Director are absent from work, one of them may officially delegate the authority to perform this function to another senior OPRS official. The processing of Cash Advances by OFT shall proceed only upon the approval of the Associate Treasurer for Operations and Banking or the Treasurer/Deputy CFO.

The District of Columbia Auditor (DCA) has noted that OFT officials failed to maintain complete records of cash advance transactions. These transactions were not recorded in SOAR, the District's accounting system of record.

In response to the DCA report, management modified its current policies and procedures to require OPRS to approve all cash advance requests. Since the implementation of this policy, OPRS has not approved any cash advances. However, if OPRS should begin to approve cash advances, the current policies and procedures do not ensure proper accounting for these transactions. We recommend that management review current procedures to ensure that all cash advance transactions will be properly accounted for in SOAR.

Management's Response:

OFT agrees with part of the finding, but disagrees with part of it. Management's revised policy preceded the DCA report. Management has eliminated cash advances, so there should be no future need to make any transactions in SOAR. Management will consider updating the policy to include specifics about how cash advances would be accounted for in SOAR if they were to be made, although management has no intention of making them going forward.

Supervisory Review

During our procedures, we noted that an erroneous journal entry had been recorded and this resulted in an understatement of the cash balance and an overstatement of the accounts receivable balance in the amount of \$13,635,571. The entry in question had been reviewed and approved.

This situation allowed an error to exist within the books and records for some time until it was identified and corrected during the audit process. We strongly suggest that management enforce strict adherence to its policies ensuring accurate supervisory review of accounting transactions. Without the necessary corrections, financial records are misrepresentative and this can allow for possible irregularities, including fraud, to exist and continue without notice.

Management's Response:

We concur with the finding and will follow the recommendation on this issue.

Process: Cash and Investments

Compliance with Investment Policy and its Parameters

The current investment policy establishes a set of broad guidelines within which the District's Office of Finance and Treasury (OFT) is to lawfully invest funds. The investment policy applies to all cash and financial investments of the various funds of the District of Columbia as identified in the District's Comprehensive Annual Financial Report (CAFR), with the exception of those financial assets explicitly excluded from coverage by this policy for legal or operational reasons. The policy also defines authorized investments, legal limits percentages, and other constraints.

The District has not been able to provide a supporting schedule as evidence that it was within the legal limit percentages and constraints at September 30, 2008.

We recommend that on a periodic basis, OFT consider a review of the current investment portfolio and document compliance with set policies. OFT should also ensure that the investment policy is current and reflects what is actually taking place with the District's investments.

Management's Response:

OFT staff provided a schedule that included support that we were in compliance with certain percentages and constraints of the investment policy. Apparently there was miscommunication regarding the need for additional information to complete testing in this area, and such information could have been provided and would have indicated that we were in compliance with the investment policy.

Transfer of Cash and Investments

Effective October 1, 2007, the component units Anacostia Waterfront Corporation (AWC) and National Capital Revitalization Corporation (NCRC) were transferred into the District's general fund. We noted the following:

- 1) The transaction to move the respective cash and investment activity into the general fund was not recorded until approximately 14 months later.
- 2) When the transaction was recorded, it was not communicated to the main employees responsible for handling the day-to-day aspects of accounting for the transfer.
- 3) The transfer was not recorded correctly, as approximately \$10 million remained in a clearing account (BID 999) at year-end.
- 4) Investment income of approximately \$222,000 and disbursements of approximately \$462,000 had not been recorded.

At year-end the activity was corrected and reflected appropriately. In these situations, we recommend that the District consider appointing a responsible person who would ensure the transaction is properly and completely accounted for and reflected on the books and records on a timely basis.

Process: Cash and Investments

Management's Response:

The initial entry to record cash and investments on the books was entered in early August of 2008, which was approximately 4 months after the FY 2007 Comprehensive Annual Financial Report (CAFR) was completed. It was our understanding that these numbers could not be entered in the system until the CAFR was finalized. The original entry was subsequently deleted from the system while making adjustments (in error) and was then put back in the system when the error was discovered.

The accounting staff for the Economic Development and Regulation Cluster recorded the entry to put the cash and investments on the books and handled all the subsequent accounting entries, so they were familiar with the aspects of accounting for the transfer. The only concern is that they received a majority of the information in piecemeal fashion, which led to making an enormous amount of adjustments. We now have procedures in place to ensure we will receive all the necessary accounting information on a monthly basis.

We believe that the transfer was recorded properly. When it was recorded, we booked all the cash and investments to BID 999. As the District received the funds from the closed accounts, the money was booked into the District's custodial account and BID 999 was reduced. There is still a balance in BID 999, but these are funds the District is waiting to receive, and once received they will also reduce BID 999.

Non-Compliance with Financial Institutions Deposit and Investment Amendment Act

For general deposit and investment requirements, the Financial Institutions Deposit and Investment Amendment Act, among other requirements, dictates the following:

The Mayor, or the Chief Financial Officer (CFO) pursuant to Section 47-351.2(c), shall not allow the amount of District funds deposited or placed for the provision of financial services in a single eligible financial institution to exceed the lesser of either:

- a) Twenty-five (25) percent of the total assets of the eligible financial institution, exclusive of the District funds; or
- b) Twenty-five (25) percent of the total District funds available for deposit or investment as of the date of such deposit or placement and as of the end of each fiscal quarter thereafter.

Our compliance test work revealed 1 instance of non-compliance with the aforementioned provision where deposits held by a single institution exceeded 25% of all District deposits. This occurred in October 2007 with Merrill Lynch. We recommend that the Office of Finance and Treasury (OFT) closely monitor the District's deposit percentages with all financial institutions.

Management's Response:

OFT management's position is that having only one single instance out of the whole year, which was detected by the District's daily monitoring process and corrected right away, constitutes compliance with the requirement.

* * * *

Process: Revenue Generation and Collection

Antifraud Policies and Procedures

On November 7, 2007, federal investigators announced the arrest of Office of Tax and Revenue (OTR) employees in connection with an alleged misappropriation of District funds by employees who were issuing and embezzling fraudulent manual real property tax refund checks.

Antifraud policies and procedures are part of an overall system of internal control. The District is responsible for designing and implementing effective systems and procedures for preventing, deterring, and detecting fraud. An effective antifraud program would not completely eliminate the possibility of fraud as there is no such thing as a fraud-proof system. For example, collusion among employees can override even a well run antifraud program. However, the District could benefit from a more comprehensive antifraud program. The basic controls of a comprehensive antifraud program include:

- 1) Prevention controls which are designed to reduce opportunities for fraud to occur. One example is updating investigations of individuals as they are promoted to positions of trust.
- 2) Detering controls which focus on controls that discourage individuals from committing fraud. While this may involve sanctions, the perception of the chance of getting caught generally persuades most individuals to not commit a fraud.
- 3) Detection controls, which are processes that will assist in the quick discovery of fraud. One example is a fraud hotline that is available 24/7 and is anonymous.
- 4) Creating an ethical culture, such as establishing and communicating the proper "tone at the top" and creating a positive work environment.
- 5) Implementing antifraud controls, such as the internal development of a fraud risk assessment process.
- 6) Developing an oversight process.

The District needs to continue to reevaluate its antifraud program with an immediate emphasis on its risk assessment. The leadership of the District will need to provide both the resources and the necessary support to assist in the success of this program.

Management's Response:

OTR benefited from significant and aggressive actions taken by the Office of the Chief Financial Officer (OCFO) during FY 2008 that were indicative of progress towards implementing a vigorous and effective antifraud program. Among the steps taken by the OCFO to enhance the antifraud program are the following:

- 1) Retention of the consulting firm Deloitte & Touche to perform an OMB Circular A-123 review of internal controls and to perform electronic monitoring of key databases and systems.
- 2) 1,400 OCFO employees received integrity training in the months of May and June 2008, and a new round of training will commence in June 2009.
- 3) Background investigations were initiated for every current employee hired before the testing program was implemented, and a periodic background investigation program will be instituted to ensure that investigations are updated on a five-year cycle.

Process: Revenue Generation and Collection

- 4) Hotline operations have been outsourced to EthicsPoint, Inc., an experienced third-party hotline operator; the OCFO instituted a tracking system for audit recommendations that holds managers accountable for implementation of recommendations.
- 5) A Risk Manager will be hired to oversee the antifraud program.

OTR is cooperating with the Treasury Inspector General for Tax Administration (TIGTA) through the Office of Oversight and Integrity (OIO) to institute a risk based audit plan. Specifically:

- 6) OTR has produced an Interim Refund Directive that provides guidance to employees when processing refunds.
- 7) OTR created the Taxpayer Account Maintenance Unit to direct and monitor compliance with the Interim Refund Directive and a special Refund Review Team was established to ensure that all refund requests are properly documented.
- 8) Training workshops were conducted on the Interim Refund Directive across all OTR administrations.
- 9) New hold for pick up procedures were implemented.
- 10) A multilevel tier review process for ITS and SOAR refunds was instituted.
- 11) The recommendations from the Kroll and Wilmer Hale reports will be implemented.

The OCFO and OTR are aggressively implementing steps to prevent fraud and will continue to take action on an ongoing basis to ensure that the procedures put in place to guard against fraudulent activity are followed.

Redeemed Properties – Tax Sale Process

During our review over Redeemed Properties, we noted that 5 out of 10 sampled items did not have supporting documents for Real Property Tax Sale Registrations.

The SOAR Revenue Refund Voucher (SRRV) is approved by the Revenue Accounting and Administration (RAA) within the Office of Tax and Revenue. This is essential in the process to ensure that postings to SOAR, the District's accounting system of record, are valid and properly approved. The tax sale registration is required from the tax sale purchaser to be filled out and signed before his/her participation in the tax sale is formalized. It is also at this stage that the tax sale purchaser is required to make payment to the District cashier. The District cashier stamps the registration indicating that the tax sale purchaser has made the payment.

Absence of the above document(s) may increase the risk of payments to fraudulent individuals and refunding of amounts to those not actually eligible to receive refunds. We identified these discrepancies from a sample of transactions that were selected for testing. Management should recognize that the potential exists for additional discrepancies. A significant effort should be undertaken to ensure that all supporting documentation is located, properly filed, and retained. This information is of the utmost importance to the accounting process, and its loss or misplacement simply should not be accepted.

Process: Revenue Generation and Collection

Management's Response:

RAA has been developing and will implement a checklist to attach to each SRRV to track required documentation and the review procedures performed (on each refund voucher). Also, note that the Interim Directive was implemented in March 2008. Prior to that time, the tax sale registration was not required as part of the refund package.

Interest Calculation Method

The interest calculation method is not clearly defined and documented in the Tax Sale Unit and the Adjustment Unit's policies and procedures manuals. We noted the following:

- 1) Tax Sale Refunds – If a tax lien sold at the District's annual Tax Sale is redeemed by the original property owner, the purchaser of the tax lien is due a refund of the money that was deposited with the District Government at the time of the tax lien purchase, as well as any subsequent payments made with respect to that property's real property tax assessment bill.

Per the Tax Sale policies and procedure manual (Tax Sale Business Model) which was implemented as of December 2008, the interest on the refund amount is computed at the monthly simple interest amount of 1.5% on the purchase price which relates to the principal of the outstanding tax lien. However, the Tax Sale Business Model does not indicate whether the interest period should include the month of the tax sale and the month of the redemption or cancellation, or whether partial months should be computed for the month of the tax sale and the month of redemption or cancellation.

In 9 of 49 tax sale refunds sampled, interest was calculated including the month of the tax sale and the month of redemption or cancellation. In 39 of the selections, only the month of redemption or cancellation was included in the calculation.

- 2) Court-Ordered Real Property Tax Refunds – The Adjustment Unit policies and procedures manual (Adjustment Unit User Guide) does not set forth guidelines for the calculation of interest on court-ordered refunds. The court order specifies the interest rate, the start of the interest period, and states that interest is due through "the date of making the refund."

The Real Property Tax Administration and Adjustment Unit (RPTAAU) employee preparing the refund packet must estimate the number of days that will elapse between initiating the refund and the date of the refund check in order to calculate the interest due to the taxpayer.

There is no specific process to guide employees on the number of days that should be estimated for processing time. As a result, the interest calculated may not comply with the court order.

To ensure that interest paid to the taxpayers is accurate, the Tax Sale Business Model and Adjustment Unit User Manual should include detailed guidance on how to calculate the interest owed to the taxpayer. The guidance should specifically state which days and/or time period should be included in the interest calculation.

Process: Revenue Generation and Collection

Management's Response:

The D.C. general ledger (a consolidated database of all properties that have been purchased at the Tax Sale through various years, including purchase amounts and buyer information) does not provide for the variance in interest calculations described above. Interest is calculated in the system automatically when the redemption date is entered. The Tax Sale Business Model is a draft document and has not been implemented to date. The Tax Sale Business model correctly describes the process in the D.C. general ledger on page 135.

Interest must be paid on court ordered refunds to the date of issuance of the check. Real Property Tax Administration (RPTA) and Revenue Accounting Administration (RAA) are currently developing policies for handling the calculation of interest to comply with court orders. The Adjustment Unit User Guide is a draft document and has not been either completed or implemented at this time. Procedures for calculating interest will be included in the Adjustment Unit User Guide.

Buyer's Report

A Buyer's Report is generated using the information stored in the D.C. general ledger. This report includes the properties purchased by the buyer at the District's annual tax sale auction, the original tax lien amount, and the surplus paid by the buyer. The Buyer's report is then attached to the SOAR Revenue Refund Voucher (SRRV) to support the Tax Sale refund.

In 2 of 49 tax sale refunds tested, the Buyer's Report stated the incorrect tax sale lien amount. Per the Real Property Tax Administration and Adjustment Unit's (RPTAAU) Information Technology Specialist, the Buyer's Report is capturing an incorrect field from the D.C. general ledger. In our sample selections where the Buyer's Report was incorrect, the error in the report did not result in an overpayment to the taxpayer, since other supporting documentation attached to the refund voucher was correct.

However, it should be noted that inaccurate Buyer's Reports may result in processing of erroneous tax sale refunds. Management should review the programming related to generation of the Buyer's Report to ensure that the report is linked to the appropriate fields within the database.

Management's Response:

Management concurs with the finding and will implement the recommendation.

Exemption from Real Property Tax

Pursuant to D.C. Official Code 47-1007, each owner of real property that is exempt from taxation under the provisions of subsections (4) to (20) of the D.C. Official Code 47-1002 must submit to the Office of Tax and Revenue an "Exempt Property Use Report" (Form FP-161) on or before April 1st of each year. If the report is not filed by the deadline (including any extensions granted by the Deputy Chief Financial Officer), the property shall immediately be assessed and taxed until the report is filed. In addition, a \$250 late penalty will be assessed.

Per discussion with the Exempt Specialist and Acting Director of the Real Property Tax Assessment Division, these assessments and penalties are not being strictly enforced. Failure to identify property owners not complying with this law will result in potential loss of revenue to the District.

Process: Revenue Generation and Collection

We recommend that the Office of Tax and Revenue (OTR) implement stronger controls over monitoring the annual filing of Form FP-161 and consider adding Integrated Tax System (ITS) capability to capture and bill the entities that did not comply with the requirement.

Management's Response:

OTR will consider strategies and review options for implementing stronger controls connected with filing Form FP-161. OTR will follow up on a timely basis with non-filers. Program changes will be made that will allow OTR to assess fines against non-filers. After careful review of the filings, OTR will take steps to revoke exemptions for non-filers.

Review and Approval of SOAR Revenue Refund Vouchers (SRRV)

The Recorder of Deeds (ROD) Division at the Office of Tax and Revenue (OTR) is responsible for the collection of all recordation and transfer taxes and fees on instruments being recorded. ROD also maintains these records for public inspection.

We selected and performed test work over 30 records. Each record is accompanied by a SRRV. We noted that 28 SRRVs were missing review and/or approval signatures. Failure to properly review and approve transactions can result in improper journal entries which can lead to inaccurate accounting records and reports. We recommend that the District follow its existing policies and procedures with respect to review and approval and maintain its existing internal controls.

Management's Response:

We will ensure that OTR's review and approval policies are followed for all SOAR vouchers.

Batching of Tax Returns

We noted that in 1 out of 29 selected items for test work, the Integrated Tax System (ITS) did not calculate the correct liability amount due to an error in the batch processing of tax returns. We noted that a 2005 return was erroneously batched with the 2006 returns. This error in batching of income tax return(s) resulted in incorrect data capture by ITS, which in turn resulted in ITS computing a lower tax amount on the return.

Errors are generally likely in this area due to the manual process of batching tax returns. We recommend that the Receipt and Control Unit diligently review the process of sorting and batching tax returns to ensure that all similar tax returns are batched in the correct tax year to avoid errors. In addition, the Code and Edit Unit and the Receiving Unit should also ensure that appropriate review of the batches is performed before taxpayer information is entered into ITS.

Management's Response:

The Receipt and Control and Code and Edit Units at the Office of Tax and Revenue will be instructed to conduct thorough reviews of batches to ensure that tax returns are batched in the correct year and that taxpayer information is accurately entered into ITS.

Process: Revenue Generation and Collection

Estate Taxes

Currently, estate tax collection information is logged into an excel spreadsheet known as the SOAR receipts log, which is maintained by tax auditors in the Compliance Division at the Office of Tax and Revenue (OTR).

We noted that there is no process to reconcile the SOAR receipts log to SOAR, the District's accounting system of record. Reconciliations play a key role in proving the accuracy of accounting data and information included in interim financial reports. We recommend that the District reconcile the SOAR receipts log with SOAR on a periodic basis to ensure completeness and accuracy of amounts recognized as revenues.

Management's Response:

The Revenue Accounting Administration (RAA) will team with the Audit Division, Compliance Administrative, to ensure that estate tax revenues received are reconciled to the general ledger monthly.

Policies and Procedures

We observed that there have been no updates to the following policies and procedures at the Office of Tax and Revenue:

- 1) Compliance Administration Collection Division – Training Manual – not been updated since September 2001.
- 2) Homestead Policies and Procedures – not updated since June 1, 2005.

It is recommended that the District annually review its policies and procedures. Components of internal controls, accounting, and the financial reporting system should be regularly updated and documented in writing to provide employees a clear picture of the District's controls, accounting procedures, and practices. Outdated policies and procedures may result in unjustified or inconsistent transactions processing, increased risk of errors, and possibly, loss and misuse of assets.

Management's Response:

The Homestead Business Practice Module has been drafted and is currently being reviewed. Upon completion of the review, a policies and procedures manual will be created. It is anticipated that the Homestead Policies and Procedures Manual will be completed by August 1, 2009.

Ball Park Fees and Receivables

During our review of the receivable balance at year-end, we noted that approximately \$1,600,000 had been outstanding for over 12 months. To improve control over receivables and revenue, we suggest that past-due balances be reviewed on a periodic basis. Any outstanding balances should be resolved and appropriately cleared from the books and records. Prompt collection action should be pursued when it is believed that amounts are valid and due to be paid. Otherwise, old, questionable, or unidentified balances should be written off.

Process: Revenue Generation and Collection

Management's Response:

We will implement the recommended analyses, reviews, and accounting procedures. Also, we will ensure coordination among Office of Tax and Revenue administrations with the Office of Financial Operations and Systems.

Department of Employment Services (DOES)

Section 44 of the Longshore and Harbor Workers' Compensation Act authorizes an annual assessment of each authorized insurance carrier and self insurer for administration of the District's Workers' Compensation Program. In the last quarter of each fiscal year, assessment invoices are mailed out for the following fiscal year. Any collections received during the current fiscal year are recognized as deferred revenues and subsequently recognized as revenues in the following fiscal year, when they are considered earned.

- 1) We noted that \$2,800,000 should have been recognized as revenue in FY 2008 as it was collected in FY 2007 but related to FY 2008 worker compensation assessments. This adjustment was made during the audit process.
- 2) DOES was unable to provide supporting cash receipts documentation for \$5,000,000. The balance related to assessment fees collected in FY 2008 but pertaining to FY 2009 worker compensation assessments.

A timely review will ensure revenue is properly recognized and the liability is properly recorded. Furthermore, adequate supporting documentation should be properly maintained. The availability of records is critical to any organization in the event of an audit, a lawsuit, an insurance claim, or a number of other circumstances. Management should institute certain procedures and decide on a systematic manner of filing and retaining documents.

Management's Response:

The Agency will review the outstanding deferred revenue balances on a timely basis, recognize the revenue accordingly, and record the liability properly.

Department of Consumer & Regulatory Affairs (DCRA)

During our specific procedures over revenue processed at the agency, we noted that for 16 out of 20 SOAR journal vouchers selected for testing, the agency was not able to provide revenue detail at the individual taxpayer level. We recommend that management should take steps to ensure that it is able to produce certain detailed reports and records at specific time periods, and maintain these records for review, analysis, and decision making by users such as management, independent auditors, and other governmental bodies.

Management should institute certain procedures and decide on a systematic manner of filing and retaining documents.

Management's Response:

The revenue detail was provided; however, it was after the period for completing test work. Management has a well organized and complete supporting documentation plan that includes information at the individual level.

Process: Revenue Generation and Collection

Office of the Chief Financial Officer (OCFO)

During our review of the receivable balance at year-end, we noted that approximately \$8,000,000 had been outstanding for over 12 months. It was also noted that dishonored checks and forfeitures were reflected in the year-end balances despite having been confirmed, by the Office of Finance and Treasury (OFT), to be no longer collectible.

To improve control over receivables and revenue, we suggest that past-due balances be reviewed on a periodic basis. Any outstanding balances should be resolved and appropriately cleared from the books and records. Prompt collection action should be pursued when it is believed that amounts are valid and due to be paid. Otherwise, old, questionable, or unidentified balances should be written off.

Management's Response:

The Dishonored Check Unit of OFT is responsible for the recording and collection of dishonored checks (with the exception of returned tax checks). Currently, our process to collect returned items is to (1) electronically re-deposit the items to the bank at least twice and (2) send notices to individuals notifying them of the returned check and informing them of their obligation to pay.

In addition, in our front-end process, we utilize Telecheck to verify collectability. We are in the process of procuring services for check guarantee which would give us the opportunity to collect 100% on checks presented at point-of-sale. However, we will still have the risk of checks not received in the mail as an exception. Moreover, we are in the process of procuring a collection agency to facilitate collection of receivables.

Considering such, we will work with the Office of Financial Operations and Systems (OFOS) to determine an adequate allowance to offset risk of uncollectible returned checks. In the FY 2008 closing process, \$8,000,000 of dated receivables was written off, leaving only a balance of \$1,000,000, all of which was outstanding one year or less.

We will monitor the outstanding receivable balances and the allowance associated with them at least on an annual basis, and appropriately adjust these balances on an on-going basis.

* * * *

Process: Compensation

During FY 2008, the District implemented a new PeopleSoft Payroll System. The PeopleSoft system replaced the previous Unified Personnel Payroll System (UPPS) used by the District. UPPS was less automated and required more manual interfaces and adjustments to record payroll expenditures in SOAR, the District's accounting system of record. The new PeopleSoft system is intended to be a more dynamic and integrated system requiring less manual adjustments.

We obtained a data extract from the Production environment at the end of FY 2008 for purposes of evaluating user access review as they relate to PeopleSoft HRMS applications (modules).

Without proper controls over sensitive privileges, users with access to transactions beyond their job responsibilities increase the risk that unauthorized transactions may be processed. We recommend that management ensure that the user privileges be reviewed to verify that access is appropriately restricted to only those privileges that are necessary to perform jobs. In addition, user access to the master file data should be sufficiently segregated from transactional access.

It should also be noted that in lieu of these observations, there are numerous controls (both process and monitoring) that appear to mitigate the related implications of these PeopleSoft findings. Management should further review these mitigating controls to ensure that they are sufficient to mitigate the risks noted below.

Sensitive Privilege Access within PeopleSoft – Human Resources

Sensitive privileges are functions in PeopleSoft that have inherent risk on their own but do not necessarily cause a conflict by themselves (i.e. Create/Modify Journal Entries; Processing Payments; etc.). However, since they are considered sensitive, these privileges should be limited to as few individuals as possible.

The following is a list of the sensitive functions within the Human Resources module and the corresponding number of users who have enter/update access to these functions:

- 1) 34 users have access to assign or approve employee group salary increases. Failure to restrict access to these sensitive pages increases the risk of unauthorized changes that could lead to payment errors or fraud.
- 2) 34 users have access to update employee variable compensation. The employee variable compensation pages allow access to sensitive employee payment information and therefore access should be restricted to authorized personnel. Failure to appropriately restrict access to these pages increases the risk of unauthorized changes that could lead to payment errors or fraud.
- 3) 34 users have access to view and update employee variable compensation details. Failure to restrict access increases the risk of unauthorized transactions which could lead to payment errors, fraud, and improper disclosure of sensitive employee information.
- 4) 361 users have access to hire an employee. Failure to restrict access increases the risk of fraud through the creation of ghost employees.
- 5) 36 users have access to update employee contracts. Employee contract information consists of sensitive HR data and therefore access to this information should be restricted to authorized individuals. Failure to restrict access to these pages increases the risk of disclosure of confidential employee information and could lead to unauthorized modifications.

Process: Compensation

- 6) 35 users have access to update employee earnings or deductions. Employee earnings and deductions represent sensitive and confidential information and therefore access to this data should be restricted to authorized personnel. Failure to appropriately restrict access to this information increases the risk of unauthorized changes that could lead to payment errors or fraud.
- 7) 35 users have access to update the salary increase setup data. Access should be highly restricted to authorized personnel due to the sensitive nature of the associated transactions. Failure to appropriately restrict access increases the risk of incorrect or unauthorized updates that could lead to payment errors or fraud.
- 8) 35 users have access to view and update employee credit card and bank account information. Failure to restrict access increases the risk of payment errors, fraud, and improper disclosure of sensitive information.
- 9) 35 users have access to view and update employee earnings and deductions information. Failure to restrict access increases the risk of unauthorized transactions which could lead to payment errors, fraud, and improper disclosure of sensitive employee information.
- 10) 446 users have access to update employee salaries. Access to sensitive employee salary information should be restricted to authorized personnel. Failure to appropriately restrict access to these pages increases the risk of unauthorized changes that could lead to payment errors or fraud.
- 11) 80 users have access to view and update employee benefits data. Failure to restrict access to this sensitive and confidential information increases the risk of unauthorized transactions and could lead to payment errors, fraud, and improper information disclosure.
- 12) 361 users have access to view and update employee compensation data. Failure to restrict access increases the risk of unauthorized transactions which could lead to payment errors, fraud, and improper disclosure of sensitive information.
- 13) 361 users have access to view and update employee personal data. Failure to restrict access increases the risk of unauthorized transactions which could lead to payment errors, fraud, and improper disclosure of sensitive employee information.
- 14) 448 users have access to view and update employee salary history. Failure to restrict access increases the risk of unauthorized transactions which could lead to payment errors, fraud, and improper disclosure of sensitive employee information.
- 15) 35 users have access to view and update employee salary increase information. Failure to restrict access increases the risk of unauthorized transactions which could lead to payment errors, fraud, and improper disclosure of sensitive employee information.
- 16) There were 3 instances where it appeared there was no segregation of duties between the Compensation Administrator and the HR Administrator roles. The Compensation Administrator role allows the user to define salary plans, define merit increases, maintain budgets, change salaries, calculate compensation, etc. The HR Administrator role allows the user to create budgets, maintain positions, maintain competency data, maintain and update employee personal information, terminate workforce, monitor and update absences, etc. Failure to segregate access to these roles increases the risk of fraud (e.g. the creation of ghost employees and subsequent payroll payment).

Process: Compensation

- 17) There were 3 instances where it appeared there was no segregation of duties between the Compensation Administrator and the Recruitment Administrator roles. The Compensation Administrator role allows the user to define salary plans, define merit increases, maintain budgets, change salaries, calculate compensation, etc. The Recruitment Administrator role allows the user to recruit the workforce and update their contracts and personal information. Failure to segregate access to these roles increases the risk of fraud (e.g. creation of ghost employees and subsequent payroll payment or unauthorized salary increases).
- 18) 5 users have access to the HR Administrator role. The HR Administrator role allows the user to create budgets, maintain positions, maintain competency data, maintain and update personal employee information, terminate workforce, monitor and update absences, etc. Therefore, this very sensitive role should be assigned to a limited number of individuals. Failure to limit access to this role could lead to payment errors, unauthorized transactions, and fraud.

Management's Response:

- 1) *Access to assign or approve employee group salary increase; access to update employee variable compensation:*

Connection: PSFTHRMS_AI, User Count: 34

All the users in this group are within the IT support area. You will note that some of the User IDs are named ASMP_BATCHxxx or SCRxxxx. These are created in response to a specific user request to process mass updates of employment information. The User ID name links to a System Change Request (SCR) which can be referenced for the appropriate approvals and authorizations.

We have now instituted a practice whereby the "SCR" user IDs will be deleted once the activity is completed and the SCR has been closed.

Although 'Read Only' access is required for trouble shooting, update access has been reduced to a smaller group.

- 2) *Access to Hire an Employee:*

Connection: PSFTHRMS_AI, User Count 361

Except for the IT support population identified above, these are business users.

There are several customizations around HR security that need to be considered when counting users in this category. Only users with the following role combinations have access to hire an employee:

- Independent Personnel Authorities (IA): DCG_Agency_HR_Spec and DCG_PAR_PROC_IA and do not have the role DCG_HR_SPEC_NA assigned
- District of Columbia Human Resources (DCHR) Authority (DCHR): DCG_DCOP_HR_Spec and DCG_PAR_PROC_DCOP and do not have the role DCG_HR_SPEC_NA assigned
- Error Handlers (ERR): DCG_Error_Handler_Mgr
- DCG_Hire_Processor

There are a total of 209 users that can hire.

Process: Compensation

3) *Access to Update Employee Contract:*

Connection: PSFTHRMS_AI, User Count: 36

The users listed in this group are IT Support. The District Government does not use employee contracts, so the access to these components is incidental due to a "Super user" access.

4) *Access to View and Update Employee Earnings, Deductions, Credit Card, Bank Account, Salary Increase Set up:*

Connection: PSFTHRMS_AI, User Count: 35

All the users in this group are within the IT support area. You will note that some of the User IDs are named ASMP_BATCHxxx or SCRxxxx. These are created in response to a specific user request to process mass updates of employment information. The User ID name links to a System Change Request (SCR) which can be referenced for the appropriate approvals and authorizations.

The Office of Chief Technology Officer (OCTO) has instituted a practice whereby the "SCR" user IDs will be deleted once the activity is completed and the SCR has been closed.

Although 'Read Only' access is required for trouble shooting, update access has been reduced to a smaller group.

5) *Access to Update Employee Salary:*

Connection: PSFTHRMS_AI, User Count: 446

Except for the IT support noted previously, these are business users designated as HR Advisors or Specialists, CFOs, and Agency Directors. Updates to employee salary information go through a workflow approval: HR Advisor, Budget Authority, Agency Director, HR Specialist. So while these users do have access to update salary data, they can do so only within the established approval flow.

There are several customizations around HR security that need to be considered when counting users in this category. Only users with the following role combinations have access to process any personnel action affecting the salary of an employee:

- Independent Personnel Authorities: DCG_Agency_HR_Spec and DCG_PAR_PROC_IA and do not have the role DCG_HR_SPEC_NA assigned
- DCHR Authority: DCG_DCOP_HR_Spec and DCG_PAR_PROC_DCOP and do not have the role DCG_HR_SPEC_NA assigned
- Error Handlers: DCG_Error_Handler_Mgr

DCHR may initiate and process the changes without electronic approval flow, but rely on paper approval process in these cases.

There are a total of 188 users that can process salary changes.

Process: Compensation

6) *Access to View and Update Employee Benefits Data:*

Connection: PSFTHRMS_AI, User Count: 80

Except for the IT support noted previously, these are users within the DCHR Benefits Administration Division.

7) *Access to View and Update Employee Compensation Data:*

Connection: PSFTHRMS_AI, User Count: 361

Except for the IT support noted previously, these are business users designated as HR Advisors or Specialists, Budget Directors, and Agency Directors.

Updates to employee compensation data goes through a workflow approval: HR Advisor, Budget Authority, Agency Director, HR Specialist. So while these users do have access to update compensation data, they can do so only within the established approval flow.

DCHR may initiate and process the changes without electronic approval flow, but rely on paper approval process in these cases.

There are several customizations around HR security that need to be considered when counting users in this category. Only users with the following role combinations have access to process any personnel action affecting the salary of an employee:

- Independent Personnel Authorities: DCG_Agency_HR_Spec and DCG_PAR_PROC_IA and do not have the role DCG_HR_SPEC_NA assigned
- DCHR Authority: DCG_DCOP_HR_Spec and DCG_PAR_PROC_DCOP and do not have the role DCG_HR_SPEC_NA assigned
- Error Handlers: DCG_Error_Handler_Mgr

DCHR may initiate and process the changes without electronic approval flow, but rely on paper approval process in these cases.

There are a total of 188 users that can update compensation data.

8) *Access to View and Update Employee Salary History:*

PSFTHRMS_AI, User Count: 448

Except for the IT support noted previously, these are business users designated as HR Advisors or Specialists, Budget Directors, and Agency Directors.

Updates to employee salary history go through a workflow approval: HR Advisor, Budget Authority, Agency Director, and HR Specialist. So while these users do have access to update compensation data, they can do so only within the established approval flow.

DCHR may initiate and process the changes without electronic approval flow, but rely on paper approval process in these cases.

Process: Compensation

There are several customizations around HR security that need to be considered when counting users in this category. Only users with the following role combinations have access to process any personnel action affecting the salary of an employee:

- Independent Personnel Authorities: DCG_Agency_HR_Spec and DCG_PAR_PROC_IA and do not have the role DCG_HR_SPEC_NA assigned
- DCHR Authority: DCG_DCOP_HR_Spec and DCG_PAR_PROC_DCOP and do not have the role DCG_HR_SPEC_NA assigned
- Error Handlers: DCG_Error_Handler_Mgr

DCHR may initiate and process the changes without electronic approval flow, but rely on paper approval process in these cases.

There are a total of 188 users that can update salary history.

9) *Access to View and Update Employee Salary Increase Information:*

PSFTHRMS_AI, User Count: 35

The users listed in this group are IT Support and as outlined in the first User Count section, will be reduced.

10) *Compensation Administrator, HR Administrator, Recruitment Administrator:*

PSFTHRMS_AI, User Count: 3

The users listed are Data Base Administrators (DBA).

11) *HR Administrator:*

PSFTHRMS_AI, User Count: 4

All users listed are Data Base Administrators (DBA), except for one. Through a data entry error this user was inadvertently assigned "HR Administrator" instead of "DCG_HR_Administrator". This has been corrected. This has been added to the list of Security audits regularly run to ensure it does not occur again.

User privilege and controls will be continually reviewed and updated, as required to ensure, proper internal controls, consistent with the authority of the District Human Resources offices and the OCFO Financial Offices (OPRS central office), as well as at Agency levels.

Sensitive Privilege Access within PeopleSoft – System Administration

Sensitive privileges are functions in PeopleSoft that have inherent risk on their own but do not necessarily cause a conflict by themselves (i.e. Create/Modify Journal Entries; Processing Payments; etc.). However, since they are considered sensitive, these privileges should be limited to as few individuals as possible.

The following is a list of the sensitive functions within the System Administration module and the corresponding number of users who have enter/update access to these functions:

Process: Compensation

- 1) 36 users have access to their department's security table. Access to update the HRMS security table allows the user to modify configurations related to the reporting structure, approval levels, etc. Therefore, failure to restrict access to these pages could lead to unauthorized configuration modifications, improper approvals, reporting errors, etc.
- 2) 148 users have access to foundation tables. Access to the HRMS foundation tables (company, tableset ID, business unit, tableset control table, operator preferences, business unit HR defaults, establishment tables, location table, department table, salary plan/grade/step tables, job code table, and pay group table) should be highly restricted. Failure to restrict access to these sensitive tables increases the risk of unauthorized transactions, payment errors, fraud, or financial reporting errors.
- 3) 9 users have access to the installation table. The Installation Table contains most of the system default settings such as minimum and maximum standard hours, compensation rate codes, default compensation frequency, etc. that drive data processing. Therefore, access to the Installation Table should be restricted to authorized individuals. Failure to restrict access to the table increases the risk of unauthorized and inappropriate modifications which could lead to processing delays, payment errors, fraud, or system unavailability.
- 4) 39 users have access to update the HRMS security menu. The menu allows access to application settings (e.g. pay groups) and therefore access should be restricted to authorized personnel. Failure to appropriately restrict access to these pages increases the risk of payment errors, processing delays, fraud, and system unavailability.
- 5) 7 users have access to update user security. The user security pages allow users to create new users and lock existing users and therefore, access should be restricted to authorized personnel. Failure to appropriately restrict access to these pages increases the risk of unauthorized system access or improper user lockout.
- 6) 8 users are assigned to the PeopleTools role. The PeopleTools role allows users to access PeopleSoft's powerful system tools such as Application Designer, that can be used to modify the underlying system codes. Therefore, access to this role should only be granted to a small number of authorized employees. Failure to restrict access to this role could lead to payment errors, processing delays, fraud, and system unavailability.
- 7) 10 users are assigned to the Portal Administrator role. The Portal Administrator role gives users access to folder administration, portal registry, menu security, menu folder structure, etc. Therefore, access to this critical role should be restricted to a limited number of authorized individuals. Failure to restrict access to this role could lead to payment errors, processing delays, fraud, and system unavailability.

Management's Response:

- 1) *Access to Department Security Table:*

PSFTHRMS_AI, User Count: 36

All the users in this group are within the IT support area. You will note that some of the User IDs are named ASMP_BATCHxxx or SCRxxxx. These are created in response to a specific user request to process mass updates of employment information. The User ID name links to a System Change Request (SCR) which can be referenced for the appropriate approvals and authorizations.

Process: Compensation

We have now instituted a practice whereby the "SCR" user IDs will be deleted once the activity is completed and the SCR has been closed.

Although 'Read Only' access is required for trouble shooting, update access has been reduced to a smaller group.

2) *Access to Foundation Tables:*

PSFTHRMS_AI, User Count: 148

These users have a role called "DCG_HR_Classifier" and are authorized to create Job Codes. It is their access to Job Code creation only that causes them to appear under this category. Only IT Support has access to update the other items falling under this category (Locations, Salary Plans, Pay Group, Departments, business units, tableset, etc).

3) *Access to Installation Tables:*

PSFTHRMS_AI, User Count: 9

This has been reduced to Data Base Administrators; only (3).

4) *Access to Update HRMS Security:*

PSFTHRMS_AI, User Count: 39

There is a role which grants limited access to Time & Labor security administration. Full Security Admin access is limited to 5 users.

5) *Access to Update User Security:*

PSFTHRMS_AI, User Count: 7

This is limited to Data Base Administrators only.

6) *Access to PeopleTools:*

PSFTHRMS_AI, User Count: 8

This is limited to Data Base Administrators only.

7) *Access to Portal Administrator:*

PSFTHRMS_AI, User Count: 8

This is limited to Data Base Administrators and full Security Administrators.

Process: Compensation

Sensitive Privilege Access within PeopleSoft – Payroll

Sensitive privileges are functions in PeopleSoft that have inherent risk on their own but do not necessarily cause a conflict by themselves (i.e. Create/Modify Journal Entries; Processing Payments; etc.). However, since they are considered sensitive, these privileges should be limited to as few individuals as possible.

The following is a list of the sensitive functions within the Payroll module and the corresponding number of users who have enter/update access to these functions:

- 1) 35 users have access to compensate employees. Access to HR setup tables and master file transactions should be adequately restricted to authorized users. Specifically, access to 'Compensate Employees' pages should be restricted to authorized personnel. Failure to appropriately restrict access increases the risk of unauthorized transactions, payment errors, and fraud.
- 2) 72 users have access to view, update, and review payroll. Failure to restrict access to view and update payroll information increases the risk of unauthorized transactions which could lead to payment errors, fraud, and improper disclosure of sensitive employee information.
- 3) 34 users can export payroll files. Access to export payroll files should be highly restricted. Failure to restrict access to this capability increases the risk of unauthorized payments and fraud. Furthermore, it could lead to the disclosure of sensitive employee payment information.
- 4) 66 users can generate off-cycle payments. Access to generate off-cycle payroll checks/payments should be adequately restricted. Failure to restrict access to this capability increases the risk of unauthorized payments and fraud.
- 5) 4 users are assigned to the NA Payroll Administrator role. The NA Payroll Administrator role allows the user to define and maintain global payroll data and manage the global payroll process, etc. Therefore, this very sensitive role should be assigned to only a limited number of authorized individuals. Failure to limit access to this role could lead to payment errors, processing delays, fraud, and system unavailability.
- 6) 35 users have access to payroll reporting. Access to the payroll reporting functionality should be highly restricted to only authorized personnel. Failure to restrict access to these pages increases the risk surrounding distribution of sensitive employee payroll information.
- 7) 66 users have access to transfer payroll information. Access to transfer payroll information to the bank should be adequately restricted. Failure to restrict access to this capability increases the risk of unauthorized payments and fraud.
- 8) 366 users can view employee data. Access to view employee job details should be restricted to authorized personnel. Unauthorized access to this sensitive data may result in its misuse and/or improper disclosure.

Management's Response:

- 1) *Access to Compensate Employees:*

PSFTHRMS_AI, User Count: 35

Process: Compensation

All the users in this group are within the IT support area. You will note that some of the User IDs are named ASMP_BATCHxxx or SCRxxxx. These are created in response to a specific user request to process mass updates of employment information. The User ID name links to a System Change Request (SCR) which can be referenced for the appropriate approvals and authorizations.

We have now instituted a practice whereby the "SCR" user IDs will be deleted once the activity is completed and the SCR has been closed.

Although 'Read Only' access is required for trouble shooting, update access has been reduced to a smaller group.

2) Access to View-Update-Review Payroll Information:

PSFTHRMS_AI, User Count: 72

Some of the users in this group are within the IT support area. You will note that some of the User IDs are named ASMP_BATCHxxx or SCRxxxx. These are created in response to a specific user request to issue a mass update of employment information. The User ID name links to a System Change Request (SCR) which can be referenced for the appropriate approvals and authorizations.

We have now instituted a practice whereby the "SCR" user IDs will be deleted once the activity is completed and the SCR has been closed.

Although 'Read Only' access is required for trouble shooting, update access has been reduced to a smaller group.

The non IT Support users are within the Office of Pay and Retirement Services (OPRS) business unit.

3) Access to Export Payroll Files:

PSFTHRMS_AI, User Count: 34

All the users in this group are within the IT support area. You will note that some of the User IDs are named ASMP_BATCHxxx or SCRxxxx. These are created in response to a specific user request to process mass updates of employment information. The User ID name links to a System Change Request (SCR) which can be referenced for the appropriate approvals and authorizations.

We have now instituted a practice whereby the "SCR" user IDs will be deleted once the activity is completed and the SCR has been closed.

Although 'Read Only' access is required for trouble shooting, update access has been reduced to a smaller group.

4) Generate Off-Cycle Payments:

PSFTHRMS_AI, User Count: 66

Some of the users in this group are within the IT support area. You will note that some of the User IDs are named ASMP_BATCHxxx or SCRxxxx.

Process: Compensation

These are created in response to a specific user request to issue a mass update of employment information. The User ID name links to a System Change Request (SCR) which can be referenced for the appropriate approvals and authorizations.

We have now instituted a practice whereby the "SCR" user IDs will be deleted once the activity is completed and the SCR has been closed.

Although 'Read Only' access is required for trouble shooting, update access has been reduced to a smaller group.

The non IT Support users are within the Office of Pay and Retirement Services (OPRS) business unit.

5) NA Payroll Administrator:

PSFTHRMS_AI, User Count: 4

These are Data Base Administrators.

6) Access to Payroll Reporting:

PSFTHRMS_AI, User Count: 35

All the users in this group are within the IT support area. You will note that some of the User IDs are named ASMP_BATCHxxx or SCRxxxx. These are created in response to a specific user request to process mass updates of employment information. The User ID name links to a System Change Request (SCR) which can be referenced for the appropriate approvals and authorizations.

We have now instituted a practice whereby the "SCR" user IDs will be deleted once the activity is completed and the SCR has been closed.

Although 'Read Only' access is required for trouble shooting, update access has been reduced to a smaller group.

7) Access to Transfer Payroll Information:

PSFTHRMS_AI, User Count: 66

Some of the users in this group are within the IT support area. You will note that some of the User IDs are named ASMP_BATCHxxx or SCRxxxx. These are created in response to a specific user request to issue a mass update of employment information. The User ID name links to a System Change Request (SCR) which can be referenced for the appropriate approvals and authorizations.

We have now instituted a practice whereby the "SCR" user IDs will be deleted once the activity is completed and the SCR has been closed.

Although 'Read Only' access is required for trouble shooting, update access has been reduced to a smaller group.

The non IT Support users are within the Office of Pay and Retirement Services (OPRS) business unit.

Process: Compensation

8) *View Employee Data:*

PSFTHRMS_AI, User Count: 366

These are business users in the areas of Human Resources and Payroll Support, as well as IT Support individuals.

OPRS, along with appropriate IT support, has access to View, Update, and Review payroll information; Agencies have limited access to View/Review individual payroll information for their employees. OPRS' central payroll office, Special Pay division are the only employees authorized to enter and generate off-cycle payments.

Other Observations within PeopleSoft

We also noted the following items:

- 1) Information technology (IT) personnel have access to enter transactions in the production system which is beyond their normal job function.
- 2) A known default user ID (PS) is not disabled and assigned access to all functionality within the PeopleSoft HRMS system.
- 3) Based upon our request for information and discussion with various District employees, we noted that PeopleSoft does not currently track and report actual full-time equivalent (FTE) counts. Without the ability to track and monitor actual FTEs, there is an increased risk that payroll expenditures will not be properly monitored and that management will not be able to accurately measure statistics.

The system capability to track and monitor actual FTEs was originally designed to be part of the PeopleSoft system. However, it does not appear to be functioning.

We recommend that management adopt better controls over logical security and may consider reviewing the access currently granted to IT and support staff and limit it to "view only" as it pertains to production transaction data. Further, we recommend that management disable the PS user ID from the PeopleSoft HRMS system. Inappropriate or excessive access may result in unauthorized data changes or transactions.

The District should also consider implementing capabilities within the PeopleSoft system to track and report actual FTEs. Management should establish policies and procedures to ensure that designated employees are responsible for the monitoring and oversight of payroll and FTEs.

Management's Response:

- 1) The PeopleSoft Program Manager has reviewed the IT personnel who have access to enter transactions in the production system. Currently, only 4 IT support staff have access, i.e. 2 Security Administrators who assist with the ASMP PeopleSoft Help Desk, 1 backup Help Desk Security Administrator, and 1 OCTO Program Manager who manages all PeopleSoft Modules.

Process: Compensation

- 2) While the known default user ID (PS) has not been disabled, it is password protected and only the Data Base Administrator (DBA) has access to the password. Nevertheless, the OCTO PeopleSoft Program Manager is reviewing the need to continue the default user ID and will recommend that it be disabled or renamed with a User ID specific to the DBA.
- 3) FTEs are counted on budgeted positions. PeopleSoft provides a Position Control Report that compares actual FTE counts with budgeted positions identified in the District's Adopted Budget. While this report is available to the CFO role in the PeopleSoft module, all agency finance staff may not be aware of it. Consequently, we will communicate with all CFO finance staff the custom reports that are available for managing their payroll expenditures.

Health Benefit Payments made after Termination

The District pays health benefits to third parties for its employees. We reviewed 45 terminated employees and noted that in 2 cases, the District continued to pay health benefits for employees for up to 2 months after the employee's separation from the District government. Based on District policies and procedures, employees are not entitled to health benefits after termination.

In one instance, benefits were continued to be paid because the HR approval was not processed in a timely manner. In the second instance, the employee was on leave without pay for three months and the premiums continued to be paid. The employee was subsequently terminated, and there is no evidence of recoupment of the premiums.

Insufficient coordination appears to exist between District Agencies, the Office of Personnel, and the Office of Pay and Retirement Systems in the timely processing and monitoring of terminations of employees. Delays in processing and failure to closely monitor personnel actions for terminated employees may result in unnecessary benefit costs being incurred by the District for terminated employees.

We recommend that the District improve its policies and procedures over the timely processing of personnel actions for terminated employees. In addition, the District should consider enhancing its payroll system to prevent benefits payments beyond employees' termination date(s). The District also needs to evaluate and enforce its procedures over the benefit reconciliation process.

Management's Response:

In 2 of the cases cited, the employees' termination actions was processed after the effective date of the termination, thereby causing additional benefits payments to be made by the agency and the employee.

In the case of the individual that was on a Leave Without Pay Status (LWOP) for three months, only the agency portion of the benefits was paid. To avoid future occurrences, District of Columbia Human Resources (DCHR) will run periodic, monthly LWOP and termination reports in order to capture this information more quickly. Finally, DCHR will capture this information through its reconciliation process.

Reconciliations of the five health benefit plans have historically been done on an annual basis. This process includes a review of eligibility and premium payment records. In calendar year 2008, the District recovered in excess of \$1,000,000 in overpayments. During calendar year 2009, DCHR will be conducting more frequent reconciliations in an effort to maintain more synchronized records with our health benefit carriers.

* * * *

Process: Management of Grants

Transfer of Grants Receivable

Effective October 1, 2007, the component units Anacostia Waterfront Corporation (AWC) and National Capital Revitalization Corporation (NCRC) were transferred into the District's general fund. As such, certain applicable activity was transferred into the books and records for the Deputy Mayor for Planning and Economic Development (EB0) Agency.

Based on a review of EB0's receivable balance at year-end, we noted an outstanding balance due from the Department of Housing and Community Development (DHCD), another District agency, for approximately \$2,400,000. This related to activity between DHCD and AWC before the aforementioned dissolution of AWC and incorporation of its activities into the District's books and records.

This has resulted in an overstatement of the ending accounts receivable by \$2,400,000 because EB0, AWC, and DHCD are all different agencies or activities of the District, at large. We recommend that EB0 monitor and review its receivable balances. In this specific instance, the Agency should make eliminating entries to remove the "due to/due from NCRC and AWC" activity from its books.

Management's Response:

The Agency has a plan in place to monitor and review the collectability of the receivables. In addition, the Agency will increase its effort to collect and clean up any outstanding balances. The Agency will also make the eliminating entries to remove the "due to/due from NCRC and AWC" activity from its books.

Income Maintenance Administration (IMA)

Temporary Assistance for Needy Families (TANF)

The Department of Human Services' Income Maintenance Administration (IMA) is responsible for determining eligibility for the TANF program. IMA uses the Automated Client Determination System (ACEDS) to evaluate the eligibility of an applicant. During our review, we noted the following from a sample of 45 items selected for test work:

- 1) We could not determine whether the applicant was eligible to receive TANF benefits as 1 case record was not provided.
- 2) The supervisor did not sign the required recertification form for 1 case record reviewed.

We also noted that TANF benefits do not automatically terminate at the end of the specified six-month period or when the participant becomes ineligible. We noted that at the end of the eligibility period, ACEDS does not automatically send a recertification letter to the participant notifying him/her to recertify for TANF benefits. TANF benefits continue to be provided until IMA manually processes the request for the participant to recertify. Therefore, since TANF benefits continue after the period of eligibility, it is very possible that there are participants receiving TANF benefits, who are not eligible for the benefit.

Adequate internal controls to monitor TANF benefits are essential to ensure that TANF benefits are only paid to eligible participants. We recommend that IMA improve internal controls to ensure that documentation is maintained to support eligibility decisions and properly maintain and secure such documentation in participant files. We also recommend that management review TANF eligibility determinations to ensure that they are in accordance with established Federal regulations.

Process: Management of Grants

Food Stamps Program

The Department of Human Services' Income Maintenance Administration (IMA) is responsible for determining eligibility for the Food Stamps program. The Food Stamps program enables low-income families to buy the food they need to maintain good health. IMA uses the Automated Client Determination System (ACEDS) to evaluate the eligibility of an applicant. During our review, we noted the following from a sample of 45 items selected for test work:

- 3) We could not determine whether the applicants were eligible to receive Food Stamp benefits as 2 case records were not provided.
- 4) The supervisor did not sign the required recertification form for 1 case record reviewed.

Adequate internal controls to monitor Food Stamps benefits are essential to ensure that benefits are only paid to eligible participants. We recommend that IMA improve internal controls to ensure that documentation is maintained to support eligibility decisions and properly maintain and secure such documentation in participant files.

Management's Response:

IMA is modernizing its entire business process. IMA has just completed the first phase of that process. In the first phase, the paper files at each of the respective service centers was migrated from a numerical filing system, based on the customer's address, to an alphabetical filing system, based on the head-of-household's name.

The Centers also moved to a case-banking system and away from individual caseloads. The high worker turnover among SSRs meant that cases were often floating between workers, and at times left incomplete. With case banking, a worker only touches the case to update it, and then returns to a controlled central file at each respective center.

These two changes lay the foundation for moving to a fully automated system. IMA is presently preparing the paper case files to be scanned and stored in an electronic filing system and linked to the case record. This will eliminate lost or missing files, and enable workers to identify documents that are needed to complete the file or application. The physical scanning of records should begin this spring, and once complete no paper records will be maintained.

Following the scanning of the case files, IMA is developing an automated application and recertification process. The automated application and recertification process will have system triggers, which will force both workers, as well as customers to complete certain fields (such as applicant signature) before a final determination of benefits is rendered. The system will also have alerts, which insure that administrative functions – such as supervisory approval and the closing of cases are further automated into the system, thus eliminating the potential for worker error.

Child and Family Services Agency (CFSA)

During our review of the Foster Care and Adoption Assistance programs as administered by CFSA, we noted the following from a sample of 45 items selected for test work:

- 1) In 3 instances, CFSA was unable to provide evidence that the foster family home provider met a criminal records background check, including a fingerprint-based check.

Process: Management of Grants

- 2) In 3 instances, CFSA failed to provide evidence of a child abuse and neglect registry check with respect to prospective foster and adoptive parents and any other adult living in the home who had resided in the provider home in the preceding 5 years.

It is noted that internal controls are not functioning as intended. Failure to properly support claims can result in noncompliance with laws and regulations. We recommend that the District review and revise its policies and procedures to ensure that items claimed for eligibility are supported by proper documentation and that checklists are maintained within the filing system to ensure that all necessary documentation is included in a child's records before filing a claim.

Management's Response:

The Agency concurs with the recommendations. However, the agency does not concur with the findings.

Office of the State Superintendent of Education (OSSE)

We noted that OSSE had \$94,627,793 in outstanding grants receivable at September 30, 2008. This balance pertained to several phases of federal grants and we noted that the balance had grown significantly from the prior year. Upon further audit investigation, it became apparent that the balance had grown significantly due to duplicate recording of revenues by both OSSE and the Office of Finance and Risk Management. As such, District personnel were requested to reconcile the grant activity and the amount was written-off.

We recommend that there should be continuous monitoring and review of receivable balances and their collectability. Any outstanding balances should be resolved and appropriately cleared from the books and records. Prompt collection action should be pursued when it is believed that amounts are valid and due to be paid. Otherwise, old, questionable, or unidentified balances should be written off. We also recommend that the appropriate individuals review and approve journal entries to improve controls over adjustments and to avoid reoccurrences of such errors.

Per discussion with personnel from OSSE and the Office of Financial Operations and Systems, this was a one time exception which will not be repeated.

Management's Response:

The OSSE Controller is responsible for adherence to the CFO policy on the administration, recording, and collection of receivables for federal grants. OSSE accepts the recommendation for the administration and collection of receivables. Collections will be executed for federal grant related payroll expenditures on a bi-weekly basis. All other federal grant related expenditures will be collected monthly. The OSSE Senior Accountant has been assigned responsibility accruing revenue for unreimbursed federal grant expenditures monthly.

* * * *

Process: Disbursements

Purchase Cards

The District's purchase card transactions are primarily governed by statute, as well as rules and regulations outlined in the District of Columbia Official Code. In addition, the Mayor, Chief Financial Officer, and Director of the Office of Contracting and Procurement (OCP) can issue directives, orders, and memorandums governing purchasing actions. We noted the following issues during our audit process:

Review of Purchase Card Reporting Requirement

The District did not submit, to the Council, quarterly reports by agency of all expenditures in the purchase card program for each quarter of the fiscal year. The District submitted one report during FY 2008, which covered, October 1, 2007 through the end of the billing cycle in September 2008 (i.e. September 19, 2008). This report did not agree to the detail of the purchase card transactions provided by the Office of Contracting and Procurement (OCP), as it did not include at least the last eleven days of the fiscal year, which were included on the statements for October 2008.

Transaction Usage

Purchase card transactions are required to be supported by an original invoice or vendor receipts, cardholder transactions logs, monthly statements of account, statement of questioned items, and memorandum of explanation for documentation. Of the 45 transactions selected for testing:

- 1) No supporting documentation was available for 13 transactions.
- 2) The Approving Official Account Summary as identified in the Purchase Card Policies and Directive (Effective 02/16/2004) was not provided for 31 purchase card transactions.
- 3) The invoice for 1 transaction selected for testing was not provided. In addition, although documentation was provided for another transaction we noted that it did not identify the nature of the item purchased. Only a copy of the part of the invoice which identified the store, the amount of the purchase, and the method of payment was provided. The cardholder transaction log for these 2 transactions was not provided. We were therefore unable to determine the following:
 - Whether the cardholder used the card to buy commercially available goods and services for Official Government Business Only.
 - Whether the purchase was deemed reasonable within the District's standards (i.e. no purchases were for personal use, travel, and travel-related expenses, taxicab fees, cash advances or ATM withdrawals, utility payments, motor vehicle fuel, criminal or illegal activity, entertainment, or any prohibited usage designated by the Agency Head.
- 4) For 1 transaction selected, it was noted that this transaction was identified by the cardholder as a fraudulent transaction. The purchase card holder reported the transaction to U.S. Bank Card member Services Fraud Prevention. The cost of the transaction was credited back to the account. However, no statement of questioned items or memorandum of explanation for documentation was provided.

Official Government Usage

- 5) There were 5 instances where the District did not provide the "Delegation of Contracting Authority-Purchase Card" waiver forms for the amounts over the monthly limit of \$10,000.

Process: Disbursements

- 6) There was 1 transaction where the purchases tested exceeded the standard monthly purchase limit. The "Delegation of Contracting Authority-Purchase Card" waiver form provided to us did not cover the period of this transaction.
- 7) There was 1 instance where the card holder had two purchase cards, but only made purchases on one card during the cycle. These purchases exceeded the standard monthly purchase limit of \$10,000 and no "Delegation of Contracting Authority-Purchase Card" waiver form was provided to us to support the amounts over the limit.
- 8) There were 3 instances where the purchases made on the card at the beginning of the billing cycle, prior to the approved date on the waiver form exceeded the standard limit of \$10,000. The purchases that exceeded the \$10,000 limit were not covered by the waiver forms provided.
- 9) There was 1 instance where a purchase during the billing cycle did not exceed the monthly limit of \$10,000, but exceeded the single transaction limit of \$2,500. OCP provided a "Delegation of Contracting Authority-Purchase Card" waiver form authorizing a single transaction limit of \$35,000 for a period which did not cover the transaction identified.
- 10) We noted that items identified by prohibited codes were paid through verbal waivers by the responsible parties; however, there was no evidence that OCP has a formal process in place to address the items requiring waivers.

Management's Response:

Review of Purchase Card Reporting Requirement

- OCP agrees with the finding that only one quarterly report (Q4/year end) was submitted to Council in FY 2008.
- The Council reports were manually compiled from individual hard copy reports from agencies. Apparently in the first three quarters, OCP was missing a few of the individual agency's reports and it was decided not to submit the reports to Council because they were incomplete. We now (in FY 2009) can pull data in the reports directly from the financial system and from the purchase card bank system, and no longer need to rely on paper submissions from the agencies.
- The finding also highlighted that the last 11 days of the fiscal year were not included. The purchase card is on a billing cycle that runs through the 20th of the month. Because the report was manually compiled from paper reports from each agency — based on the bank statements/billing cycle — we were unable to easily isolate the transactions that occurred during FY 2008 (from September 20-30) that were part of the October 20 billing cycle.
- The new purchase card program (begun November 30, 2008) is with a new bank partner that has a more robust electronic access tool that will allow OCP to run automated quarterly reports. These reports can also be run by transaction post date, in order to capture data through the end of the fiscal year, regardless of whether it falls in the middle of a billing cycle.

Transaction Usage

These are findings related to documentation maintained by agencies, not OCP. OCP has no information about which agencies were missing documentation and why. It should be noted that the new Purchase Card Policies and Procedures have eliminated paper from the process (other than receipts), so transaction reviews, approvals, and disputes will be performed and archived in the system. Further, many vendors provide item level information to the bank, which is captured in the system.

Process: Disbursements

Also, original receipts will stay on-site with the Agency Program Coordinator rather than be sent via interoffice mail to the Office of Chief Financial Officer (OCFO). If the current automated system and procedures were in place, most of the findings would be removed.

Official Government Usage

- There were seven findings of purchases above the \$10,000 monthly cycle limit. There was a bank inquiry to understand how one of the District's purchase cards could actually have more than \$10,000 charged on it, since these cards are supposed to have a \$10,000 cycle limit cap that would trigger a decline. From what the bank explained, these situations involved more than one transaction with the same vendor. In these cases, the vendor "called" the bank for only 1 authorization code and applied it to the second transaction as well. The second transaction pushed the cycle total above \$10,000. There was no second "call" for an additional authorization code, which would have triggered the decline. Unfortunately, there is no corrective action that the District can implement to prevent this from occurring. The total overage in these seven cases was \$2,709.60. While the District is exposed to this phenomenon occurring in the future, since there is a \$2,500 single purchase limit, the maximum amount of an overage occurring in this situation is \$2,500. (Findings 5, 6, and 7)
- We agree that OCP was unable to locate the signed delegation for increased limits in three cases. As a corrective action, OCP is now creating PDFs of all delegations, maintaining an electronic file of these PDFs, and emailing a copy to the cardholder. (Finding 8)
- We agree that the single purchase limit increased authority did not cover the date of the purchase — it was made a few days later. It is unclear why the limits were not reduced in the system upon expiration of the delegation. This item was also one of the items listed in Finding 8 and not another instance. (Finding 9)
- In terms of Finding 10, OCP provided evidence that all six transactions purchased with blocked MCCs were legitimate purchases and well within programmatic guidelines. As a corrective action, OCP is rewording the procedures to describe the codes as "high risk" that are blocked as an initial safeguard against possible prohibited items being purchased. There is no such thing as a prohibited MCC, but the procedures do imply this as they are currently worded. MCCs are an imperfect method for preventing prohibited purchases since many legitimate items may come from a vendor who selected a "high risk" MCC. The concern/focus of the procedures should be on the items purchased, not on the MCCs. When cardholders get a decline due to a blocked MCC, they are instructed to call the Program Management Office to explain what item is being purchased. It is not reasonable to expect a written request/formal approval in these situations — expediency is required when the cardholder is at the register. The safeguard to ensure items are legitimate is the approval process/Agency Review Team scrutiny. There will not be a formal waiver process pursued when the item being purchased is within policy guidelines.

Direct Vouchers

Before a payment is approved and payment information is submitted to SOAR, the District's accounting system of record, the disbursement should be supported by a requisition, a contract (if amount is over \$100,000), a purchase order, an invoice, and a voucher. However, the District has made an exception for certain types of payments under the Financial Management and Control Order No. 07-004 where certain types of expenditures are excluded from the requirement and that all expenditures should first be obligated in SOAR.

During our review of 45 vendor files, we noted the following:

Process: Disbursements

- 1) In 9 instances, the expenditures did not meet the requirements of the Financial Management and Control Order No. 07-004 line no. 29, where rent should be obligated at the beginning of each new fiscal period by either contracts or purchase orders starting October 1, 2007 and the expenditures did not meet the requirements under the Financial Management and Control Order No. 07-004 line no. 25, where unauthorized commitments should subsequently be ratified.
- 2) In 2 instances, the expenditures were long term treatments that did not meet the requirements of the Financial Management and Control Order No. 07-004 line no. 20 and the expenditures did not meet the requirements under the Financial Management and Control Order No. 07-004 line no. 25, where unauthorized commitments should subsequently be ratified.
- 3) In 3 instances, the District was unable to provide invoices supporting the expenditures incurred.

We noted a lack of adherence to internal controls which require that funds be first obligated in SOAR before payment occurs unless the type of expenditure is specifically excluded from such requirement as listed under the Financial Management and Control No. 07-004.

We recommend that personnel in-charge of authorizing transactions paid as direct vouchers should strictly comply with the Financial Management and Control Orders prior to authorizing any payments. In addition, the District should strengthen its review and approval processes at both the agency level and at the Office of Financial Operations and Systems to ensure that all transactions paid as direct vouchers are adequately supported and meet the necessary criteria.

Management's Response:

The following response was provided by Office of Financial Operations and Systems (OFOS) personnel:

The Office of the Chief Technology Officer (OCTO) has no involvement in the authorization and/or disbursement of District Government funds to vendors, either through the regular procurement/payment process, or through the use of direct vouchers for goods and/or services, transfers, pass-throughs or other items that can not be obtained through the regular procurement/payment process. While OCTO processes check payments to vendors through the use of their computers, they have no responsibility for initiating, authorizing, and/or approving the underlying transactions that, when done properly, will result in the processing, printing, and disbursing of vendor checks.

Issue #1: Last year, the Office of Financial Resource Management (OFRM), inquired about whether OFOS was going to extend OFRM's authority to use direct vouchers to pay rent. This was because CFO Order No. 07- 004 had indicated that rents would not be included as an exception under Item #29 - Fixed Costs because OFRM had promised in 2007 that a mechanism to obligate rents at the beginning of FY 2008 would be created.

It was discovered, at that time, that the obligating mechanism had not been established, and the person who had made that assertion was no longer at OFRM. OFOS requested a written description of the reason for the delay in the process, and an up-to-date justification for rents to be added back to Item #29. OFOS did not receive the requested justification, and OFRM, apparently continued operating as they had up to September 30, 2007. OFOS did not send an E-mail explicitly authorizing OFRM to continue that practice, but it was understood that such an authorization would be forthcoming, pending the requested information, and an OFOS review of their request, that would be added to the updating/revision of CFO Order No. 07-004.

Process: Disbursements

OFRM has subsequently sent the request, dated February 4, 2009. OFOS has promised OFRM that the issue of fixed costs, especially rents, would be included in the draft to update CFO Order No. 07-004 that is to be completed and sent out for comments by the end of this month. The payment of rents is considered an appropriate use of the direct voucher process, but, even so, OFOS is pushing for agencies that use the direct voucher process to include as much documentation into both PASS and SOAR to support the continued use of such authority, and to also have such documentation available on-line to demonstrate adherence to District procurement and payment policies and procedures.

The Office of the Chief Financial Officer issued CEO Order No. 08-008 to require that documentation be entered in PASS for the "payment of any bills, invoices, and other evidences of claims, demands, or charges against the District" for: (1) contracts; (2) letter contracts; (3) settlement agreements; (4) judgments or court orders, and; (5) grant agreements. These requirements will be added to the revision of CEO Order No. 07-004.

Issue #2: These direct vouchers would have been entered by the Health and Human Services Cluster, and do not need to be reviewed and approved by OFOS. Unauthorized commitments would have to have been ratified by the Office of Contracts and Procurement, prior to their ending that practice last year. OFOS cannot, and does not, ratify unauthorized commitments.

Issue #3: OFOS does not concur with the findings, and, in the normal course of reviewing CEO Order No. 07-004 for any items that should be covered, or changes in the execution of direct vouchers, will be updating the District's direct voucher policy and procedure within the next two-months.

The following response was provided by Government Operations Cluster (GOC) personnel:

All payments are issued by the Office of Finance and Treasury. Within the Government Operations Cluster (GOC), all payments are made from a purchase order that originated in PASS, except for those expenses identified under the Financial Management & Control Order 07-004. In response to bullet #1, a revised Financial Management & Control Order was released that included rent as an allowable direct payment. Rent is a fixed cost similar to the other fixed costs such as electricity, fuel, security, etc. Rent has always been paid by direct voucher just as the other fixed costs. There was a consideration to pay rent based upon a purchase order; however, it was deemed that this was not feasible. As a result, OFOS revised the Financial Management Order and sent an email indicating that it was okay to continue to pay rent as a direct payment. In response to bullet #2, the GOC does not make medical payments for long term disability. The GOC only makes payments for short term disability through the Office of Risk Management. In response to bullet #3, all paid invoices are maintained in a file.

Lack of Adequate Supporting Documentation

During our review of 77 vendor files, we noted the following:

- 1) The District was unable to provide sufficient supporting documentation for 3 journal entries, thus we could not determine whether the transactions were properly recorded and classified. The SOAR journal voucher provided stated that the purposes of the journal entries was to reallocate intra-District funds to different administrative units or object codes or to reclassify amounts from one fund group to another. However, based on the supporting documents provided, we were unable to conclude that these journal entries were properly classified and recorded.

Process: Disbursements

- 2) In 1 instance, the District was unable to provide the supporting invoice.
- 3) We also noted that other intra-District transactions were inadequately supported. This was apparent in some cases, where we attempted to trace the transfers to the actual costs incurred by the transferring Agency. We also noted that the buying Agency did not obtain documentation of the items purchased from the selling Agency.

We recommend that the personnel in charge of authorizing payments or recording transactions should comply with established internal controls to ensure that documentation is complete before authorization of payments and implement measures to ensure that all journal entries are supported by adequate documentation. We also recommend that the District review and revise its documentation policy regarding intra-District transactions. Lastly, the availability of records is critical and management should institute certain procedures and decide on a systematic manner of filing and retaining documents.

Management's Response:

The District has adequate supporting documents for its transactions. Concerning the comment on the buyer obtaining documentation of the items purchased from the seller, the District promotes a paperless system; hence, only the seller agency maintains the supporting documentation (i.e. invoices) which is available upon request by the buyer or other parties.

Subsequent Disbursements

During our search for unrecorded liabilities, we noted the following:

- 1) The District had not recorded liabilities in the amount of \$22,098,565. These liabilities pertained to transactions which should have been posted to the capital and operating funds at year-end. This resulted in an understatement of liabilities and expenditures at September 30, 2008.
- 2) We also noted that expenditures in the amount of \$975,868 which pertained to FY 2009, had been improperly recorded in FY 2008.

It appears that controls over the recording of liabilities are not operating effectively and that personnel responsible for recording financial transactions are not adhering to proper cut-off.

Proper cut-offs are critical for the accuracy of the accrual basis of accounting and even though the District made the necessary adjustments during the audit process, we recommend that the District strengthen its oversight and monitoring controls to ensure that all transactions are recorded in the proper period and to ensure an improved system of fiscal management.

Management's Response:

The Government Operations Cluster (GOC) records liabilities as soon as we are made aware of them. The GOC records liabilities for both operating and capital funds.

The amount of \$22 million is likely related to liabilities that were not recorded city-wide and not just related to the Government Operations Cluster. The GOC will continue to record liabilities as we become aware of them and continue to work to ensure that expenditures are recorded under the correct fiscal year.

Process: Disbursements

Purchase Orders and Requisitions

During our testing, we noted several instances during which the purchase order issue date preceded the final approval date on the requisition. Upon further inquiry, we were informed that there was a system flaw for which the Office of Chief Technology Officer (OCTO) failed to identify and correct on the requisition print screen.

Purchase orders should only be issued after all required approvals on the requisitions are obtained.

Management's Response:

The District affirms that it is not possible for the ordered date to precede the final approval date. However, there is a problem with the print view in the Procurement Automated Support System (PASS) where some of the approval dates are displayed incorrectly. The problem was introduced with the Ariba upgrade in September 2008. The underlying data, however, is still correct. Upon examination of the actual audit log found within the PASS user interface, the actual approval and PO issuance dates are found in the proper sequence. The District notified Ariba, Inc. of the problem when the issue was found and Ariba is working to correct it. The fix is complete and is scheduled for PASS release 3.10 (May 2009).

* * * *

Process: Management of the Disability Compensation Program

The District through the Office of Risk Management (DCORM) administers a disability compensation program under Title XXIII of the District of Columbia Comprehensive Merit Personnel Act of 1978.

Tort Liability Claims

We noted the following exceptions during our testing of 45 sample items. The exceptions were directly related to the system change from Risk Master, DCORM's former claims database for tort liability to American Technical Services, Inc. (ATS), the claims database that replaced Risk Master effective September 23, 2008. Whenever a system change is made, there must be adequate controls in place to ensure that all of the information is completely and accurately transferred from the older system to the new system.

- 1) In 5 instances, there was a reserve established against a closed claim. The reserve should have been cleared upon settlement of the claim; however, it remained outstanding on the books. This would result in an overstatement of the liability accrual at year-end.
- 2) In 12 instances, claim settlements were made subsequent to year-end; however, these were reported as payments during the fiscal year. Since these claims had not yet been settled as of September 30, 2008, they should have been recorded as part of liability accrual. This would result in understatement of the liability accrual and overstatement of payments made at year-end.
- 3) In 5 instances, claims were not properly reported as either a closed claim or an open claim. If a claim was closed prior to year-end, it should be reported as a closed claim; however, if closed subsequent to year-end, it should be reported as an open claim as of year-end. This would result in the liability accrual being inaccurately stated as this affects the Incurred But Not Reported (IBNR) computation.
- 4) In 1 instance, the date of loss was erroneously recorded.
- 5) In 3 instances, payment was recorded twice through the system. This would result in an overstatement of payments.
- 6) In 1 instance, settlement had already been made to the claimant; however, payment was not reflected in the system. This would result in an understatement of payments made.
- 7) We also noted that claims subject to litigation are handled separately by the Office of the Attorney General (OAG). Although the claim is initially encoded into the system, there is no way of knowing the progress of the claim unless it has been settled. At least every month, OAG sends a pro-law report to DCORM which shows the status (i.e. closed), disposition outcome, disposition date, and disposition value of the claims forwarded to them. However, this report is only used by DCORM to update the claim status in the system. DCORM had to manually correct the database submitted for actuarial valuation purposes to include claims handled by OAG. As such, there is a risk that tort liability claims reported may not be complete.

We identified these differences from a sample of items that had been selected for testing. Management should recognize the possibility that additional discrepancies may exist. In addition, we noted delays in the time from when a claim is reported to the time it is ultimately paid. This has been noted to occur because tort liability claims are paid by each District agency separately. In order to increase efficiency and reduce the time it takes to pay a claim, we recommend that the District consider that the claims payment process be centralized at DCORM.

Process: Management of the Disability Compensation Program

We also recommend that management explore the functionality of ATS to lessen manual processing and avoid differences such as the ones noted above. Strong internal controls over the tort liability claims process should be maintained to ensure that all claims have been properly processed and documented. Reviews should be present to detect possible errors, particularly when the current system in use is new.

Management should also maintain a complete and adequate documentation trail of claims handled separately by OAG. A procedure should be implemented to regularly update DCORM of the status of those claims and to document them in the claims database such that completeness of data is ensured.

Management's Response:

- 1) This issue resulted from the claims being transferred from the Risk Master System to the new ATS System. The issue causing the closed claims with reserves posted has been resolved and all of the claims are balanced. The ATS Regional Account Manager made a run of all claims with this error and made the corrections.
- 2) Claim settlements were not made subsequent to year-end, the claim payment was requested during the fiscal year and documented in the notes but the actual payment was issued by the various agencies subsequent to year-end. DCORM does not issue any checks, therefore the notes reflect requesting payment (this process is sending a payment request form to the agency with the amount in which to issue the check for claim settlement). New wording such as "Claimant's release and W-9 sent to the agency" will be placed in the notes when requesting a check to be issued. The Claims Handling Manual has been updated with this additional requirement.
- 3) The 5 instances where claims were not properly reported as either closed or open was a conversion error from Risk Master to the ATS system. This error has been corrected. The ATS Regional Account Manager conducted a run of all claims without an open or closed date and updated the status of the claims. DCORM tested and confirmed the correction.
- 4) The erroneously recorded date was a system transfer error; the claim event date was left blank in Risk Master; as the transfer took place, the ATS system defaulted to and filled in the blanks with 1-9-1900. The date of loss was recorded in the system and corrected.
- 5) No duplicate payments were issued. This was an ATS system error with recording the names in only one format. For example, Doe, John went into the system when the file was set up and the payment was documented as John Doe. ATS is for documentation only; no payments are issued out of DCORM. This process has been corrected and the Claims Handling Manual has been updated with the new procedures. Only the Claims Specialist will document payments in the ATS system to avoid any confusion.
- 6) To address the 1 instance where settlement was already made to the claimant, settlement was not made; the notes reflect that there was a negotiation and the payment was issued two months later by the agency.
- 7) In response to DCORM manually correcting the database in regards to OAG litigated claims, DCORM and OAG will communicate monthly to update the movement and status of the litigated claims into the ATS system. DCORM will receive the pro-law reports from OAG and input the final disposition of the claims into the ATS system, therefore, eliminating the manual process.

Process: Management of the Disability Compensation Program

Fire and Emergency Medical Services (FEMS) Claims

We noted the following exceptions during our testing:

- 1) In 10 out of 18 claims tested, differences were noted with the hourly rates when compared to the information obtained from PeopleSoft. Hourly rates to compute the claimant's benefits should be determined through the latest salary received prior to the injury. This would result in benefits payments and the liability accrual being inaccurately stated.
- 2) In 7 instances, either no disability hours were entered into the system or no hourly rate was entered into the system. After manually calculating the benefits and completing FEMSD Form 44, information is encoded into the system. However, no reviews are done to check whether the information as it appears in the hard copy form is accurately transferred to the system. This would result in benefit payments and the liability accrual being inaccurately stated.
- 3) In 1 instance, the FEMSD Form 44 did have the approval of the Battalion Fire Chief and company officer notified. These controls are important to determine whether there is concurrence with the incident reported by the claimant. If this control is not strictly implemented, there is a risk of paying benefits on invalid claims.
- 4) In 3 instances, differences were noted with disability hours when compared with the results per our independent calculation. This would result in benefit payments and the liability accrual being inaccurately stated.

We identified these differences from a sample of items that had been selected for testing. Management should recognize the possibility that additional discrepancies may exist.

We recommend management make every effort to closely follow its review process over FEMS claims handling procedures particularly as this involves a large amount of manual processing, which is inherently prone to error. Proper segregation of duties must be ensured such that preparation and review functions are not combined in only one person. Management may also consider linkage of required information from PeopleSoft and Roster to lessen manual intervention and avoid recurrence of such differences. Stricter controls prior to accepting claims for processing, particularly concurrence by the supervising officers, should be implemented to ensure that benefits payments are made only for valid claims.

Management's Response:

The Fire Department is in the process of getting a program in place to generate reports from PeopleSoft for accurate amounts of Salary-Hourly Rate(s) and also for Administrative-Sick Leave (Performance of Duty) taken. Once in place, we believe this will eliminate the discrepancies.

Data in Actuary Report

The District's actuarial report should be complete so that it can be relied upon for a comprehensive analysis of the loss and loss expense reserve liability related to worker's compensation. DCORM should provide certain analyses and data information to the actuary in order to achieve a completed report. During our review of the 2008 report, several conditions were noted as follows:

Process: Management of the Disability Compensation Program

- 1) We noted significant increases in pre-1983 claims case reserve. The claims over prior periods have increased significantly over the past two to three years. If this trend continues, we believe DCORM management should communicate this to the actuary on an ongoing basis and this should be factored into the assumptions to determine the overall IBNR liability.
- 2) The actuarial report stated that there were a large number of open general liability claims with a zero incurred value and that the case reserve was probably understated. Additional analysis should be done to determine whether a reserve should be established for these claims.
- 3) The current claims administrator for DCORM is CMI, Inc. While all outstanding claims have been transferred to CMI, the history of closed claims was not transferred to CMI. As a result, there is no current record of these claims.
- 4) As time goes on, DCORM will have the ability to track paid and reported losses by date of evaluation but at the current time only three years of history is available.
- 5) DCORM, along with the actuary, should compile an exposure base, such as payroll, to monitor ultimate loss trends, such as frequency and severity, by policy year.
- 6) DCORM should establish a process to monitor changes on case reserves for older claims on a quarterly basis. As an example, DCORM's actuaries based their estimates on the assumption that the reserves for pre-1983 claims were adequate, despite reserves actually increasing over the last two years substantially.

We recommend that DCORM should institute a procedure for communication between DCORM, the DCORM claim processors, and the DCORM actuaries, for all material reserve changes, regardless of the claim year, along with auditable rationale for making such changes. We also recommend that the actuary should perform the above analyses to help compare the trends and other statistics related to the computed liability, and therefore satisfactorily explain changes in the liability related to worker's compensation. DCORM and its claims processing organization will have to provide the necessary data to the actuary, in order to enable the actuary to perform these analyses.

Management's Response:

Issue #1: As previously discussed with the actuary and auditors, there have been significant increases in pre-1983 claims primarily due to an increase in adverse awards and settlement payments made to claimants that resulted in a significant number of aged claim files being closed and claimants being removed from the Program. A change in status from temporary total disability to permanent total disability was another reason for significant reserve increases. Such changes are the natural progression for old claims that are constantly being monitored and updated. In addition, steps have been taken to consolidate pre-1983 claims so that only one claims adjuster is responsible for handling and monitoring these issues. This will allow DCORM to closely monitor reserve changes and communicate these trends to both Senior DCORM management as well as the actuary. All reserve trends are reviewed in determining our overall IBNR liability.

Issue #2: The large number of open general liability claims with zero incurred reserves are claims that were not captured in a reserve category during the system conversion from Risk Master to the new ATS System. This has been corrected by the ATS Regional Account Manager and reserves have been adjusted and tested for accuracy.

Process: Management of the Disability Compensation Program

Issue #3: When the CMI's contract began, CMI received an electronic transmission of all open and closed file data from the Risk Master Disability Claims Management System. CMI was subsequently purchased by Sedgwick CMS who currently holds the Disability Compensation Program's contract. When the CMI system was replaced by the JURIS system, data was transferred in its entirety to the new claims handling system. Prior to the RiskMaster claims system, files were handled manually. DCORM currently has hard copy closed files stored at D.C. General. It is well documented that prior to the creation of DCORM, the Disability program was improperly handled and was moved from TPA to TPA with little regard for the condition of the files. During the many transitions closed claim files were lost. While DCORM has attempted to recreate some of these closed files, we were not able to recreate all of them.

Issue #4: This statement is accurate. DCORM concurs.

Issue #5: Per last year's audit findings, DCORM has compiled an Exposure Analysis for the DCP claims. It is included on Exhibit WC-4, page 2 and referenced on page 10 of the report.

Issue #6: Based on last year's findings, DCORM has contracted with an actuary to work closely with the DCP Program and monitoring reserve changes and trends. Currently this review is done on a 6-month basis which can be modified to a quarterly basis. Currently we have 133 pre-1983 open claims, which are primarily pension files that are managed by one Sedgwick adjuster. Keeping track of changes has been simplified because of the utilization of one focused claims adjuster. DCORM will run a detailed report and discuss with our actuary, reserve adequacy and action plans.

* * * *

Process: Fixed Assets

Inventory of Fixed Assets

The District has an investment of approximately \$7 billion in depreciable and non-depreciable assets and we recommend that controls be strengthened in this area. Most fixed assets, except items classified as personal property, have not been physically inventoried in recent times.

We also noted that although the District conducted a physical inventory of personal property in FY 2008, the results have not yet being reconciled to the fixed assets subsystem; hence, assets that may have been scrapped, misplaced, or otherwise deemed unusable may continue to be considered "in service."

A physical count of property should be periodically taken, compared to the items carried on the detailed subsidiary records of property and equipment, and significant differences investigated. The establishment of updated subsidiary records will assist the District in maintaining control over individual assets and provide a means whereby information pertinent to the property and equipment assets can be kept up to date. Such physical counts will also help detect the loss or unauthorized use of valuable property.

Management's Response:

The personal property physical inventory was completed on September 30, 2008. We are aware of the necessity to reconcile the inventory results with the fixed asset subsystem. Because this effort is a manual one, it occurs over several months, and we simply could not complete the reconciliation before the year-end audit. The reconciliation will be complete by March 31, 2009.

The Office of Financial Operations and Systems (OFOS) will review the feasibility of conducting a Real Property inventory while taking into account the budget constraints that the District is currently operating under.

Classification of Capital Expenditures

We noted that a purchase of washers and dryers for the Department of Mental Health was expensed through repairs and maintenance instead of being properly classified as a personal property capital expenditure. We also noted that the Office of Unified Communications improperly classified advertising campaign expenditures as repairs and maintenance expenditures; these should have been reflected as advertising or professional/contractual services expenditures.

It is important to maintain correct classification of expenditures so that management can accurately report the financial results of the District and we recommend that the District improve and strengthen its controls over proper recording of expenditures in the system. It should be noted that we identified these discrepancies from a sample of transactions that were selected for testing. Management should recognize that the potential exists for additional discrepancies.

Management's Response:

The following response was provided by Department of Mental Health personnel:

The Saint Elizabeth's Facilities and Environment Department (FED) Director will ensure that staff that is responsible for managing contracts and purchases is fully aware of the correct classification of expenditures in order to ensure proper recording in the system.

Process: Fixed Assets

The following response was provided by Office of Unified Communications personnel:

The Office of Unified Communications incorrectly charged advertising expenditures to repairs and maintenance. This was an isolated error. Management will review all expenditures as part of the quarterly Financial Review Process (FRP) to ensure correct classification.

Personal Property

According to existing policies and procedures, purchases of fixed assets must be added to an agency's fixed assets listing, as maintained on the Fixed Assets System (FAS), within 3 working days from the date of payment for the respective fixed asset.

During our sample test work over personal property additions, we noted that an acquisition by the Judicial Nomination Committee agency was included in the list of additions for FY 2008 but had actually been purchased in FY 2007. The acquisition was recorded in FAS over six months after it was purchased. Issues like these can lead to an understatement of depreciation expense and fixed assets acquisitions. District agencies should have proper controls in place to ensure that fixed assets and relevant information (i.e. cost, useful life, in service date, asset class, etc.) are entered into the system accurately and in a timely manner.

Management's Response:

Management does not concur with the finding. The records show that the item was received on September 28, 2007 and the value of the asset was accrued in the accounting records in FY 2007. However, the invoice for payment was not received until November. Further, that payment was effected on November 28, 2007 and the asset was recorded in the fixed asset system with that effective date.

It is the agency's determination that this transaction had no negative impact on both the FY 2007 and FY 2008 financial reports.

Confiscated Property

Based on existing District policy, we attempted to trace the values, via a sample of 3 confiscated vehicles, by agreeing them to the National Automobile Dealers Association (NADA) website. All 3 vehicles were recorded at a lower value than listed on NADA's website.

It is important to accurately value properties so that management can accurately report financial results. We recommend that the District improve and strengthen its controls in this area and ensure that existing policies are followed or if there are any exceptions to existing policies, that these are clearly documented and evident.

Management's Response:

These assets are used by the NSID Unit for undercover operation and, as a result, there are significant controls placed on these assets. Despite the NADA valuation, Fleet Management has responsibility to determine the final valuation that should be placed on assets and uses the condition of the property when it enters the fleet.

Process: Fixed Assets

Baseball Project Expenditures

It appears that the Office of the Chief Financial Officer (OCFO) records expenditures without review of proper documentation for accuracy and validity of transactions. The OCFO records transactions based on information provided by the District of Columbia Sports and Entertainment Commission (i.e. e-mail, Excel spreadsheets, etc.), but does not review supporting documentation (i.e. vendor invoices) to verify transaction prior to posting. We noted the following:

- 1) Approximately \$27,000,000 was recorded as FY 2008 expenditures, although an accrual for that amount had also been recorded in FY 2007. An adjusting journal entry was recorded during the audit process.
- 2) We noted another journal entry recorded by the District for \$1,100,000. The journal entry was recorded to reduce FY 2008 accruals; however, supporting documentation was not obtained and reviewed to determine if the transaction was accurate and valid.
- 3) We also noted that there is one individual recording journal entries related to the Baseball Project and that there is no subsequent management review of these entries.

The District must strengthen controls to ensure that transactions are only recorded when the necessary documentation has been obtained and management has determined that transactions are valid and accurate. In addition, transactions recorded in the system must be reviewed and approved by an individual other than the one preparing the journal entry. This process would improve controls over adjustments to the general ledger.

Management's Response:

We partially concur with the finding. Full disclosure of the payment process for stadium invoices provides clarification. For stadium expenditures, the District of Columbia Sports and Entertainment Commission (the Commission) OCFO staff submit approved invoices to the Office of Finance and Treasury (OFT) and the Office of Economic Development Finance (EDF).

EDF and OFT review these; then upon approval from the Treasurer, OFT advances funding to the Commission to make payments to the vendors. After this disbursement has occurred, the Commission then sends reports, including the cash report used for recording expenditures in SOAR, the District's accounting system of record, to EDF which reviews them for release to the Council. Once these reports are approved for release, they are forwarded to OCFO Financial Operations for recordation in SOAR. All disbursements processed at the Commission are reviewed and approved by OCFO personnel at the Commission both prior to requesting the cash for disbursement and upon disbursement. The final recordation entries based upon these reports are also reviewed monthly by EDF.

As the accrual is for activities which occurred in the fiscal period but did not have expenditures, the review of OFT and transfer of cash did not occur prior to 9/30. The invoice information was, however, forwarded to OCFO Financial Operations through EDF. The final adjustment was made to mirror adjustments made on the books of the Commission at the request of their auditors.

The Office of the Chief Financial Officer has already made some changes to the process as outlined in the finding. All quarterly expenditure journals in FY 2008 were prepared by the Financial Systems Specialist, entered into SOAR by the Senior Accountant, and reviewed and approved by the Controller. It is only the accrual that missed this treatment — which will not happen again. The OCFO will continue to employ a division of responsibilities to minimize the risk of error in recordation of stadium costs.

Process: Fixed Assets

Unrecorded Land Swap

While performing our audit procedures related to fixed assets, we noted that the District exchanged land (a portion of the land where the old Convention Center was located for a portion of land across the street from the new Convention Center to build the Convention Center headquarters hotel). However, the transaction was not recorded in the Fixed Assets System. In addition, the effect of the transaction was not reflected in the District's financial records.

The District must strengthen its review process in the fixed assets area to ensure that all transactions are properly reviewed, reconciled, and recorded.

Management's Response:

The Office of Financial Operations and Systems (OFOS), together with the District agencies, will create a process whereby acquisitions and dispositions of real property noted in the media and elsewhere will be investigated and the documents supporting such transactions will be obtained and held in a central file at OFOS to support the disclosures made in the Comprehensive Annual Financial Report (CAFR).

Also, periodic follow-up with the Office of the Attorney General's Real Estate Section should ensure that all title transfers to and from the District are accounted for on a timely basis.

* * * *

Process: Management of the Postretirement Health & Life Insurance Trust

Accounting for Daily Activity

During our audit process, we noted the following:

- 1) Several assets and liabilities were not recorded or were improperly recorded. The liability related to premiums payable to insurance carriers was initially not reflected on the books and records. This was due to the District's policy of recording expenses when paid as opposed to when they were incurred. Further, although deemed insignificant to overall operations, the District did not record any receivables related to contributions from retirees.
- 2) The financial statements were not prepared in a timely manner and the balances were changed several times during the course of the audit. Further, auditable support for certain balances included in the financial statements was difficult to obtain and alternate methods were required to satisfy audit procedures.
- 3) Amounts related to beginning of year net assets, investment income, and investment losses were not correctly presented or reported on the financial statements provided for our review. In addition, several required note disclosures were missing, along with certain required supplemental information.

We recommend that management should strengthen its processes to ensure that the financial statements are accurately presented and that financial activity is recorded in a timely manner.

Management's Response:

Most of these comments were addressed with the release of the final version of the financial statements and net assets were correctly reflected. Financial statements were delivered as soon as possible. The District hired a new firm to assist with the preparation of the financial statements and this contributed to the time required to complete the reports. The statements were changed several times in response to comments received from various parties who reviewed them. We will review procedures to record assets and liabilities and we will make changes if they are appropriate.

Data in Actuary Report

The District's actuarial report should be complete so that it can be relied upon for a comprehensive analysis and for an accurate calculation of the ending liability. The District should make every effort and ensure that certain analyses and data information are provided to the actuary in order to achieve a completed report. During our review of the 2008 actuarial report, several conditions were noted as follows:

- 1) An estimated salary increase of 5% was used in the actuarial valuation; however, it is noted that on average, the salary increase for the past several years has not been more than 3-4%. This has the effect of overstating costs in initial years and understating costs in succeeding years.
- 2) There were several changes in assumptions that were not disclosed in the actuarial report and it was unclear who had taken full responsibility for all the assumptions used in the valuation.
- 3) The report did not include a description of how administrative costs were being funded.
- 4) While deemed relatively insignificant, we noted that there was no separate analysis conducted on the portion of the Plan which relates to the life insurance liability.

Process: Management of the Postretirement Health & Life Insurance Trust

- 5) There were participant data inconsistencies which resulted in significant changes to the amount of the actuarially determined liability during the audit process.

We recommend that the District should institute a procedure for clear communication with the actuary and that the actuary should perform certain analyses to help compare trends and other statistics related to the computed liability, and therefore satisfactorily explain changes. The District will have to provide the necessary data to the actuary, in order to enable the actuary to perform these analyses.

Management's Response:

Management will work with the actuary to make sure an industry standard for salary increases is used when calculating the actuarial valuation. Management will also address other weaknesses that were identified in the finding; specifically, findings related to the data provided to the actuary and the communication between management and the actuary.

* * * *

Process: Management of the Medicaid Program

Findings of the Medicaid Fraud Control Unit

The Medicaid Fraud Control Unit (MFCU) is a unit of the Office of the Inspector General (OIG) that has a dual mission. It investigates and prosecutes Medicaid providers who engage in fraudulent billing. The MFCU also investigates and prosecutes the abuse, neglect, and financial exploitation of persons who reside in Medicaid-funded facilities.

As reported in the District's FY 2006 and FY 2007 Office of Management and Budget Circular A-133 Audit Report, the Medical Assistance Administration (MAA) is not referring all potential fraud cases directly to MFCU. The MAA's Office of Surveillance and Utilization (SUR) is mandated to perform surveillance and utilization reviews that monitor and control improper or illegal utilization of the program by the providers and recipients of medical services and make referrals to MFCU if they suspect fraud or abuse.

However, it was noted that the SUR unit is referring potential fraud cases to the Office of Investigation and Compliance (OIC) within the Department of Health (DOH) instead of referring the cases directly to the MFCU. The OIC conducts an investigation into the potential fraud case and then after inquiry and data gathering, refers the case to MFCU. This is a duplication of effort for OIC and interferes with MFCU investigating potential fraud cases once the case is referred to them.

On May 27, 2003, a Memorandum of Understanding (MOU) was signed between the MFCU and MAA. The MOU delineates the terms and conditions for both parties. Specifically, it requires that MAA refer matters when they have suspicion of fraud. Based on discussions with MFCU, there has been no improvement in the current situation and the number of cases being referred from MAA remains minimal.

We recommend that MAA comply with the terms and conditions of the MOU and make SUR referrals directly to MFCU.

Management's Response:

Based on comparative data collected by the Department of Health Care Finance (DHCF) (formerly the Medical Assistance Administration), and an analysis conducted by the Federal Office of the Inspector General, the number of referrals the District's Medicaid program makes to the District's MFCU is comparable to the number made by other states, given the size of the District's program.

For example, DHCF referred 5 cases of suspected provider fraud over a one year period. DHCF's 5 referrals per 150,000 beneficiaries is higher than neighboring jurisdictions of Maryland and Virginia who only referred 9 of 600,000 and 8 of 750,000 respectively. Furthermore, a 2007 Federal Office of Inspector General report, found that nationwide, MFCUs reported receiving 13,733 suspected fraud referrals over a 3-year period, of which 29 percent of the referrals came from State Medicaid agencies.

In December 2008, a new Memorandum of Understanding (MOU) was executed between MFCU and the District's Medicaid program, which clarified the process whereby the Medicaid program is to make referrals to MFCU. This MOU, in part, states that the Medicaid program will:

- "1. Conduct a preliminary investigation to determine whether there is sufficient basis to warrant a full investigation if it receives a complaint of alleged Medicaid fraud or abuse (as defined by 42 CFR § 455.2) from any source or identifies any questionable practices, as required by 42 CFR § 455.14.*

Process: Management of the Medicaid Program

2. On a quarterly basis, discuss with the MFCU the DHCF preliminary investigations it has completed in the prior quarter and has determined warrant a full investigation. If, after discussion, the MFCU and DHCF determine that these matters involve potential fraudulent activity, the DHCF will directly refer these matters to the MFCU."

These and other provisions of the MOU are expected to help achieve improved understanding of the federal requirements with respect to Medicaid referrals to MFCU, and the number of referrals that should reasonably be expected. DHCF is committed to abiding by the terms of the MOU and continue making appropriate referrals to MFCU in FY 2009.

* * * *

Process: Health Care Safety Net

Participant Eligibility

The Department of Human Services' Income Maintenance Administration (IMA) is responsible for determining participant eligibility for the District of Columbia Healthcare Alliance Program (the Program) and uses the Automated Client Eligibility Determination System (ACEDS) to evaluate the eligibility of the participant.

The IMA Policy Manual, Part VII Chapter 4, establishes residency requirements for the Program and the IMA Policy Manual states that, "To be eligible for program benefits, a person must be a presently living in the District of Columbia voluntarily and not for a temporary purpose and have no current intention of moving out of the District." The Code of District of Columbia Municipal Regulations, Title 22 Chapter 33 - *Health Care Safety Net Administration*, sets forth the policy and requirements for enrollment in the Program. Specifically, the Code's section 3304.3 states that, "In verifying an applicant's eligibility, IMA shall accept any form of proof that reasonably attests to District residency, income, and resources." This language in the Code is very vague and provides loopholes for applicants to apply for and be accepted in the Program.

During our review of eligibility for 45 participants which had been selected for testing, we noted the following:

- 1) 5 participant files could not be located and thus were not provided for testing.
- 2) 1 participant file did not have the signed application form.
- 3) 3 participant files did not have documentation to support District residency.
- 4) 1 participant file did not have verification of the applicant's income.
- 5) 1 participant file did not have evidence of supervisor review and approval of the eligibility determination decision.

Ineligible participants may be receiving Program benefits that they are not entitled to receive. In addition, the District may be incurring unnecessary expenditures for medical care to non-District residents. We identified these differences from a sample of items that had been selected for testing. Management should recognize the possibility that additional discrepancies may exist. We recommend that the Department of Human Services' IMA review its Policy Manual to include procedures to verify that the applicant is a District resident. In addition, we recommend that IMA review current participants in the Program and discontinue benefits for participants identified to be non-District residents.

Management's Response:

- 1) In response to those sample periods in which documentation was not available for this audit, IMA is taking the following actions:
 - IMA's Program Managers must submit a corrective action plan to address the safeguarding, proper filing, and tracking of case documents, which shall include a detailed plan for implementation of IMA procedures.
 - To enhance IMA's ability to store and retrieve records, the Department of Human Services (DHS) is in the process of conducting an assessment of IMA's case records for the purpose of procuring a contractor to scan all existing records and equipment for the ongoing scanning and maintenance of e-documents. This innovation will enhance IMA's efforts to manage case records.

Process: Health Care Safety Net

- 2) The auditor determined that the income section for this case on the recertification form was not completed nor was the recertification signed by the customer. IMA Policy requires the customer to sign the application. IMA Policy, Part 8 Chapter 4, section 10, states that if residency is established at initial application and there is no change reported at recertification, then there is no need to re-establish residency. However, because IMA cannot locate the original case record, IMA is unable verify the accuracy of the determination. Therefore, IMA agrees that this action was taken in error and IMA will implement measures to prevent such incidents in the future, including second level review of eligibility determinations by Section Chiefs.

- 3) Management does not concur with the finding.
 - The first case record contains a statement dated 1/21/2008, from the person the claimant lives with, verifying District residency. The ACEDS narrative dated 1/23/2008 reflects that the statement was verified via telephone call from this agency. This practice is consistent with IMA Policy, Part 4 Chapter 2, Section 7 which permits statements from a landlord as acceptable means of verification of residence.

 - The second case record contains current pay stubs, which reflect the customer's name and address of record and which coincides with a telephone bill verifying the customer's name and current District address, thereby satisfying the residency requirement. This is consistent with IMA Policy, Part 4 Chapter 2, Section 7, which states that utility bills are acceptable means of verification of residence.

 - The third instance refers to the case record in Finding 2. As mentioned above, the historical case record could not be located and the recertification record did not have adequate documentation to support the determination. IMA Policy, Part 8 Chapter 4, section 10, states that if residency is established at initial application and there is no change reported at recertification, then there is no need to re-establish residency. However, because IMA cannot locate the original case record, IMA is unable verify the accuracy of the determination. Therefore, IMA agrees that this action was taken in error and IMA will implement measures to prevent such incidents in the future, including second level review of eligibility determinations by Section Chiefs.

- 4) This refers to the instance in Finding 2. As stated earlier, the historical case record could not be located and the actions of the worker at recertification, pursuant to the Supervisor's instructions, were not consistent with IMA policy.

- 5) Management partially concurs with the finding. This refers to the instance in Finding 2. Supervisory review and approval for this case is noted in ACEDS and IMA is not required to sign each written application. However, as stated in findings No. 2 and 4, the historical case record could not be located. Therefore, management believes that such approval without proper documentation in the case record is inappropriate and inconsistent with IMA policy.

DHS policies and procedures for verification of residence are consistent with District law and Federal law. These procedures are addressed in IMA's Policy Manual Part IV, Chapter 2.7. In addition, IMA currently monitors various data sources, such as TALX, PARIS and BENDEX, and Maryland CARES for customer verification of public benefits, income, and/or residence in another state. Customers that received wages or benefits in another state are subject to investigation and discontinuation of benefits, upon verification. IMA policy currently requires the applicant to sign his/her application and IMA will continue to provide focused monitoring and training to address this error.

* * * *

Process: Budget and Planning

Capital Budget Corrections

Our review of the capital budget process identified various items where management should consider developing policies and procedures for better coordination, communication, and internal controls. Out of 25 projects selected for testing, we noted 1 large reprogramming that pertained to budget/technical corrections. This entry was to correct past data input errors and was processed in an effort to match the remaining project budget with data reported in SOAR, the District's accounting system of record.

While management has made progress to address these issues, we continue to recommend that OBP-Capital focus on getting these items resolved and processed effectively and efficiently and ensure that data in SOAR is a current and reasonable presentation of the capital program.

Management's Response:

The Office of Budget and Planning (OBP) continues to correct budgets in SOAR to align with authorized budgets. We have met with every agency for which budget corrections are necessary and have obtained cooperation from all agencies and the Office of the City Administrator. We are systematically correcting budget authority and allotments in SOAR, ensuring that budgets in SOAR fully reflect all authorized budget levels by project. Since the start of FY 2009, we have completed these corrections for two additional large capital agencies – the Office of the Chief Technology Officer and the Department of Parks and Recreation. OBP plans to complete this effort for all remaining agencies in FY 2009.

Lack of Written Policies and Procedures

In prior years, we noted that the capital program did not have a written policies and procedures manual. Management has represented that a manual is in process and a draft has been formulated, but the project has not yet been completed.

Written procedures, instructions, and assignments of duties will prevent or reduce misunderstandings, errors, inefficient or wasted effort, duplicated or omitted procedures, and other situations that can result in inaccurate or untimely accounting records. A well-devised procedures manual can also help to ensure that all similar transactions are treated consistently and that records are produced in the form desired by management. Further, a good procedures manual can also aid in the training of new employees and possibly allow for delegation to other employees. We recommend that management continue its efforts towards the completion of such a manual.

Management's Response:

The Office of Budget and Planning (OBP) agrees that publication of a written manual with detailed policies, practices, and procedures is essential to the delivery of accurate and timely accounting records. Many of OBP's policies and procedures are detailed in various annual and periodic publications issued by OBP to agency financial staff. These include the annual Capital Budget Manual and Capital Budget Formulation Application User Guide. The budget manual includes, for example, a detailed list of expenditure types eligible for capital budget. OBP has also published the Capital Budget Spending Plan (C-SPIN) Guide and issued a policy directive regarding capital budget personnel costs, or full time equivalents (FTEs). We are drafting all remaining portions of the manual, including entry of capital budget transactions, and will publish a complete manual in FY 2009.

Process: Budget and Planning

Lack of Compliance with the Reserve Requirement

Per the D.C. Appropriations Act of 2008, Sec. 822, the District must meet the following requirement with respect to the Emergency and Contingency Reserves:

Provided further, that 100 percent of the funds borrowed shall be replenished within 9 months of the time of the borrowing or by the end of the fiscal year, whichever occurs earlier.

Also, per the District Code Sec. 1-204.5a, Paragraph (7):

The District of Columbia shall appropriate sufficient funds each fiscal year in the budget process to replenish any amounts allocated from the emergency reserve fund during the preceding fiscal years so that not less than 50 percent of any amount allocated in the preceding fiscal year or the amount necessary to restore the emergency reserve to the 2 percent required balance, whichever is less, is replenished by the end of the first fiscal year following each such allocation and 100 percent of the amount allocated or the amount necessary to restore the emergency reserve fund to the 2 percent required balance, whichever is less, is replenished by the end of the second fiscal year following each such allocation.

We noted that the Emergency Reserve had not been replenished to the required 2% level until February of 2008. Lack of compliance with the reserve requirements can lead to inadequate amount of reserves in case of an emergency. We recommend that the Emergency and Contingency reserves are reviewed on a regular basis to assess whether replenishment is needed to meet the 2% requirement.

Management's Response:

The issue was not that amounts allocated or borrowed from the reserves were not replenished timely. The issue was that a required increase in the balance as of the beginning of FY 2008 was not executed until February 2008. There was uncertainty about the potential replenishment of certain amounts associated with one of the reserves and the calculation of the appropriate 10/01/07 balance, which was a factor in the delayed action to bring the balances to their required FY 2008 level. The 10/01/07 Target balance, as of that date, was necessarily an estimate based on projected end-of-year CAFR balances. Going forward, the Office of Budget and Planning and the Office of Finance and Treasury will ensure that the required beginning-of-year reserve balances are appropriately estimated and established at the beginning of the fiscal year, and then adjusted as appropriate once the final end-of-prior-year CAFR balances are known.

Appropriation Act Reporting Requirements

Per the 2005 District of Columbia Omnibus Authorization Act:

The Chief Financial Officer shall prepare and submit quarterly reports to the Committees on Appropriations of the House of Representatives and Senate on the certification of and amount paid by the Government of the District of Columbia, including the District of Columbia Public Schools, to attorneys in cases brought under Individuals with Disabilities Education Act (IDEA). The Inspector General of the District of Columbia may conduct investigations to determine the accuracy of the certifications.

Process: Budget and Planning

We noted the District did not prepare and submit quarterly reports to the Committees on Appropriations. Not submitting reports in a timely manner can result in potential penalties and reduced appropriations. It is recommended that each agency is informed of reports they are required to submit and that they update the Office of the General Counsel as to when the reports are due and when they are submitted.

Management's Response:

Reports will be filed in a timely manner going forward.

* * * *

Process: Inventory

Reconciling Inventory

The District maintained an inventory balance of approximately \$16,800,000 at the end of FY 2008. Of this total balance, approximately 65% is maintained at the Department of Health (DOH), the Department of Mental Health (DMH), and the Department of Transportation. We selected 32 items for our test work from these three agencies.

During our process of comparing the physical count to what had been reflected on the general ledger, we noted minor and insignificant variances throughout our sample. Some variances had understated the inventory balances and others had overstated the inventory balance. We did, however, note a larger variance of approximately \$58,000 for a pharmaceutical product at DOH and another larger variance of approximately \$27,000 for a pharmaceutical product at DMH.

We suggest that the District consider a system that would track all pertinent information in such a way that returns, damaged items, sales, and purchases would be accounted for on a more current basis. This would benefit the District by providing an up-to-date listing of on-hand products and enhanced control of the assets. Also, management's decision-making ability will be improved and timelier.

Management's Response:

The following response was provided by Department of Health Personnel:

Management researched the discrepancy, and it was discovered that an employee had incorrectly entered the wrong warehouse item number for a drug thereby receiving the wrong item into the inventory system and also failing to receive the correct item. This occurred for the same drug item on two different invoices. Essentially two receiving errors were made for the same drug item resulting in the count being off for the original item. These two errors for the one (1) drug item totaled approximately \$58,000. The correct drug item and quantities were delivered by our prime vendor as evidenced by the invoices and the correct drug item and quantities were delivered to the customer as evidenced by the pick lists. Once the receiving error was discovered by the auditors, management made the proper inventory adjustments to assure the correct information is in the inventory system going forward.

Management discussed the error with the employee directly involved and gave written directions for the future to the entire staff of the Warehouse. Management has also implemented stricter controls involving better checks and balances for all warehouse processes to eliminate preventable errors of this type in the future.

The following response was provided by Department of Mental Health personnel:

DMH does not concur with the finding.

* * * *

Process: Journal Entries

Review, Approval, and Documentation

The District has a procedure in place by which the person authorizing a journal entry document must be distinct from the person preparing the respective document. Our review over a sample of 121 journal entries revealed the following:

- 1) For 10 items, either the reviewer was the same person as the preparer of the journal entry, or it had not been documented who had reviewed and authorized the journal entry.
- 2) 7 items did not have adequate supporting documentation.

Internal controls are designed to safeguard assets and help or detect losses from employee dishonesty or error. A fundamental concept in a good system of internal controls is the segregation of duties. The District should enforce its policies which are set up to improve existing internal controls without impairing efficiency. Further, all entries should be initialed by the preparer and the individual approving them in order to attribute responsibility to the appropriate individuals.

Lastly, journal entries should always be supported by appropriate documentation where possible. Good documentation serves as an accounting record and facilitates future follow-up as well as additional insight for other users.

Management's Response:

The Office of Financial Operations and Systems (OFOS) will work closely with the affected agencies to ensure that proper documentation is provided with each journal entry and that the preparation and approval of all journal entries are properly segregated.

* * * *

Information Technology Environment: General Controls

The District's complex organization is comprised of numerous agencies that serve the public welfare. The complexities of the various decentralized agencies necessitate the use of specialized information systems that perform as stand alone modules. The data processed and housed in the different information systems is either directly or manually converted to a format that can be interpreted by the District's overall general ledger and financial reporting system, SOAR.

The District also has five (5) datacenters which are the central computer centers that provide the core data processing capabilities in the District and to the majority of the District's agencies.

During our procedures over District agencies with significant business processes, we noted many similar issues and these are outlined on the pages which follow. As a result, we recommend the following for the District as a whole and management's responses are provided on the following pages, agency by agency.

- 1) One of the basic elements of internal control is separation of duties so that no one person controls all phases of an operation. Separating certain duties improves internal controls and reduces the possibility of errors and irregularities. Access to production environments should be restricted from developers/programmers and migration of codes should be performed by designated IT personnel that are not responsible for program modifications. Additionally, the roles of the developer/programmer and the person migrating codes should be segregated. We recommend that management adopt better controls.
- 2) A formal change management methodology should be documented and enforced to ensure requested changes are documented, reviewed, the appropriate approvals are received, and changes are tested by the requesting party prior to migration into production. Inappropriate modifications to applications can cause incorrect calculations and compromise functionality. We recommend that management create a formal change management methodology that ensures documented procedures are followed. The procedure could include the following items:
 - a. Change request initiation, approvals, and sign off requirements.
 - b. Testing requirements, approvals, and sign offs.
 - c. Change request migration approval and sign offs.
- 3) Where possible, strong password controls should be implemented to strengthen the integrity of significant systems and financial applications. Some computer specialists have estimated that as much as 80% of network security breaches occur from within the network rather than from outside hackers. Security could be improved if an "intruder lockout" feature were added to the system(s) so that three or more incorrect log-in attempts would suspend the account(s). A network help desk would then have to reset the account(s). We also recommend that management consider requesting that applicable vendor(s) develop and implement application password configuration settings. In order to further reduce the risk of access to computer files by unauthorized personnel, we recommend that the District institute a policy that requires passwords to be changed on a regular basis. The District may also wish to investigate building into its various software, automatic expiration of passwords to ensure that they are changed periodically.
- 4) User administration (user addition, modification, removal) controls should be implemented to ensure that appropriate access is granted and terminated employees are removed in a timely manner. For terminated employees, among other processes, there should be a process for immediate deletion of passwords in the system and immediate change of all locks or passwords giving access to hardware or software. Inappropriate or excessive access may result in unauthorized data changes or transactions.

Information Technology Environment: General Controls

- 5) Without proper documentation, management is not assured that its policies and procedures are being carried out. Evidence over review processes should be documented and retained and the District should ensure a methodical identification and documentation of its significant operational and accounting processes, so that the necessary reviews and existing internal controls are not compromised.

Office of the Chief Technology Officer

During our procedures, we noted the following:

- 1) Default system accounts in the UNIX system are not disabled in PASS.
- 2) Based on the sample items selected for PeopleSoft terminated users test work, it was noted that:
 - a. 5 users were removed from the operating system; however, they remained active within PeopleSoft.
 - b. 1 user was still active in the SOAR mainframe.
 - c. 1 user was still active in the Faces.net domain.

Based on the sample items selected for CAPPs terminated users test work, it was noted that:

- d. 6 users were removed from the operating system; however, they remained active within PeopleSoft.
 - e. 2 users were removed from the operating system; however, they remained active within CAPPs.
 - f. 1 user was still active in the CAPPs mainframe.
 - g. 4 users were still active in the PASS mainframe.
 - h. 6 users were still active in the SOAR mainframe.
 - i. 1 user was still active in the ACEDS mainframe.
- 3) Minimum password complexity controls are either weak or not implemented for the following systems:
 - a. Estar Windows domain (password complexity is disabled and account lockout threshold is set at 0 for invalid log-in attempts).
 - b. OBP domain password(s) do not expire and the password history is not maintained.

Management's Response:

The following response was provided by Office of Financial Operations and Systems (OFOS) personnel:

- 1) As of the PASS Upgrade on 9/2/2008, the District has complied with this finding.
- 2) We concur with the findings and will conduct an investigation and correct all identified discrepancies. Procedures will be reviewed and improved to notify Financial Systems Security Administrators to immediately remove application access of terminated employees upon notification from the business unit or Human Resources.
- 3) Based on the finding, Estar domain password complexity has been enabled and the account lockout threshold has been set to three (3) attempts. OBP domain password complexity has been enabled and the account lockout threshold has been set to three (3) attempts.

Information Technology Environment: General Controls

The following response was provided by Department of Human Resources (DCHR) personnel:

DCHR concurs with this recommendation and has already taken steps to remedy this issue. Specifically, a comprehensive audit of PeopleSoft Access was conducted with the DCHR IT team and the Office of the Chief Technology Officer. Based on the findings in that audit, DCHR has reduced PeopleSoft access by nearly 50% in order to establish more stringent security controls. Additionally a protocol has been established that will allow DCHR to immediately deactivate accounts for all separated employees.

Office of Finance and Treasury

During our procedures, we noted the following:

- 1) The DBC and ARP applications do not have a formal methodology in place to support program changes.
- 2) We noted that programmers have access to the ARP datasets.
- 3) We noted that all users in SunGard Treasury Management system have been granted administrative functions, such as user setup restrictions.
- 4) The ARP application user IDs "KEY 1-3 ENTRY PERSON" are unknown.
- 5) Minimum password complexity controls are either weak or not implemented as follows:
 - a. The DBC application does not have any password requirements configured due to system limitations.
 - b. Again, due to system limitations, the only password parameter ARP requires is a minimum of 4 characters and this is not in accordance with industry "best practices."
 - c. For the SunGard application, the following password parameters exceptions have been noted:
 - i. Minimum password length is 4 characters; it should range between 6 - 8 characters.
 - ii. User accounts locking out after 100 invalid attempts appears excessive; it should range between 3-5 attempts.

Management's Response:

The Office of the Chief Information Officer (OCIO) recognizes the importance of implementing effective change management processes to ensure security and functionality of production systems. Although change management processes are currently in place in all OCIO departments, these processes differ from each other. The OCIO has developed an enterprise change management process that is currently being reviewed. Upon approval by the CIO, the process will be implemented to coordinate and communicate all changes related to production systems.

- 1) See response below:
 - a. In reference to DBC, DBC Debt Manager is a COTS product that is supplied by SS&C Technologies. As such, no development or configuration changes are performed for this product. Any changes are limited to version upgrades performed directly by the COTS vendor. All version changes or upgrades are performed through close coordination between the IT team and OFT business users.

Information Technology Environment: General Controls

- b. In reference to ARP, the documented ARP Software Program Change procedures are being followed. The procedures include controls of the software revisions, requestor, and implementation.
- 2) Access controls are being tightened so that programmers only have READ access to ARP datasets. OCIO has completed an analysis of the permissions and is in the process of updating them accordingly.
- 3) The OFT IT group commenced the process with the SunGard vendor to review user access and segregation of duties related to the User Table Restriction and will determine if the proposed restrictions will affect any other functionality/ability for OFT users to conduct their assigned duties. Additionally, at this point we are unsure if the access to User Table Restriction is the only access via "ResIQ Admin tool" which users have no access to or with privileges assigned. Additionally, OFT Business owners are consulted to set forth the granular requirements for User Table access and in accordance with vendor's best practices.
- 4) An analysis is underway of all ARP Application User IDs. Based upon the results, permissions will be updated and unneeded access will be removed.
- 5) See response below:
 - a. DBC application has a limitation and does not allow any configuration to set password complexity. We had contacted the vendor in the past to address this limitation and so far have not been provided with any solution.
 - b. For SunGard application, we configured the minimum password length to 6 characters and in accordance with the provided recommendations.
 - c. User accounts locking within SunGard RESIQ is now set to four (4) invalid attempts and is in accordance with the provided recommendations. In addition, the SunGard application is tied with OCFO Domain Authentication and is configured to lock out domain account after three (3) invalid attempts.

Medical Assistance Administration

During our procedures, we noted the following:

- 1) There appears to be an excessive number of users that have the ability to move packages into production; we noted that only 5 users have been listed as approvers while 40 have been listed as users that can move changes into production following approval.
- 2) Based on 9 out of the 67 program change sample items selected for test work, we noted the following exceptions:
 - a. 1 program change request was not signed.
 - b. 6 test results and/or sign offs were not provided/performed.
 - c. 5 endeavor checklists were not provided and there were no completion letter(s).
- 3) During our process, we noted that one user's access was not setup based on the MMIS Access Request Form. Subsequent to year-end, on December 12, 2008, the District provided a screen print of the updated user access and we noted that the user's access had been corrected.

Information Technology Environment: General Controls

- 4) During our process, we noted no evidence of a terminated employee's account deactivation. We were informed that subsequent to year-end, on November 26, 2008, this user was deactivated and reactivated for another user.

Management's Response:

- 1) The Department of Health Care Finance (DHCF), formerly the Medical Assistance Administration, does not concur with this finding. Packages can only move into production with the review/approval of the selected approvers (5). DHCF does not concur with the observation that this is excessive. The 40 users are developers (programmers) that have access to modify MMIS programs. They do not have final approval authority to move changes into the production system. That is the responsibility of the 5 "approvers".
- 2) Proper controls are currently documented and in place. The Fiscal Agent will review these procedures with staff.
- 3) Once the oversight was pointed out to us, the user's access was corrected.
- 4) DHCF does not concur with the finding. The noted employee's access was terminated on 11/3/08. However, the user ID was reissued to a new employee on 11/26/08 with a new password.

DHCF does not concur with the recommendation. The Fiscal Agent maintains and documents current Security Procedures for User Administration controls to add, change, and delete terminated employees. The Fiscal Agent's procedures utilize the proper documentation and they instituted regular reviews of the forms/results.

Department of Employment Services

During our procedures, we noted the following pertaining to program change management:

- 1) The DOCS, DUTAS, WEBS, and BARTS applications do not have a formal change management methodology in place to support program changes.
- 2) For the DOCS, WEBS, and BARTS applications, the District was unable to provide evidence that all program changes were authorized, developed, tested, and approved prior to being migrated into the production environment.
- 3) The vendor, On Point, does not utilize any form or tool to control copies of the source code. As such, data and program code integrity may be compromised during the migration process.

During our procedures, we noted the following pertaining to logical security:

- 4) User administration (user addition, modification, removal) is performed informally for WEBS and BARTS.
- 5) There is no formal procedure to remove terminated users from the DOCS and DUTAS applications.
- 6) We observed that there are an excessive amount of users that have access to the BARTS SQL database. Thus, it is possible for unauthorized employees to gain access.

Information Technology Environment: General Controls

Management's Response:

- 1) DOES has a change management methodology to support program changes for each of the systems identified.

The methodology is followed by DOES staff and contractors. For DOCS, DUTAS, and WEBS, email is used for change requests as well as approvals to implement the changes. The agency doesn't utilize forms to record those activities; instead these requests are tracked through emails and discussions.

DUTAS also includes a separate and more formal process when changes/modifications are significant:

- Decision/Information Request (DIR) is prepared by an IT analyst. The DIR describes the change requested, the reason for the change, and how the new process will work.
- The Tax Chief may accept the DIR orally or by e-mail.
- The software is modified.
- When the modifications are significant, they are described in a specification document.
- All changes are marked within the software itself, in the remarks section of the COBOL program, and with comments in the code when needed.

BARTS change control process is a formal process that includes email as well:

- All BARTS technical issues and enhancement requests are communicated from DOES via email.
- Reported issues are documented and tracked on the contractor's corporate issues portal.
- Periodically, DOES and the contractor review issues and determine priorities for development.
- Issues are wrapped into service packs and/or hot fixes and given a specific build number.
- Once the build is complete, the contractor deploys the build to the DOES QA environment.
- DOES reviews and tests the build and approves the migration to production. These approvals are documented through email.
- DOES IT uses the installation script and instructions to complete the production installation.

While these procedures were not accepted as formal, they have worked well for the Department. DOES is committed to improving processes and will create an electronic Change Request form to be emailed to the vendor directing action.

- 2) All program changes were authorized, developed, tested, and approved before being migrated into production. The testing for DOCS and WEBS is conducted by the contractor. As set forth above, DOES staff is involved in the testing of changes in BARTS. For DUTAS, the IT staff tests the new software, then turns it over to tax staff for testing. Tax staff has access to a copy of the tax system in a test environment. This environment can be used to test new processes. Confirmation that the new process works correctly is conveyed orally or through e-mail. The processes used have worked well for the Department. DOES is committed to improving processes and will create a formal change management methodology and ensure that documented procedures are followed. DOES will:

Information Technology Environment: General Controls

- Create an electronic Change Request form to be emailed to the contractor directing action.
 - Require submission of an electronic test plan from the contractor for changes exceeding 24 hours.
 - Require submission of an electronic migration plan from the contractor for all changes.
 - Create an electronic approval form to be emailed to the contractor granting approval to implement the change.
- 3) DOES does not concur with this finding in its entirety. The contractor utilizes a product provided by the OCTO data center Panvalet to manage Mainframe (DOCS) copies of the source code. The contractor utilizes Visual Source Safe to manage web copies of the source code. Both these products are industry standard products. As to BARTS, the contractor utilizes CVS and industry standard branching and tagging methods to control copies of the source code. There are no recommendations with respect to security of the source code and DOES does not plan any changes.
 - 4) DOES does not concur with this finding. Additions, modifications, and deletions are audited within the Security Portal making it easy to track/review all changes. Changes in WEBS and BARTS are effected immediately upon entry by authorized staff.
 - 5) DOES does not concur with this finding. The agency's Office of Compliance and Independent Monitoring tracks the separation of DOES employees and terminates their access. DOES has included a section in interagency agreements wherein a point person is identified so that employees who separate from service are removed from system access.
 - 6) DOES does not concur with this finding. User administration is limited to the BARTS administrator (one employee who is the user able to add users to the BARTS system and remove their access). Per the recommendation, DOES will formalize the electronic administration of user accounts by expanding the existing Security Portal.

Child and Family Services Agency

During our procedures, we noted the following:

- 1) 2 programmers had inappropriate access to the FACES production environment.
- 2) Minimum password complexity controls are weak as there is no lockout policy in place for failed log-in attempts for the FACES system.

Management's Response:

- 1) Production access to the programmers listed above was revoked in September 2008.
- 2) The FACES.NET password controls are the same as OCTO's password policy for Outlook (in fact for the District Government, FACES.NET users the passwords are synchronized). Passwords must meet the following minimum requirements:
 - Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
 - Be at least six characters in length.

Information Technology Environment: General Controls

- Contain characters from three of the following four categories:
 - i. English uppercase characters (A through Z)
 - ii. English lowercase characters (a through z)
 - iii. Base 10 digits (0 through 9)
 - iv. Non-alphabetic characters (for example, !, \$, #, %)

There are two main reasons for maintaining a "non-lockout" policy. First, the complexity of the password controls makes it difficult to guess a user's password even with multiple tries. Second, access to FACES.NET is required 24/7 for CFSA to continue business critical operations. However, CFSA does not maintain a 24/7 Help Desk which would be necessary in order to assist workers who were locked out of the application. Given these facts, CFSA does not concur with the finding.

Department of Mental Health

During our procedures, we noted the following:

- 1) The eCura application does not have a formal methodology in place to support program changes.
- 2) Minimum password complexity requirements, lockouts, and expiration controls are not in place for the eCura application due to certain inherent limitations.

Management's Response:

Issue #1: We continue to work to formalize the change process. All requests are recorded on our change request form and are sent through the necessary signature process. Once the change is authorized, IT reviews requirements and determines feasibility; prepares a project plan and completes the SDLC procedures; then conducts the requirements analysis, design, development, testing, and implementation. Following internal testing applications, the director signs off on the changes. Following user acceptance testing, users sign that the change meets the requirements. Once testing is completed, a written request is made to database administrative to load changes into Production. All changes implemented into Production are recorded in a SharePoint database. While the above steps are taken, we are working to more consistently follow these steps and implement the required use of formal documentation so that signatures are attached to the appropriate documents, i.e. requirements, design, development, testing documentation, migration, and deployment. We foresee this level of consistency and documentation being in place by 09/2010.

Issue #2: The eCura password requirements have been met to the extent possible in eCura. As mentioned previously, we employ password changes on a standard and routine basis on our network. We have placed written requirements for our users to change their passwords on a regular schedule on the splash screens of the WEB based portion of eCura and will do so within the eCura database as well. Internal users are able to change their passwords at will but presently cannot be automatically forced to change the password by the system. While eCura does exit a user from the system on the third unsuccessful attempt to access the system, it does not suspend the account. The vendor has no plans to provide this capability.

Department of Health

During our procedures, we noted the following:

- 1) The ACEDS application does not have a formal methodology in place to support program changes.

Information Technology Environment: General Controls

- 2) Programmers have the ability to promote ACEDS codes to production as well as having direct access to the database. We also noted that an ACEDS programmer has inappropriate administrative access to the application.

Management's Response:

- 1) Finding #1: Effective October 1, 2008, IMA implemented a Change Control procedure that requires identification of the desired change, a preliminary assessment of the impact of the change, a final evaluation of the impact of the change, migration dates, and sign-offs. These procedures vary depending on whether the change request is a screen, batch, or other type of change. The Office of Information Systems (OIS) has also recently implemented an automated change control system.

OIS uses a tool called PANAPT to check out Natural or COBOL programs, JCI, PROC'S or CTICARDS, to the DEVELOPEMENT region from the PRODUCTION region.

OIS recently installed a Change Control Application for controlling change request processing. It is used by staff from both IMA and OIS.

- A Change Request is initiated by IMA.
 - A change request is written up, in our new change request tracking system.
 - Sent to the supervisor of Applications Support Division II.
 - The Supervisor will assign the Change Request to the appropriate Application Programmer.
 - The programmer will check out the program from Production to Development region using PANAPT.
 - The programmer will write or modify the program in the Development region.
 - IMA will sign off on the request, to be moved to the TEST region.
 - The Supervisor will approve the move request, to be moved to the TEST region using PANAPT.
 - IMA will do further testing in the test region.
 - The Application Programmer will make further modifications if necessary.
 - After the final testing in the TEST region, IMA will sign off on the request, to be moved to Production.
 - The PANAPT move request is approved by the Supervisor or his backup and moved to Production.
- 2) Finding #2: OIS Application Programmers have 'read only' access to the ACEDS database and do not have update capabilities. Therefore, this finding and recommendation are not applicable.

Office of Tax and Revenue

During our procedures, we noted the following:

- 1) User administration (user addition, modification, removal) is performed informally for the Estar application.
- 2) The Estar application password encryption has not been enabled to 17 out of the 18 Estar users.

Information Technology Environment: General Controls

Management's Response:

- 1) User administration (user addition, modification, removal) for ESTAR application is performed by the IT TechSupport group in a formal and controlled process. We have formal addition/termination user access request forms. We receive a formal email request along with a form from ROD, which is used to create internal Help Desk tickets and all user access provisioning requests are tracked using email, the access form, and Helpdesk SDK tickets.
- 2) All accounts within Windows 2000 server are hashed using Kerberos protocol and the user ID/Passwords are transmitted in encrypted form. OCFO has discussed this matter with the Estar vendor to request whether all account passwords can be encrypted. Based on the response from the Estar vendor, OCFO will implement encryption of all accounts if the system allows for it.

Metropolitan Police Department

During our procedures, we noted the following:

- 1) The TACIS application does not have a formal methodology in place to support program changes.
- 2) 2 HP/UX accounts associated with terminated users remained active.

Management's Response:

- 1) The MPD IT Division will implement a Change Board to govern any add, modification, and deactivations to the Agency's Information structure and critical applications to include the TACIS system. The Board will govern any security modifications and any future security audits. The anticipated implementation is May 29, 2009.
- 2) The implementation of the Change Board will ensure that all terminated employees/users are removed in a timely manner. It should be noted that the terminated employees included in this review did not have access to the live production region.

Office of Financial Operations and Systems

During our procedures, we noted the following:

- 1) The "Everyone" group has access to the MS Access and Excel OBP files.
- 2) User administration (user addition, modification, removal) is performed informally for the OBP application.

Management's Response:

- 1) Management does not concur with the finding. The "Everyone" group is not included in the access controls granting access to the network directory where the Reprogramming related access and Excel files reside; and user rights are limited by named user.
- 2) The OCIO follows a structured methodology for user administration. The process for new/terminated domain users are as follows:

Information Technology Environment: General Controls

OBP administration/HR personnel communicate via email to OCIO that an employee needs to be added/changed or removed from the BUDGET domain. OCIO retains all such emails for audit support. All reprogramming related applications (Excel, Access) are only accessible via OBP domain credentials. Upon termination, OBP and HR notify OCIO via email. OCIO immediately disables the associated account on the budget domain, restricting access to all applications.

Office of the Chief Financial Officer

During our procedures, we noted that SOAR developers have update access to the production environment and databases and conduct system administrator responsibilities.

Management's Response:

OCIO maintains that segregation of duties is in place. All SOAR development is performed by contractors (currently one contractor is retained for all software changes/development). Once the contractor has completed unit testing of the code in the development region, a request is made to the SOAR PMO staff to migrate the code to a User Acceptance Testing environment.

Once the Office of Financial Operations and Systems (OFOS), the business user, tests and formally approves the software change, a request is made to the SOAR PMO to promote the software to production. SOAR PMO staff does not perform any development work and is primarily responsible for test facilitation and production migration.

The contractor developer is restricted to "read only" access rights to production libraries. The developer has authority to browse production libraries but does not have the authority to change production libraries or the data.

RACF is used to secure the SOAR application programs and data. Any unauthorized access attempt is reported to the SOAR PMO and appropriate measures are taken.

In order to ensure continuity of service, a process is in place for a SOAR PMO staff member to edit or develop the software code. Such instances require management approval. Documented procedures require a different SOAR PMO member to migrate the code to production than the one who made the code changes, ensuring separation of duties in this instance.

District of Columbia Public Schools

During our procedures, we noted that CAPPs developers have update access to the production environment and databases and conduct system administrator responsibilities.

Management's Response:

The internal control of segregation of duties is in place. Contractors within the Payroll PMO fulfill the different roles of CAPPs Developers, CAPPs Production Control, CAPPs Production Support, and CAPPs DBA.

Information Technology Environment: General Controls

The CAPPs Developers do not have update access to the production software or data, but are restricted to "READ ONLY" access where needed. Attempts to violate security are detected by RACF and reported to the Payroll PMO Security Administrator and the Payroll PMO Director for appropriate action.

* * * *

Information Technology Environment: Treasury Functions

User Access and Segregation of Duties

During our review of the SunGard Treasury Management system user access and segregation of duties, we noted the following:

- 1) Business users have access to administrative functions such as User Table Restriction Setup.
- 2) User access rights within the District's banking systems (SunGard, Bank of America Direct, and Wachovia Connections) are not reviewed on a periodic basis.

We recommend that management remove such access and limit the administrative functions to only appropriate individuals. In addition, we recommend that management review user access rights and authorizations and ensure access has been granted to only those functions required for an individual's job responsibilities. Access rights should be reviewed at least annually to ensure that they remain appropriate as this could result in unauthorized entries or adjustments being made.

Management's Response:

The Office of the Chief Financial Officer /Treasury IT group has commenced the process with the SunGard vendor to review user access and segregation of duties related to the User Table Restriction Setup to determine if the recommended restrictions will affect the functionality/ability of Office of Finance and Treasury (OFT) users to conduct their assigned duties.

It should be noted that OFT management is consulted in the process of establishing the granular requirements for User Table access and in accordance with vendor's best practices.

In regards to the Bank of America and Wachovia online systems, the system administrator does review the User List on a periodic basis (more than annually).

Opening of Bank Accounts

In order to open an account, a written request is forwarded to the Banking Services Officer or Associate Treasurer for Banking and Operations from either the CFO or Controller of the requesting agency for approval. During our procedures we noted the following:

- 1) For 3 Bank IDs which had been selected for test work, we observed that the request to create the Bank ID came significantly after the actual open date of the respective bank account.
- 2) For another 4 Bank IDs in the same testing population, we observed that no notification was received from the respective agency to create the Bank ID within SOAR, the District's accounting system of record. These accounts were discovered through a joint review performed by the Office of Finance and Treasury (OFT) and the Office of Financial Operations and Systems (OFOS).

We recommend that management ensure adherence to written policies and procedures which in turn, will ensure good internal controls and efficient administration of its bank accounts. We identified these items from a sample of transactions selected for testing. Management should recognize that the potential exists for additional violations of set policy.

Information Technology Environment: Treasury Functions

Management's Response:

Management has communicated the proper procedures to agencies, but agencies have not always complied with the proper protocol regarding the establishment of a Bank ID. Management has diligently sought to ensure that all Bank IDs were in compliance with established procedures, and will continue to be proactive in this regard to seek to ensure full compliance.

Closing of Bank Accounts

To close an existing bank account, a written request is forwarded to the Banking Services Officer or Associate Treasurer for Banking and Operations from either the CFO or Controller of the requesting agency. The Banking Services Officer will contact the Office of Financial Operations and Systems (OFOS) to determine if the account has been reconciled prior to closing the account.

- 1) For 1 Bank ID which had been selected for test work, we observed that no notification was received from the agency to disable the Bank ID within SOAR, the District's accounting system of record. The account was discovered through a joint review performed by the Office of Finance and Treasury (OFT) and OFOS.
- 2) For another Bank ID which had been selected for test work, we could not confirm the request to close the bank account was approved by the agency's CFO and the Banking Services Officer/Associate Treasurer for Banking and Operations.

We recommend that management ensure adherence to written policies and procedures which in turn, will ensure good internal controls and efficient administration of its bank accounts. We also recommend that documentation to support activity be retained and stored in a central location that is accessible. We identified these items from a sample of transactions selected for testing. Management should recognize that the potential exists for additional violations of set policy.

Management's Response:

- 1) Management discovered and rectified the one instance cited in the finding and no funds were at risk. Management adheres to the written policies and procedures associated with this finding. Management will continue to be proactive to seek to ensure that all agencies comply such that there are no recurrences of the one instance indicated in the finding.
- 2) The closing of an account does not place any funds at risk. Given that the account was closed, it had to have been approved by officials with authority to close it. We will continue to be proactive to seek to ensure that all agencies comply with the appropriate procedures for account closing and to ensure that the appropriate documentation of all such account closings is maintained. The Banking Relations Unit has established a central location for the retention of bank account related documents.

Bank Polling and Parsing

On a nightly basis, the SunGard Treasury Management system and other utilities will poll the District's various bank systems and pull down the respective banking information. Once the banking information has been polled, it is parsed into the appropriate format for posting and recording into SunGard.

Information Technology Environment: Treasury Functions

To ensure the bank polling and parsing processes have executed successfully, a member of the EBT Electronic Banking unit will review the polling and parsing status of the various bank accounts set up within SunGard. The SunGard system generates audit reports for each account, describing the success/failure of the posting process. Currently, this review is done on an informal basis by physically "eye-balling" the communication screens within SunGard. There is no documented evidence of this review.

Without proper documentation, management is not assured that its policies and procedures are being carried out. Evidence over the review of the SunGard polling and parsing process should be documented and retained.

Management's Response:

The Office of Finance and Treasury (OFT) believes there is documented evidence of the review as follows:

- Review of bank communication screens for any errors.
- If the results show an error, manually poll the bank file.
- There is a screen that allows OFT to select and review a bank file after being polled.
- There is a screen that is used to verify that a bank file has successfully posted with no errors.

Journal Entries

There is a nightly batch job process which posts cash management transactions from the SunGard Treasury Management system into SOAR, the District's accounting system of record. To ensure that all transactions have been properly posted into SOAR, a member of the EBT Electronic Banking unit will review the SOAR 530 screen and any necessary corrections are performed manually within SOAR.

There is no documented evidence of the review over these journal entries posted into SOAR via SunGard. Without proper documentation, management is not assured that its policies and procedures are being carried out. Evidence over the review of the journal entries posted into SOAR via SunGard should be documented and retained.

Management's Response:

The Office of Finance and Treasury believes there is documented evidence of the review as follows:

- E-banking Unit runs an EIS Report the next day showing all transactions posted into SOAR.
- If there is a missing transaction, the EIS Report can assist in determining the other side that needs to be put into SOAR.
- If this is the case, the next step is to go to SOAR to enter the missing transaction into SOAR.

Expedited Payments

R*Stars allows vouchers to be paid within a minimum of 5 days. On some occasions, agencies may have the need to pay a vendor in less than 5 days. If this is the case, agencies complete an Expedited Payment Request form to request voucher(s) to be paid in less than the designated R*Stars timeframe. The Expedited Payment Request form is then sent to the Vendor Center at the Office of Finance and Treasury (OFT).

Information Technology Environment: Treasury Functions

After various steps have taken place, the expedited payment(s) are posted into R*Stars through a nightly batch process. The Vendor Center reviews the R*Stars payment error comparison processing report (DAFR 3521) to ensure payments have successfully posted into SOAR, the District's accounting system of record, and a payment number has been assigned. Currently, there is no documented evidence of this review by the Vendor Center.

Without proper documentation, management is not assured that its policies and procedures are being carried out. Evidence over the review of the R*Stars payment error comparison processing by the Vendor Center should be documented and retained.

Management's Response:

Policies and procedures will be amended to add the procedure of documenting evidence of this review by the Vendor Center, consistent with the recommendation.

Investment and Interest Income

A SOAR Revenue Receipt (SRR) is prepared by the Financial Manager to record investment transactions. The SRR, investment memos, Cash Note, and Investment Calendar/Report are reviewed by the Cash and Investment Manager.

- 1) For 1 transaction that had been selected for test work, we could not re-perform the controls to confirm the SRR was appropriately prepared. The supporting documents, including the Investment Memo and the Trade Confirmation and Investment Calendar/Report could not be provided by the District.
- 2) During our procedures over daily investment activities, we noted that for 3 transactions which had been selected for test work, the transactions had been applied against the incorrect transaction code.
- 3) For 4 interest income transactions which had been selected for test work, we could not verify the SRR was appropriately prepared and approved because no documentation was provided.
- 4) For another 4 interest income transactions in the same testing population, we could not re-perform the control over the approval of the SRR because only partial documentation was provided.

We recommend that documentation to support activity be retained and stored in a central location that is accessible. Management should ensure proper control over all supporting documentation and invoices. Further, all transactions should be reviewed carefully by the SRR approver to ensure transactions are being applied to the correct transaction codes. We identified these items from a sample of transactions selected for test work. Management should recognize that the potential exists for additional violations of set policy.

Management's Response:

The Cash Management Unit maintains daily files with appropriate documentation and recording of investment transactions. During a period of time in the first half of FY 2008, employee turnover and the corresponding temporary vacancies in the three positions in the chain of command responsible for this activity caused a temporary disruption in the standard documentation process.

Information Technology Environment: Treasury Functions

Management was very focused on ensuring that transactions were properly executed by personnel temporarily assigned to this activity while building a new team to manage and execute these functions. All transactions were properly executed.

Under its new management, the Cash Management Unit has implemented a process in which transactions entered into SOAR, the District's accounting system of record, are reviewed by another individual to ensure accuracy of data entry and then the transactions are not released until reviewed by a Certifying Officer. Once the transactions are released, the SOAR document with supporting documentation that includes the SRR, investment memos, Cash Note and Investment Calendar/Report are placed in a daily folder and then filed in a centralized location maintained only by the Cash Management Unit.

Moreover, as documented by the Office of Integrity and Oversight in its review of findings from last year's audit, by the end of FY 2008, the Office of Finance and Treasury had sufficiently addressed the issues that produced findings in this area.

Wire Transfers – Approval Limits

The District's banking systems require separate individuals to input and release/approve wire transfers. Subsequently, the wire transfer request and transaction report are provided to the Cash and Investment Manager for review and release/approval.

However, we noted that monetary transaction restrictions or authorization limits do not exist for approving wire transfers with the District's banking systems. To minimize the risk of unauthorized transactions, we recommend management consider establishing limits requiring additional approvals of wire transfers over certain pre-established dollar amounts. This would allow additional oversight over significant transactions.

Management's Response:

Wire transfer requests originate at the agency level and require approvals and sign-offs at the agency level and in SOAR, the District's accounting system of record before coming to the Office of Finance and Treasury (OFT). Associate Chief Financial Officers and Agency Fiscal Officers (who are also under the Chief Financial Officer) establish procedures and controls at the agency level to ensure that wire requests have appropriate restrictions. At OFT, before being transmitted, there is verification that the wire request has been entered into SOAR—which means appropriate budget authority exists and that the vendor has been established in SOAR—and that it is authorized and signed by an agency Certifying Officer who has been verified by the Office of Financial Operations and Systems (OFOS) as a Certifying Officer. There is oversight at OFT in that more than one approved OFT official must execute/release each wire.

The recommendation would provide an additional level of oversight, and will be considered by management, although management believes that the current level of oversight and approvals are sound.

Wire Transfers – File Format

The Bank of America online banking system was moved from a DOS based reporting system to a Web based system. As a result of this conversion, the Bank of America system cannot read the file format imported from SunGard with respect to wire transfers. The Bank of America system should be incorporated into the SunGard Treasury Management system. Management has represented that the Electronic Banking Manager is currently working with SunGard and Bank of America to remedy this problem.

Information Technology Environment: Treasury Functions

Management's Response:

The Office of Finance and Treasury (OFT), in cooperation with the Office of the Chief Financial Officer IT group, is in the process of integrating and updating the interfaces to our banking partners. When this is completed, the SunGard Treasury Workstation will have a fully integrated platform that will transfer, accept, and read the current file formats that our various banking partners utilize.

However, with respect to Bank of America wires, they are currently processed directly with Bank of America's "Direct" Cash Management website. As such, the wires are processed in a secure manner which is consistent with our policies and procedures.

* * * *

Information Technology Environment: Revenue Generation and Collection

User Access and Segregation of Duties

During our review of the Integrated Tax System (ITS) and the Computer-Assisted Mass Appraisal System (CAMA), we noted the following:

- 1) 5 terminated users still had access to the ITS application.
- 2) 4 users (2 student trainees, 1 administrative assistant, and 1 clerical assistant) did not have the appropriate access to the ITS application.
- 3) 1 user (administrative assistant) was inappropriately given access rights to the CAMA application.

Under these conditions, it is possible that unauthorized changes can be made. Thus, the existing procedures may not reasonably limit the District's exposure. To prevent unauthorized entries or adjustments, we recommend that management consider a formal process with adequate audit trails be implemented to ensure that all ITS and CAMA users are authorized, that all access rights are modified accordingly, and that users are removed from the system on a timely basis upon termination.

Management's Response:

Security access to ITS was removed for the set of five terminated employees referenced above between September 3, 2008 and September 9, 2008. Access to the network has also been disabled for the five employees. Security access to ITS was removed for three of the set of four employees referenced above between August 16, 2008 and September 4, 2008. The remaining employee has the appropriate ITS access per the RPTA Director.

In December 2008, the Office of Tax and Revenue (OTR) in conjunction with the Office of the Chief Information Officer (OCIO) Information Systems Administration (ISA) completed an analysis and revision of all user access to ITS. In February 2009, the OTR and the ISA will implement modifications to ITS to enhance administration of ITS access. These modifications will separate security administration duties, enabling the business units to administer their employees' access to ITS while preventing the technical staff from modifying this access. A formal process has been put in place to ensure all ITS users are authorized, all access rights are modified accordingly, and that users are removed from the system on a timely basis upon termination.

Management does not concur with the audit finding regarding the administrative assistant who was given access to CAMA. It is not an unusual practice to grant access to administrative assistants so that they can perform limited tasks assigned by management such as adding taxpayer comments, scheduling appeal appointments, etc. The administrative assistant in question does not make any valuation changes or any changes to critical information in the system. The only administrative assistant that has access is currently in the process of having her title changed to instrument examiner.

eTaxpayer Services Center

Taxpayers have the ability to pay their taxes through an online system known as the eTaxpayer Service Center (ETSC). As such, on a daily basis, the Systems Accountant will log onto the ETSC to retrieve the deposit and distribution reports in order to observe the amounts received by the Office of Tax and Revenue (OTR). The activity is recorded in SOAR, the District's accounting system of record, through a SOAR Journal Voucher.

Information Technology Environment: Revenue Generation and Collection

During our procedures, it was noted that the employee who prepares the SOAR Journal Voucher document is the same as the employee who approves the entry within SOAR after it has been entered and released.

One of the basic elements of internal control is separation of duties so that no one person controls all phases of an operation. Separating certain duties improves internal controls and reduces the possibility of errors and irregularities. We recommend that management review the current assignment of functions and where possible, duties should be segregated to reduce the risk of errors or fraud.

Management's Response:

The process is as follows:

- 1) The Senior Accountant prints ETSC activity on a daily basis.
- 2) The Senior Accountant pulls the daily report.
- 3) The Senior Accountant journalizes daily activity.
- 4) The Accounting Supervisor reviews/approves the journal entry.
- 5) The approved journal entry is given to the Accounting Technician for entry into SOAR.
- 6) The Senior Accountant reviews the journal entry (in the system) for accuracy. The system assigns an "A" for journal entry approval.
- 7) The Senior Accountant carries the journal entry and supporting documentation to the Office of Financial Operations and Systems (OFOS) for review. OFOS reviews/approves the journal entry. The journal entry is assigned a "P" for posted.

The control issue occurred when the Senior Accountant approved the journal voucher (step 6). The steps outlined above represent our normal process of creating, reviewing, approving, and posting journal entries but we will review the process to ensure that the risk of error and fraud are reduced or eliminated.

Lack of Review and Approval

The Revenue Accounting Administration (RAA) is responsible for ensuring that all revenue and deposit transactions for the Office of Tax and Revenue (OTR) are reconciled. For certain reconciliations of information between the Integrated Tax System (ITS) and SOAR, the District's accounting system of record, the Staff Accountant will reconcile the deposit amounts to verify that they agree. Upon completion of the reconciliation(s), they are sent to the Supervisory Accountant for review and approval.

During our procedures, we noted that there is no documented evidence of this supervisory review. Without proper documentation, management is not assured that its policies and procedures are being carried out. Evidence over the review of ITS to SOAR reconciliations should be documented and retained.

Management's Response:

We will introduce new procedures to ensure that supervisory personnel reviews and approvals are consistently performed on all reconciliations.

* * * *

Status of Prior Year Observations

Process, Entity, or Fund	Nature of Prior Year Comment	Current Year Status
General District Administration	Policies and Procedures Manual	Control Deficiency
General District Administration	Adequacy of Insurance Coverage	Not Repeated
Cash and Investments	Bank Reconciliation Process (BID 121)	Material Weakness
Cash and Investments	Cash Disbursements (BID 121)	Material Weakness
Cash and Investments	Bank Reconciliation Process (BID 200)	Material Weakness
Cash and Investments	Bank Reconciliation Process (Sampling of BIDs)	Material Weakness
Cash and Investments	Elimination of Unnecessary Accounts	Material Weakness
Cash and Investments	Advisory Neighborhood Commission Bank Accounts	Not Repeated
Cash and Investments	Compliance with Investment Policy and its Parameters	Control Deficiency
Cash and Investments	Non-Compliance with Financial Institutions Deposit and Investment Amendment Act	Control Deficiency
Cash and Investments	Inclusion of Accounts in Financial Reports	Not Repeated
Management of Grants	Administration of Refundable Deposits	Not Repeated
Management of Grants	Lack of Supporting Documentation – Income Maintenance Administration	Control Deficiency
Management of Grants	Lack of Supporting Documentation – Office of City Administrator	Not Repeated
Management of Grants	Approval of Timesheets	Not Repeated
Health Care Safety Net	Participant Eligibility	Control Deficiency
Management of the Postretirement Health & Life Insurance Trust	Participant Data and Retiree Folders	Significant Deficiency
Management of the Postretirement Health & Life Insurance Trust	Plan Governance	Significant Deficiency
Management of the Postretirement Health & Life Insurance Trust	Plan Investments	Significant Deficiency

Process, Entity, or Fund	Nature of Prior Year Comment	Current Year Status
Management of the Disability Compensation Program	Third Party Administrator (TPA) Database	Not Repeated
Management of the Disability Compensation Program	Indemnity Payments	Not Repeated
Revenue Generation and Collection	Lack of Supporting Documentation	Significant Deficiency
Revenue Generation and Collection	Exemption from Real Property Tax	Control Deficiency
Revenue Generation and Collection	Approval of Homestead Applications	Significant Deficiency
Revenue Generation and Collection	Redeemed Properties – Tax Sale Process	Control Deficiency
Revenue Generation and Collection	Reconciliation of the Tax Sale Ledger	Significant Deficiency
Revenue Generation and Collection	Policy and Procedures	Control Deficiency
Revenue Generation and Collection	Revenue Processes at the Department of Insurance, Securities, and Banking Regulations	Not Repeated
Revenue Generation and Collection	Licensing Revenue at Department of Insurance, Securities, and Banking Regulations	Not Repeated
Revenue Generation and Collection	Revenue Process at the Department of Consumer & Regulatory Affairs	Not Repeated
Revenue Generation and Collection	Transaction Testing at the Department of Consumer & Regulatory Affairs	Control Deficiency
Fixed Assets	Inventory of Fixed Assets	Control Deficiency
Fixed Assets	Personal Property	Control Deficiency
Fixed Assets	Process over Capital Expenditures	Not Repeated
Fixed Assets	Classification of Capital Expenditures	Control Deficiency
Fixed Assets	Disbursement Approval Process	Not Repeated
Budget and Planning	Reprogrammings	Not Repeated

Process, Entity, or Fund	Nature of Prior Year Comment	Current Year Status
Budget and Planning	Intradistrict Transactions	Not Repeated
Budget and Planning	Capital Budget Corrections	Control Deficiency
Budget and Planning	Lack of Written Policies and Procedures	Control Deficiency
Loan Programs	Reconciliation of the Loan Portfolio	Not Repeated
Loan Programs	Loan Collections	Not Repeated
Management of Debt Instruments	Recent Developments in the Credit Market	Not Repeated
Journal Entries	Review and Approval Process	Control Deficiency
Allocation of Indirect Costs	Cost Recovery	Not Repeated
Anacostia Waterfront Corporation	Payroll Records Lack of Supporting Documentation	AWC has been dissolved as of October 1, 2007. All activities have been transferred to the District.
National Capital Revitalization Corporation and Related Entities	Payroll Records Contracts Governance	NCRC and related entities have been dissolved as of October 1, 2007. All activities have been transferred to the District.
Information Technology Environment: General Controls	Child and Family Services Agency	Control Deficiency
Information Technology Environment: General Controls	Department of Health	Control Deficiency
Information Technology Environment: General Controls	Metropolitan Police Department	Control Deficiency
Information Technology Environment: General Controls	Office of Budget and Planning	Not Repeated
Information Technology Environment: General Controls	Office of the Chief Financial Officer	Control Deficiency
Information Technology Environment: General Controls	Office of the Chief Information Officer	Not Repeated

Process, Entity, or Fund	Nature of Prior Year Comment	Current Year Status
Information Technology Environment: General Controls	Office of the Chief Technology Officer	Control Deficiency
Information Technology Environment: General Controls	Office of Tax and Revenue	Control Deficiency
Information Technology Environment: Hire to Pay	Lack of Supporting Documents	Significant Deficiency
Information Technology Environment: Hire to Pay	Logical Access	Significant Deficiency
Information Technology Environment: Hire to Pay	Payrates	Not Repeated
Information Technology Environment: Hire to Pay	Supplemental Payments	Not Repeated
Information Technology Environment: Revenue Generation and Collection	User Access and Segregation of Duties	Control Deficiency
Information Technology Environment: Revenue Generation and Collection	Segregation of Duties – Collections Department	Not Repeated
Information Technology Environment: Revenue Generation and Collection	Segregation of Duties – Returns Processing Department	Not Repeated
Information Technology Environment: Revenue Generation and Collection	Processing of Individual Income Tax Returns	Significant Deficiency
Information Technology Environment: Revenue Generation and Collection	Processing of Void and Cancelled Checks	Significant Deficiency
Information Technology Environment: Treasury	Wire Transfers	Control Deficiency
Information Technology Environment: Treasury	Investment Transactions	Not Repeated
Information Technology Environment: Treasury	User Access and Segregation of Duties	Control Deficiency

Note: "Not Repeated" status does not necessarily equate to the issue being resolved; it was just not noted in the audit process this year.