GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL

DISTRICT OF COLUMBIA

MEMORANDUM OF RECOMMENDATIONS

For Fiscal Year
Ended September 30, 2010

CHARLES J. WILLOUGHBY
INSPECTOR GENERAL

OIG No. 11-1-19MA **May 26, 2011**

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General

May 26, 2011

The Honorable Vincent C. Gray
Mayor
District of Columbia
Mayor's Correspondence Unit, Suite 316
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

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

Natwar M. Gandhi, PhD.
Chief Financial Officer
Office of the Chief Financial Officer
1350 Pennsylvania Avenue, N.W., Room 203
Washington, D.C. 20004

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

In connection with the audit of the District of Columbia's general purpose financial statements for fiscal year (FY) 2010, KPMG, LLP (KPMG) submitted the enclosed final Memorandum of Recommendations, known in previous years as the Management Letter. This report sets forth KPMG's comments and recommendations to improve internal control and other operating efficiencies.

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 me or Ronald W. King, Assistant Inspector General for Audits at (202) 727-2540.

Sincerely,

Charles J. Willoughby
Inspector General

Enclosure

CJW/ws

cc: See Distribution List

DISTRIBUTION:

Mr. Allen Y. Lew, City Administrator, District of Columbia
Mr. Brian Kenner, Office of the Deputy Mayor for Planning and Economic Development, District of Columbia
The Honorable Mary M. Cheh, Chairperson, Committee on Government Operations and the Environment, Council of the District of Columbia
Mr. Brian Flowers, General Counsel to the Mayor
Mr. Paul Quander, Interim Chief of Staff, Office of the Mayor
Ms. Janene Jackson, Director, Office of Policy and Legislative Affairs
Dr. Linda Wharton Boyd, Director, Office of Communications
Mr. Eric Goulet, Director, Office of Budget and Finance, Office of the City Administrator
Ms. Nyasha Smith, Secretary to the Council (1 copy and via email)
Mr. Irvin B. Nathan, Attorney General for the District of Columbia
Mr. William DiVello, Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer
Ms. Deborah K. Nichols, D.C. Auditor
Mr. Phillip Lattimore, Director and Chief Risk Officer, Office of Risk Management
Ms. Jeanette M. Franzel, Managing Director, FMA, GAO, Attention: Norma J. Samuel (via email)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives, Attention: Bradley Truding (via email)
The Honorable Darrell Issa, Chairman, House Committee on Oversight and Government Reform, Attention: Howie Denis (via email)
The Honorable Elijah Cummings, Ranking Member, House Committee on Oversight and Government Reform, Attention: William Miles (via email)
The Honorable Trey Gowdy, Chairman, House Subcommittee on Health Care, the District of Columbia, the Census and the National Archives, Attention: Anna Ready (via email)
The Honorable Danny Davis, Ranking Member, House Subcommittee on Health Care, the District of Columbia, the Census, and the National Archives, Attention: Yul Edwards (via email)
The Honorable Joseph Lieberman, Chairman, Senate Committee on Homeland Security and Governmental Affairs, Attention: Holly Idelson (via email)
The Honorable Susan Collins, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs, Attention Amanda Wood (via email)
The Honorable Daniel K. Akaka, Chairman, Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Attention: Christine Khim (via email)
The Honorable Ron Johnson, Ranking Member, Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Attention: Alan Elias (via email)
The Honorable Harold Rogers, Chairman, House Committee on Appropriations, Attention: Julia Casey (via email)
The Honorable Norman D. Dicks, Ranking Member, House Committee on Appropriations, Attention: Laura Hogshead (via email)
The Honorable Jo Ann Emerson, Chairman, House Subcommittee on Financial Services and General Government, Attention: John Martens (via email)

The Honorable José E. Serrano, Ranking Member, House Subcommittee on Financial Services and General Government, Attention: Laura Hogshead (via email)
The Honorable Daniel K. Inouye, Chairman, Senate Committee on Appropriations, Attention: Charles Houy
The Honorable Thad Cochran, Ranking Member, Senate Committee on Appropriations
The Honorable Richard Durbin, Chairman, Senate Subcommittee on Financial Services and General Government, Attention: Marianne Upton (via email)
The Honorable Jerry Moran, Ranking Member, Senate Subcommittee on Financial Services and General Government, Attention: Dale Cabaniss (via email)

KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

March 31, 2011

The Mayor and the Council of the District of Columbia
Inspector General of the Government of the District of Columbia

We have audited the financial statements of the District of Columbia (the District), as of and for the year ended September 30, 2010, and have issued our report thereon dated January 27, 2011. In planning and performing our audit of the financial statements of the District, 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.

During our audit, we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in Appendix A.

The District's written response to our comments and recommendations has not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the District's organization gained during our work to make comments and suggestions that we hope will be useful to you. We would be pleased to discuss these comments and recommendations with you at any time.

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

Very truly yours,

KPMG LLP

KPMG LLP is a Delaware limited liability partnership, the U.S. member firm of KPMG International Cooperative ("KPMG International"), a Swiss entity.

Section I – EDP Comments

During our audit of the FY 2010 basic financial statements, we performed certain procedures over the general controls and the application controls of major information technology (IT) financial systems and applications of the District. Our test work included logical access, program changes, application development, and computer operations controls of the following major IT systems:

- Automated Client Eligibility Determination System (ACEDS)
- Department of Employment Services (DOES) Applications – BARTS, DOCS, and DUTAS
- iNovah
- Meditech
- The Procurement Automated Support System (PASS)
- PeopleSoft
- The System of Accounting and Reporting (SOAR)
- The Time Attendance and Court Information System (TACIS)
- The Tax Administration System (TAS)

Within our test work, we have noted deficiencies within the areas of logical access, program changes, application development, and computer operations. In the pages that follow, we have broken down these deficiencies by application below along with both KPMG's recommendation for remediating the deficiency noted as well management's response.

1. ACEDS

We identified the following deficiencies in the general IT controls environment supporting the ACEDS application:

a. During discussions with management, we were informed that two infrastructure changes were implemented into production without prior approval from the Office of the Chief Technology Officer (OCTO) Change Advisory Board (CAB). These changes resulted in temporary service outages to District of Columbia (DC) Government IT networks and systems.

   Management has indicated that these changes were not malicious in nature and that the individuals who implemented the changes were unaware of the impact of implementing the changes directly into the production IT environment. Management also noted that the changes had no impact on the integrity of processing or data of the in-scope applications.

   Management informed us that they plan to implement an automated change monitoring system that will be installed on production infrastructure environments for purposes of automatically capturing and reporting changes to further strengthen the infrastructure change management process.

b. Management has not updated its policy that defines the minimum password configuration requirements for DCIT systems in over six years. Further, inquiry and inspection procedures performed by the audit team indicate that the policy was not effectively communicated to responsible personnel. Specifically, we noted the following:

   1) The OCTO Password Management Policy, dated September 2004, does not require that systems be configured to automatically lock out user accounts after a predefined number of invalid log-on attempts.
   2) Inquiry of four individuals at the management level who have responsibility for implementing password security parameters for in-scope applications informed us that they were neither aware of nor able to locate the OCTO Password Management Policy document.
   3) We noted various inconsistencies between the requirements outlined in the OCTO Password Management Policy and configurations set within the in-scope applications and their supporting databases and operating systems.

c. During our test work over the application program changes for ACEDS, we noted the following:

   1) For 8 of 14 changes sampled in which a change request number has not been noted within the description of the change, documentation of authorization prior to migration to production could not be provided by management.

   2) For 6 of 14 changes sampled in which a change request number has been noted within the description of the change, the documentation provided did not correspond to the specific production programs selected for testing. As a result, we were unable to map the modified programs to the specific Change Control Forms evidencing approval for those changes.

   3) For all 14 changes sampled, documentation supporting the testing procedures performed (e.g., test scripts, test plans, and test results) were not maintained.

d. Management does not periodically review physical access to the OCTO Data Center 1 (ODC1) and Data Center 2 (ODC2) facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications.

e. Developers were granted inappropriate levels of access to migrate changed ACEDS program code into production without any preventative impedance provided by other change-mitigating controls placed into operation by management.
   Specifically, three of the four developers had access to make changes to application code as well as to migrate changed application code between the ACEDS development, test, and production environments using the Computer Associates PanAPT change management tool.

f. Management does not have a formalized process in place for monitoring the generic mainframe account PC911, which has been granted elevated access to make changes to ACEDS production programs in emergency situations. This account can be utilized on a temporary basis by individuals who can authorize and implement emergency program changes in the production environment.

g. Management has not instituted a formalized process to periodically review access to update and install mainframe database system software. As a result, we noted the following instances in which such access was not assigned based on least privilege and need-to-know security concepts:

    1) Three of 15 users with the ability to update the mainframe datasets for DB2 database system software supporting the SOAR and TAS applications did not require such access to perform their job responsibilities.

    2) 55 of 57 users with the ability to update the mainframe datasets for ADABAS database system software supporting the ACEDS application did not require such access to perform their job responsibilities.

h. During our test work over the process for making changes to eligibility determination tables within ACEDS, we noted the following conditions:

    1) There is no process in place to periodically review system changes made to ACEDS eligibility tables to ensure that they were appropriately authorized.

    2) The individual primarily responsible for approving eligibility table changes also has the ability to make changes to the eligibility tables.

i. During our test work over physical access to the OCTO ODC1 and ODC2 facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications, we noted the following conditions:

    1) Management was unable to provide the physical access request form for 1 of 3 employees selected for testing, who were granted physical access to the ODC1 and ODC2 computer rooms during fiscal year 2010.

    2) We compared a list of separated employees for the period of October 1, 2009 through September 9, 2010, to ODC1 and ODC2 physical access listings generated on September 27, 2010, and identified 4 active physical access badges belonging to individuals who no longer worked for the District.

j. We compared a list of separated employees for the period of October 1, 2009 through September 8, 2010, and an ACEDS access list generated on August 30, 2010, and identified 12 active accounts with mainframe and application access that belonged to individuals who no longer worked for the District. During procedures performed to

evaluate the impact of this access, we noted that none of the 12 accounts had a logon date after the date of separation from the District.

k. Management does not periodically review ACEDS application access to ensure that user access permissions remain commensurate with employee job responsibilities.
According to management, ACEDS user accounts are reviewed periodically to determine whether they belong to separated employees. However, this review process does not include consideration of the appropriateness of users' access rights in relation to their current job responsibilities. Further, this review is not documented to evidence its completion.

l. 1 of the 4 ACEDS application developers had administrative privileges to the production database that supports the ACEDS application.

Recommendations:

a. We recommend that management periodically communicate existing OCTO change management procedures to the individual control performers. During these communications, management should ensure that the control performers are, at a minimum, aware of the following concepts:

- Recording the nature of each change being applied;
- Evaluating the impact and risk of each change relative to objective rating criteria;
- Obtaining approval/approving (and documenting such approvals of) changes; and
- Validating the functionality/system impact of each change via pre-production testing in a model environment or post-implementation confirmations.

Further, management should monitor control performer adherence to the procedures on a periodic basis. Management should also continue with their plans to implement an automated change monitoring system that will be installed on production infrastructure environments for purposes of capturing and reporting changes made to production systems.

b. We recommend that management develop and implement a process to review, update, and communicate the OCTO Password Management Policy to responsible individuals on a periodic basis to help ensure it remains current. We further recommend that this policy include, at a minimum, requirements for the following password configuration settings:

- Minimum password length;

- Password aging and update requirements;
- Password complexity (e.g., at least one number, letter, and special character);
- User account lockout after a predefined number invalid logon attempts; and
- Password history/reset restrictions.

In support of the recommended remediation, management should reconfigure existing password configuration settings at the application, operating system and database level, where applicable, in accordance with the revised OCTO Password Management Policy. Finally, we recommend that management monitor adherence to the policy on a periodic basis.

c. We recommend that management develop and formally document application program change management policy/procedures that include, at a minimum, procedural and documentary requirements for:

- Recording the nature of each change being applied;
- Evaluating the impact and risk of each change relative to objective rating criteria;
- Approving (and documenting such approvals of) changes; and
- Validating the functionality/system impact of each change via pre-production testing in a model environment.

The policy/procedures should establish specific approval and validation requirements for each defined impact/risk level such that impactful/riskier changes must undergo more stringent approval and validation activities than less impactful/risky changes.

These policies/procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

d. We recommend that management establish a formalized process for performing periodic reviews of physical access to the ODC1 and ODC2 Data Centers to determine whether individuals who have such access still require it to perform their job responsibilities. The process should include requirements for documenting the review, including the modification of any inappropriate physical access privileges identified during its performance.

This process should be recorded in a formal policy or procedure document and provided to and discussed with control performers. Further, management should monitor adherence to the process on a periodic basis.

e. We recommend that management develop and implement change management processes and controls that establish one or more of the following:

- Organizational and logical segregation of program development roles from production system administration roles among different individuals; and,

- Implementation of one or more independently operated monitoring controls over the activities of the developers (and other individuals) with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.

- Further, we recommend that management monitor the effectiveness of the controls on a regular and periodic basis.

f. We recommend that management, at a minimum, establish procedural and documentary requirements for:

- Granting management approval for the use of the generic account to make ACEDS application changes in the production environment, including segregating access between individuals who can authorize and implement application changes.

- Periodically reviewing detailed audit logs associated with the use of the generic account and, for any inappropriate activities identified, conducting research/resolution activities as needed.

These requirements should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

g. We recommend that management remove the logical access permissions which allow the individuals referenced in the condition above to update and install mainframe database system software. Management should also perform a review of all individuals with this privileged access and ensure that each individual requires this access to perform his or her job responsibilities.

Additionally, we recommend that management institute a formalized, periodic review process to determine whether users with the ability to update and install mainframe database system software require this access in order to perform their job responsibilities. In support of the recommended remediation, management should develop and formally document procedures for performing reviews that address

mandatory review steps, follow-up procedures for any exceptions identified, and documentation generation and retention requirements. These procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

h. We recommend that management establish and implement formalized procedures for changing ACEDS eligibility determination tables that, at a minimum, include consideration for following:

- Including copies of the applicable policy/legislation and corresponding authorizations in the supporting documentation that is prepared and maintained when eligibility determination table changes are performed.

- Implementing a formalized process for the periodic review of system-generated audit trails/history of changes made to eligibility determination tables. This process should include mandatory review steps, follow-up procedures as a result of inappropriate changes identified, and documentation generation and retention requirements.

- Segregating the functions for authorizing eligibility table changes and performing updates to the eligibility tables. If this segregation of duties is not feasible based on resource limitations, mitigating processes should be implemented to ensure that unauthorized changes are not made to the eligibility tables.

These procedures should be provided to and discussed with control performers. Further, management should monitor adherence to the procedure on a periodic basis.

i. We noted that management has established a formalized procedure for requesting physical access to the ODC1 and ODC2 computer rooms, which requires documented access requests and authorization from the Mainframe Security Manager. This existing procedure should be provided to and discussed with control performers within the OCTO organization. Further, management should monitor adherence to the procedure on a periodic basis.

We recommend that management establish timeliness requirements for the communication of employee separations and disablement/removal of the related physical access rights. This process should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor adherence to the procedure on a periodic basis.

j. We recommend that management establish requirements related to the procedures for the timely communication of employee separations/transfers and disablement/removal of the related user access. This process should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further,

management should monitor control performer adherence to the procedure on a periodic basis.

k. We recommend that management refine its current periodic review process to include procedures to determine whether ACEDS application user access remains commensurate with employee job responsibilities for all ACEDS user access profiles.
In support of the recommended remediation, management should develop and formally document procedures for performing reviews that address mandatory review steps, follow-up procedures for any exceptions identified, and documentation generation and retention requirements. These procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

l. We recommend that management develop and implement processes and controls that establish one or more of the following:

- Organizational and logical segregation of program development roles from production database administration roles among different individuals; and,

- Implementation of one or more independently operated monitoring controls over the activities of the developers (and other individuals) with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.

Management Response:

a. Management concurs with the facts of this finding.

b. Management concurs with the facts of this finding.

c. Management concurs with the facts of this finding. With respect to Condition #3, despite the fact that procedures are currently in place to validate the accuracy of requested changes prior to their migration to the Production environment, IMA does not maintain documentation of test cases. In the future, a log will be kept that identifies the case numbers associated with the testing along with the purpose of the test, procedures used in the test, and the results of the test.

OIS Programmers will document their programs with the Change Request Number, in the COBOL and Natural programs. We will add the Change Request Number to the PanApt move request and all Components, i.e. Proc's, JCL, Adhoc's and add the Natural/COBOL Programs in the Change Request Tracking System.

d. Management concurs with the facts of this finding.

e. Management concurs with the facts of this finding. DHS' current funding does not allow for acquiring/having the three (3) staff for each segregated administration role necessary to run a 24x7 operation and comply with the stated recommendation.

f. Management concurs with the facts of this finding. OIS Programmers will notify the OIS Chief, or Supervisor of PC Support to request PC911 to be reset, if an ACES job ABENDS.

   New procedures for resetting PC911:

   1) Call OIS Chief or Supervisor or PC Support and request PC911 to be reset and why.

   2) OIS Chief or Supervisor of PC Support will call security group, Infosec, and indicate the reason for the use of the PC911.

   3) After security group resets PC911 they will contact the OIS Chief or Supervisor of PC Support and provide a new password.

   4) OIS Chief or Supervisor of PC Support will contact the OIS Programmer with the new password.

g. Management concurs with the facts of the finding. Provider Services will conduct periodic spot audits to ensure that the provider licensure on file mirrors the license information displayed "provider eligibility/specialty" tab within the Medicaid Management Information System.

h. Management concurs with the facts of the finding. The Assistant Deputy Administrator for Information Systems is responsible for approving changes to the ACEDS eligibility tables. His ability to also update those tables has been revoked in order to comply with the audit finding. The Assistant Deputy Administrator for Information Systems will also begin a periodic review of the table update report and will certify (on the report) that it has been reviewed. Any anomalies will be noted along with follow-up actions.

i. Management concurs with the facts of the finding. .

j. Management concurs with the facts of the finding. Though ACEDS Security Officers review each user group once per year, users often fail to inform the Security Officers that staff have retired, resigned or been terminated. In order to address this weakness, the following steps will be taken:

   The ACEDS Security Manual will be updated to reflect the requirement that managing staff report such staff changes to the Security Officer(s) immediately.

The appropriate portions of the revised ACEDS Security Manual will be distributed to office contacts, highlighting this requirement.

Within IMA, the Division of Information Systems will coordinate with the other divisions to facilitate prompt reporting of personnel changes.

k. Management concurs with the facts of this finding. Currently, ACEDS Security Officers review each user location once per year. Starting with reviews conducted during the month of January 2011, a written report of findings will be submitted to the Deputy Administrator for Information Systems following each review. The report will include an evaluation of users' access rights with respect to current job responsibilities.

l. Management concurs with the facts of the finding. DHS' current funding does not support the staffing required to segregate and divide program development roles and functions from production database administration roles and functions.

2. Department of Employment Services Applications (BARTS, DOCS, and DUTAS)
We identified the following deficiencies in the general IT controls environment supporting the applications utilized by the Department of Employment Services (DOES):

a. Management informed us that a review of user access was performed for all applications in June 2010 and submitted a user listing of personnel with access to DUTAS at the database and operating system levels that they indicated was evidence of part of the June 2010 reviews. However, signed review sheets representing the formal completion of the reviews were not available for inspection. Further, we noted that DOCS and DUTAS user access lists generated in September 2010 contained user access that should have been removed as a result of a review performed in June 2010.

   Management performed user access reviews of BARTS, DOCS, and DUTAS in October 2010 upon our recommendation and submitted documentation of those reviews for inspection. Based on a review of the documentation provided, we noted that management performed actions to remove the DOCS user access we considered inappropriate based on our review of the access list generated in September 2010. We also noted that the BARTS and DUTAS reviews indicated management did not note any instances of inappropriate access as a result of their review.

b. During the months of August and September 2010, the DOCS business owner applied user access changes directly to accounts in the application instead of forwarding her approved user access requests to the security administrator for configuration.

   However, we noted that in October 2010, DOES IT management performed a DOCS user access review and indicated that although the DOCS business owner did not follow the established process, the access changes that she made were properly authorized in consideration of the users' job responsibilities and 'need-to-know.'

c. DOES management has instituted a process whereby BARTS, DOCS, and DUTAS program changes are discussed and approved during weekly change management meetings and documented in weekly status reports. For the period October 1, 2009 through July 31, 2010, management had not instituted formal procedures to document program change descriptions, approvals and the performance of change testing. As a result, prior to August 2010, management did not consistently document program change descriptions, approvals, or testing activities for DOCS and DUTAS.

   KPMG was informed that only one BARTS application deployment was implemented into the production environment during Fiscal Year 2010. KPMG noted an associated change approval form and an email documenting user acceptance test success were retained for this change. However, KPMG considered documentation of testing provided insufficient to evidence the performance of user acceptance testing procedures and associated results.

Further, a DOES Project Implementation Approval form used to document the effective date of change, description of change was not available for inspection because it had not yet been required by DOES during the initiation of the BARTS application deployment project. However, KPMG did review an e-mail sent by the Department of Health and Human Services documenting the pre-implementation approval of the project.

d. Two of seven DOCS developers and all of the DUTAS developers (two individuals) have access to the production environment and the ability to migrate DOCS and DUTAS program code into production. In addition, management has not implemented other mitigating change management controls.

   Management does not have an independently operated control to monitor and document the activities of developers that have access to the production environment. Management informed us that it has instituted an informal peer review process whereby the four developers referenced above split the responsibilities for change development and review/migration such that no changes are developed and implemented by the same individual within each system; however, documented evidence of the peer review was not available for our review.

e. During testing to evaluate the BARTS access authorization process, we noted the following related to two of three user accounts created for BARTS, DOCS and DUTAS in fiscal year 2010:

   1) For one out of the three user accounts noted above, management was unable to provide evidence of the second approver's issuance of a documented authorization of the access provided.

   2) For one out of the three user accounts noted above, management was unable to provide the signed user access form as required by the DOES process. However, we received and reviewed an email implying that the access was approved by the Chief of Tax.

   We further noted that in October 2010, DOES management performed user access reviews and indicated that although documentation evidencing the supervisory approval was unavailable for one of the two users noted above, the corresponding access granted was nevertheless authorized in consideration of job responsibilities and the users' need-to-know.

Recommendations:

a. We recommend that management institute a formalized, periodic review process to determine whether BARTS, DOCS and DUTAS user access remains commensurate with employee job responsibilities.

In addition, management should develop and formally document procedures for performing reviews that address mandatory review steps, follow up procedures for any exceptions identified, and documentation generation and retention requirements. Management should provide training on this policy to those responsible for performing these procedures and monitor to ensure adherence to the policy.

b. We recommend that management finalize its draft access management policy and procedures for the DOCS production application. The finalized policy/procedures should include, at a minimum, procedural and documentary requirements for requesting, approving and configuring user accounts. Management should provide training on this policy to those responsible for performing these procedures and monitor to ensure adherence to the policy.

c. We recommend that management enhance its current change management policies and procedures, which at a minimum include procedural and documentary requirements for:

- The completion of a formal change request form(s);
- Authorization of the change prior to initiation of the work;
- The minimum requirements for performing and documenting testing to determine whether the change is operating as required;
- Formal approval of the change prior to migration to production; and
- Monitoring controls to assess the completeness and accuracy of manual change control listings maintained by management.

Management should provide training on this policy to those responsible for performing these procedures and monitor the change management process to ensure adherence to the policy.

d. We recommend that management develop and implement change management processes and controls that establish one or more of the following:

- Organizational and logical segregation of program development roles from production system administration roles among different individuals; and
- Implementation of one or more independently operated monitoring controls over the activities of the developers (and other individuals) with access to the production environment that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.

Management should provide training on this policy to those responsible for performing these procedures and monitor to ensure adherence to the policy.

e. We recommend that management develop and formally document the access management policy and procedures for the DOES production applications. We recommend that these include, at a minimum, procedural and documentary requirements for:

   - Requesting, approving and configuring user accounts; and
   - Periodic reviews of user access performed in consideration of users' ongoing need to retain BARTS access and segregation of duties considerations, and the configuration of any updates required as a result of inappropriate access identified during the review process.

   Management should provide training on this policy to those responsible for performing these procedures and monitor to ensure adherence to this policy.

Management Response:

a. Management concurs with the facts of this finding. Documentation was provided to support the initial review of user access lists in June 2010, but we were not able to provide the requested sign-off sheets for this first formalized review. Regarding the user access reviews performed in the fall, it should be noted that this is a semi-annual review process. The next scheduled time for review is December 2010, but at the request of KPMG, we incorporated an additional review in October. At this time, we noted user access considered to be inappropriate, and removed such access. In addition, we did provide the documentation regarding the completed DUTAS access review. All of these reviews, and the subsequent modification and/or removal of access would have been performed during the semi-annual review in December, as planned.
b. Management concurs with the facts of this finding. KPMG has acknowledged that DOES has an established process for user access review and access granting, and has not cited further instances of user access being granted outside the established protocols. From the criteria you provided, "User account management typically begins with a request from the user's supervisor to the system manager for a system account." In this instance, the user who granted the access (User #1) was the manager of the division, and the supervisor of the manager (User #2) to whom access was granted. As User #2 already had access to the system, this was an add-on request for which initial system authorization had been granted.

c. Management concurs with the facts of this finding. In one of three user access accounts noted above, management provided verbal secondary approval for an access change. We have since instituted a policy that allows for email approval by appropriate management remotely when necessary. Regarding the implied approval highlighted above, management has since instituted a policy that approvals must always be explicitly stated in writing. When access to official approval documentation is not available when Management is physically unavailable, approval may be provided from a

secure email account assigned only to said Management. Upon Management return, documents must be completed, signed and attached to approval email.

d. Management concurs with the facts of this finding. However, there are three DUTAS developers and two have access to migrate changes to production. Additionally, Management is in the process of adding additional staff to fully implement best practices of separation of duties.

e. Management concurs with the facts of this finding. In one of three user access accounts noted above, management provided verbal secondary approval for an access change. We have since instituted a policy that allows for email approval by appropriate management remotely when necessary. Regarding the implied approval highlighted above, management has since instituted a policy that approvals must always be explicitly stated in writing. When access to official approval documentation is not available when Management is physically unavailable, approval may be provided from a secure email account assigned only to said Management. Upon Management return, documents must be completed, signed and attached to approval email.

3. iNovah

We noted the following deficiencies in the general IT controls environment supporting the iNovah application:

a. Management does not periodically review iNovah application access to ensure that user access permissions remain commensurate with employee job responsibilities for all of the departmental units that use iNovah.

   According to management, a bi-annual review is performed to determine whether iNovah user access remains commensurate with employee job responsibilities; however, this review is not documented consistently. Specifically, for both (two) reviews selected for testing, management was unable to provide documentary evidence that the reviews took place.

b. One of six accounts assigned administrative privileges within the production version of the iNovah application belonged to a business end user. The administrative privileges in question – '*Administrators' – provides users to which it has been assigned the ability to perform all iNovah business functions, reset passwords, create and delete user accounts and add and modify application privileges associated with user accounts.

c. According to management, vendor-initiated operating system changes issued during the 2010 fiscal year were automatically applied upon receipt. Management did not document change approval or activities performed, if any, to validate the functionality of the changes or their impact on the production environment.

d. Documentation evidencing the periodic backup and rotation of backup tapes to an offsite storage facility was unavailable prior to March 2010. Management has indicated that during the physical move of the OCFO data center during March 2010, backup records and old tape media were destroyed as a new backup process and virtual offsite storage process were put in place.

e. During our test work over physical access to the OCFO Data Center facility used to host the iNovah application, we noted the following conditions:

   1) Management was unable to provide the physical access request form for four (4) of eight (8) employees selected for testing who were granted physical access to the OCFO computer rooms during fiscal year 2010.

   2) We compared a list of separated employees for the period of October 1, 2009 through September 9, 2010 to OCFO physical access listing generated on September 27, 2010, and identified four (4) active physical access badges belonging to individuals who no longer worked for the District.

f. During our test work over operating system and database administrator access and infrastructure change management for iNovah, we noted that 19 Windows Server

operating system administrators had the ability to logon using the "secadm" user account, which allowed these individuals to perform operating system and SQL Server Database administration functions under a generic user account. Additionally, we were informed by management that no process has been established for the review of the actions performed using this super user account.

Recommendations:

a. We recommend that management review and refine as necessary the periodic review policy which includes a process to determine whether all personnel with iNovah user access remains commensurate with employee job responsibilities and communicate this policy for all of the departmental units that use iNovah. Further, we recommend that management periodically monitor the performance of the periodic user access review process to determine whether it is being performed as required by the policy.

   In addition, management should develop and formally document procedures for performing reviews that address mandatory review steps, follow up procedures for any exceptions identified, and documentation generation and retention requirements.

   Management should provide training on this policy and procedures to those responsible for performance of these controls; and monitor to ensure adherence to this policy.

b. We recommend that management develop and implement controls that establish one or more of the following:

   - Documented and periodically review policy/procedures that define the job functions authorized by management to have access to the iNovah administrator role;

   - Organizational and logical segregation of duties related to production system support, user security administration, and general business user roles among different individuals; and/or

   - Implementation of one or more independently operated monitoring controls over the activities of individuals with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.

c. We recommend that management develop and formally document and implement infrastructure change management policy/procedures that include, at a minimum, procedural and documentary requirements for:

   - Recording the nature of each change being applied;

- Evaluating the impact and risk of each change relative to objective rating criteria;

- Approving (and documenting such approvals of) changes; and

- Validating the functionality/system impact of each change via pre-production testing in a model environment or post-implementation confirmations.

The policy/procedures should establish specific approval and validation requirements for each defined impact/risk level such that impactful/riskier changes must undergo more stringent approval and validation activities than less impactful/risky changes.

Management should provide training on these policies and procedures to those responsible for performance of these controls; and monitor on a periodic basis to ensure adherence to the policies and procedures.

d. We recommend that management develop and implement formal policies and procedures for establishing minimum retention guidelines pertaining to data backups and remote storage which include, at a minimum, procedural and documentary requirements for:

    - Periodically backing up the iNovah application, operating system, database and stored data;

    - A schedule for backing up data to the offsite storage facility; and

    - Periodically restoring backup media to help ensure recoverability of data.

    Management should provide training to those responsible for performing these procedures and monitor to ensure adherence to the policy.

e. We noted that management has established a formalized procedure for requesting physical access to the OCFO computer rooms, which requires documented access requests and authorization from the Network Operating System Administration Team. This existing procedure should be provided to and discussed with control performers within the OCFO organization. Further, management should monitor adherence to the procedure on a periodic basis.

    Management should develop formalized policies and procedures for communication of employee separations and disablement/removal of the related physical access rights, which includes requirements for timely removal of this access. Management should provide training on this policy to those responsible for performing this control. Further, management should monitor control performer adherence to the procedure on a periodic basis.

f. We recommend that management re-assess the use of the "secadm" generic super user account including the associated access privileges. Additionally, we recommend that management establish requirements that administration functions be performed using unique user accounts. These requirements should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

Management Response:

a. Management concurs with the facts of the finding. Management instituted a formalized periodic access review process to review use access to the iNovah application for non-Office of Finance and Treasury (OFT) users; however, this process will be applied consistently to include the entire iNovah user community to include OFT locations. OFT will continue to refine its review process, as necessary, as the system is rolled out. At this time, iNovah will not produce an audit report to track system access. There is a quarterly system audit report under development by OCIO to capture each user's transactions and system access capabilities. It is planned that OFT, along with OCIO, will conduct audits and reviews on user access through this system-wide quarterly report generated by iNovah. The report will formally document the system access by person and identify exceptions. Again, further documentation of procedures for performing reviews, modifying application and system audit processes, following up on procedures for exceptions, as well as policy training will be ongoing as OFT and OCIO continue to implement iNovah in the remaining 31 sites. Lastly, management will monitor to ensure adherence to this procedure.

b. Management concurs with the facts of the finding. We will develop standard operating procedures for TACIS user access to include implementation of quarterly review of user access commensurate with the employee's job responsibilities, obtain the appropriate authorization, and maintain documentation to support user access in accordance with the District's records retention period.

c. Management concurs with the facts of the finding. OCIO concurs with this finding. Past practice has been to apply critical security related Operating System patches for windows operating system immediately upon receipt to the iNovah system. This policy has been necessary to thwart and mitigate the risk of critical cash and credit card data from inadvertent hack or disclosure due to weaknesses in the windows operating system. Moreover, a separate test platform instance did not exist for iNovah, making it impossible to independently test the patches and upgrades before migrating to production.

   The OCIO has implemented an infrastructure change management process and is currently being used to communicate and receive acceptance for all infrastructure changes including operating system patches and upgrades. The process has been in place for several months and includes iNovah system upgrades. The OCIO intends to

continue this process in the future. Moreover, the OCIO plans to implement a separate test environment for the iNovah system where patches can be tested and application functionality can be verified prior to migration to production.

d. Management concurs with the facts of the finding. OCIO recognizes and adheres to the agency backup and recovery processes for all critical production systems. During the relocation to the waterfront in March 2010, the OCIO took the opportunity to purge legacy backup tapes retained and started new processes that were compliant with the new server room and infrastructure. Since that time, all backup processes have been followed within the new infrastructure. OCIO will continue to comply with the backup requirements for the iNovah system.

e. Management concurs with the facts of this finding with the following caveat(s):
The DC OCFO will comply with and enforce OCFO Policy Number ITST005, OCFO Physical Security Control Standard according to the formalized and approved standards contained therein. ITST005 will be redistributed to the control performers within OCFO responsible for physical access to OCFO information technology and computing platforms. Additionally, OCFO will re-train said control performers on the tenants of ITST005 and will periodically validate control performance adherence to ITST005 on a bi-annual basis.

In addition, OCFO Human Resources does indeed have a standardized procedure for the communication of employee separations and the corresponding disablement and removal of related physical access rights. At present, the standard is to disable all facility access, including access to facility rooms housing computing infrastructure by COB on the day of employee separation. OCFO will continue to comply and enforce this standard and will document this standard in a formal policy and corresponding procedure document.

f. Management concurs with the facts of the finding. The DC OCFO will comply with and enforce the policy ITAD029 – OCIO Production Environment Access Policy.pdf. We will change the secadm password by 1/31/2011, limit its use to security officers, and force help desk personnel to log in using their own accounts. We have also implemented a change on 1/3/2011 preventing help desk personnel from changing and domain admin or service account passwords.

4. Meditech

We noted the following deficiencies in the general IT controls environment supporting the Meditech application at the United Medical Center (UMC):

a. Management has not implemented a formalized Meditech application review process to determine whether Meditech user access is commensurate with job responsibilities on an ongoing basis.

   1) Reviews of Meditech user access are performed by the IT Director or an IT Analyst; however, these reviews are not performed on a regular basis or documented. As a result, no evidence could be provided of the user access reviews that management stated it performed during audit period.

   2) We identified an active Meditech application level user account belonging to 1of 23 employees who separated from UMC during the audit period. The access remained active for approximately two months after the employee's separation.
   3) Requests for changes to Meditech user access are performed by the IT Director or an IT Analyst; however, documentation of the requests for access changes is not consistently maintained.

b. We noted the following during our testing of UMC's backup and recovery controls:

   1) Meditech backup tapes were not rotated offsite during the audit period;

   2) Management did not test the recovery of Meditech application data from the backup tapes during the audit period; and

   3) Evidence of the successful completion of backups was not available for 6 of 15 days selected for testing.

c. We were informed that IT personnel did not document computer incident impacting the Meditech application in a consistent manner. Specifically, when the help desk ticketing system was unavailable, incidents and their resolutions were informally documented via e-mail and/or discussed and resolved over the phone.

d. Management was unable to provide documentation of the completion status of Meditech application jobs executed during the audit period and, for any jobs that failed, evidence that the failure was addressed.

Recommendations:

a. We recommend that management institute a formalized, periodic review process to determine whether Meditech user access remains commensurate with employee job responsibilities.

Management should also re-emphasize existing requirements to UMC personnel responsible for maintained Change Requests and should periodically monitor staff performance to help ensure ongoing compliance.

In addition, management should develop and formally document procedures for performing reviews that address mandatory review steps, follow up procedures for any exceptions identified, and documentation generation and retention requirements. Management should provide training on this policy to those responsible for performing these procedures and monitor to ensure adherence to the policy.

b. We recommend that management implement the requirements established in UMC Policies IT 03-014 and IT-03-15 by completing the following activities:

- Establishment of an offsite location for the storage of backup tapes;
- Implementation of a process to deliver backup tapes to the offsite location and consistently document all tape movements to and from the offsite location; and
- Implementation of a periodic process to recover backup tapes on a test basis to verify their ongoing integrity.

Management should also re-emphasize existing requirements to UMC personnel responsible for printing out and filing the backup tape log on a daily basis and should periodically monitor staff performance to help ensure ongoing compliance.

c. We recommend that management enforce UMC Policy IT 03-001 by taking the following actions:

- Remediate issues associated with the ticket tracking system;
- Re-introduce the ticket tracking system into operation as the system of record for documenting computer-related incidents and activities taken to resolve them; and
- Communicate the implementation of the remediated ticket tracking system to personnel responsible for its use as the singular method for documenting computer-related incidents and activities taken to resolve them.

d. We recommend that management implement requirements that responsible personnel document the completion status of Meditech application jobs executed during the audit period and, for any jobs that failed, evidence that the failure was addressed. These requirements should be documented in a policy or procedure and management should periodical monitor adherence to the requirements.

Management Response:

Appendix A

a. Management concurs with the facts of the finding. The United Medical Center Information Technology Department is committed to the process of continuous improvement of its privacy and security practices. This includes the introduction of new enabling technologies and updating of policies and procedures. Technology is in a rapid state of change and threats to our environment are equally dynamic. Therefore, we are engaged in a never ending cycle of improving our interior and perimeter security.

   Management has a policy that requires audit reviews be performed of user access levels. The purpose of our policy is to prevent unauthorized use or access that is not consistent with job responsibilities. UMC IT staff performs routine reviews of user access to determine compliance with our policies. It has not been our practice to prepare supporting documents of these reviews. In the future, we will develop documentation consistent with actions taken to ensure compliance of this policy.

   It is Management's policy that all requests for access changes be submitted to the help desk on our "IT Request for Access or Change Request Forms." These change request forms are received by the help desk, reviewed, executed and filed for record keeping. It has also been our unofficial practice to accept change requests via email. These requests have not been maintained consistently. In the future, we will only accept properly authorized change request forms. This change in practice will ensure only properly authorized access level changes are made and also increase our documentation.

b. Management concurs with the facts of the finding. Management previously utilized Hadley, a sister facility of our previous owner, for storing offsite daily tapes. The change of ownership essentially eliminated this option. We will reinstitute this process at an alternate site. Management is currently evaluating the site where our medical records are stored and will use this site for now.

   Castle Systems is our disaster recovery vendor. We send them a back up tape annually. Management currently does not have a contract with Castle. Since the agreement was with the previous owner. Management will initiate the contracting process, then set up and perform a formal recovery from tape. Management is also evaluating our infrastructure to determine if we can perform a formal recovery from tape in our existing environment.

   Backups in our HIS system are automatic. Care taker messages are printed out, reviewed and subsequently discarded. Our process states in addition, we will perform a screen print of the backup and place in a log. Management's practice has not been consistent with our policy. We have implemented an extra layer of supervisory sign-off to ensure compliance with our policy.

c. Management concurs with the facts of the finding. IT takes Security for the organization seriously and every effort is taken to ensure that there are no intrusions or breaches within our system or network environment. We strive to stay in a continuous

improvement mode that will allow us to always secure our technology environment, while meeting the needs of our users. We look at this audit as an opportunity for improvement and to assist us with always meeting or surpassing our goals.

A healthy Helpdesk tracking system is essential to us meeting those goals. It's the point of entry for IT services, department and organization statistics, as well as PI initiatives for IT. Issues with not being able to consistently access and use our helpdesk has limited our ability to adhere to our policy that all requested be entered in our helpdesk tracking system. Therefore, we deployed alternate measures to maintain records of requests for IT services.

We have been reviewing CRM vendor systems in an effort to find a replacement solution. Management is seeking a system that will track electronic requests, customer satisfaction feedback as well as statistical reporting. We hope to have a new system implemented within the fiscal year 2011.

d. Management concurs with the facts of the finding. Management's primary goal for the IT Department is assuring that our systems are up and functioning at optimal levels at all times. A monitor at the helpdesk tracks and gives a visual when systems are not connected to the network, and will remain that way until it is addressed and the system is back on the network.

   Meditech daily backups are done automatically by the system. In addition, there is a feature called caretaker messages inherent within the system. This feature tracks all messages generated, and can be run for a limited date range to view what the actual status of the system was for that given time period. While all network interruptions are not documented such as with power surges, system crashes, and planned downtimes are logged. Management will be incorporating into the current process that staff document all downtimes and resolutions of the event for better tracking.

5. PASS

We noted the following deficiencies in the general IT controls environment supporting the PASS application:

a. During discussions with management, we were informed that two infrastructure changes were implemented into production without prior approval from the OCTO Change Advisory Board (CAB). These changes resulted in temporary service outages to DCIT networks and systems.

   1) Management has indicated that these changes were not malicious in nature and that the individuals who implemented the changes were unaware of the impact of implementing the changes directly into the production IT environment. Management also noted that the changes had no impact on the integrity of processing or data of the in-scope applications.

   2) Management informed us that they plan to implement an automated change monitoring system that will be installed on production infrastructure environments for purposes of automatically capturing and reporting changes to further strengthen the infrastructure change management process.

b. Management has not updated its policy that defines the minimum password configuration requirements for DCIT systems in over six years. Further, inquiry and inspection procedures performed by the audit team indicate that the policy was not effectively communicated to responsible personnel. Specifically, we noted the following:

   1) The OCTO Password Management Policy, dated September 2004, does not require that systems be configured to automatically lock out user accounts after a predefined number of invalid log-on attempts.

   2) Inquiry of four individuals at the management level who have responsibility for implementing password security parameters for in-scope applications informed us that they were neither aware of nor able to locate the OCTO Password Management Policy document.

   3) We noted various inconsistencies between the requirements outlined in the OCTO Password Management Policy and configurations set within the in-scope applications and their supporting databases and operating systems.

c. Management does not periodically review physical access to the OCTO ODC1 and ODC2 facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications.

d. One of three application developers had access to the 'system administrator' role within PASS. Users assigned this role can create, modify access to, and delete PASS user accounts.

   Management informed us that it authorized the developer's access levels described above for the express purpose of providing on-going support of the performance and availability of PASS.

e. During our test work over physical access to the Office of the Chief Technology Officer OCTO ODC1 and ODC2 facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications, we noted the following conditions:

   1) Management was unable to provide the physical access request form for 1 of 3 employees selected for testing, who were granted physical access to the ODC1 and ODC2 computer rooms during fiscal year 2010.

   2) We compared a list of separated employees for the period of October 1, 2009 through September 9, 2010, to ODC1 and ODC2 physical access listings generated on September 27, 2010, and identified 4 active physical access badges belonging to individuals who no longer worked for the District.

f. During our test work over operating system administrator access and infrastructure change management for PeopleSoft and PASS, we noted the following conditions:

   1) UNIX operating system administrators have the ability to and typically logon directly to the 'root' user account, which allows these individuals to perform operating system administration functions under a generic user account. Additionally, no process has been established for the review of the actions performed by this super user account.
   2) Oracle database administrators currently utilize generic user accounts to perform database administration functions. No process has been established for the review of the actions performed by these generic user accounts.

   3) Management does not have a formalized process in place for periodically changing the password for the 'root' operating system privileged user account or generic privileged accounts with access privileges to perform Oracle database administration functions.

g. We compared a list of separated employees for the period of October 1, 2009 through September 8, 2010 and a PASS access list generated on September 23, 2010, and identified a significant number of active accounts with application access that belonged to individuals who no longer worked for the District.

h. For the period June 1, 2010 through September 30, 2010, management did not adhere to the formal process in place to rotate backup tapes for the PeopleSoft and PASS applications, operating systems, databases, and their data to an offsite storage facility.

i. We noted deficiencies in the design of management's existing process to periodically review PASS application user access permissions. Specifically, the following was noted relating to the adequacy of the periodic review process:

   1) Two of seven DC Government Agencies selected for testing were not included in the FY2010 annual review process.

   2) Of three DC Government Agency Security Officers (ASOs) interviewed, we noted that the ASOs did not maintain the PASS user access listings, which include the associated roles, privileges and approval limits, that were generated in order to perform the PASS application access review.

j. Management has not established a monitoring process to ensure that PASS production jobs complete in a successful manner, specifically, for identifying and remediating PASS production jobs that end abnormally.

k. 5 of 8 user accounts, assigned the QA TEAM and QA LEAD roles, with the ability to migrate PASS application changes into the production environment through the Serena Dimensions change management tool belonged to employees that did not require such access to perform their job responsibilities. During procedures performed to evaluate the impact of this access, we determined based on inspection of a listing of PASS application changes migrated to production during fiscal year 2010, that none of these individuals performed any migration activities for the PASS application

Recommendations:

a. We recommend that management periodically communicate existing OCTO change management procedures to the individual control performers. During these communications, management should ensure that the control performers are, at a minimum, aware of the following concepts:

   - Recording the nature of each change being applied;

   - Evaluating the impact and risk of each change relative to objective rating criteria;

   - Obtaining approval/approving (and documenting such approvals of) changes;

   - Validating the functionality/system impact of each change via pre-production testing in a model environment or post-implementation confirmations; and

- Further, management should monitor control performer adherence to the procedures on a periodic basis. Management should also continue with their plans to implement an automated change monitoring system that will be installed on production infrastructure environments for purposes of capturing and reporting changes made to production systems.

b. We recommend that management develop and implement a process to review, update, and communicate the OCTO Password Management Policy to responsible individuals on a periodic basis to help ensure it remains current. We further recommend that this policy include, at a minimum, requirements for the following password configuration settings:

- Minimum password length;
- Password aging and update requirements;
- Password complexity (e.g., at least one number, letter, and special character);
- User account lockout after a predefined number invalid logon attempts; and
- Password history/reset restrictions.

In support of the recommended remediation, management should reconfigure existing password configuration settings at the application, operating system and database level, where applicable, in accordance with the revised OCTO Password Management Policy. Finally, we recommend that management monitor adherence to the policy on a periodic basis.

c. We recommend that management establish a formalized process for performing periodic reviews of physical access to the ODC1 and ODC2 Data Centers to determine whether individuals who have such access still require it to perform their job responsibilities. The process should include requirements for documenting the review, including the modification of any inappropriate physical access privileges identified during its performance.

This process should be recorded in a formal policy or procedure document and provided to and discussed with control performers. Further, management should monitor adherence to the process on a periodic basis.

d. We recommend that management develop and implement change management processes and controls that establish one or more of the following:

a. Organizational and logical segregation of program development roles from production system administration roles among different individuals; and

b. Implementation of one or more independently operated monitoring controls over the activities of the developers (and other individuals) with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.

e. We noted that management has established a formalized procedure for requesting physical access to the ODC1 and ODC2 computer rooms, which requires documented access requests and authorization from the Mainframe Security Manager. This existing procedure should be provided to and discussed with control performers within the OCTO organization. Further, management should monitor adherence to the procedure on a periodic basis.

   We recommend that management establish timeliness requirements for the communication of employee separations and disablement/removal of the related physical access rights. This process should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor adherence to the procedure on a periodic basis.

f. We recommend that management establish and implement formalized operating system and database security policies that, at a minimum, include consideration for following:

   - Configuring the UNIX operating system to prevent users from logging on directly to the 'root' user account;

   - Implementing a formal process that requires users to logon using their unique user accounts before executing the switch user (SU) or 'SUDO' command to access the 'root' account, thus establishing an audit trail of administration activity performed;

   - Periodically reviewing 'SU' or 'SUDO' logs and, for any inappropriate activities identified, conducting research/resolution activities as needed;

   - Implementing a formal process that requires database administrators to use unique user accounts when performing their daily administration responsibilities; and

   - Implementing a formal process that requires password for the 'root' user account to be changed on a periodic basis.

   These requirements should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

g. We recommend that management establish requirements related to the procedures for the timely communication of employee separations/transfers and disablement/removal of

the related user access. This process should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

h. We recommend that, upon completion of the transition to the new OCTO data center, management ensure that backup and offsite tape rotation processes implemented include, at a minimum,

- Periodically backing up the PeopleSoft and PASS applications, operating systems, databases and stored data;
- A schedule for backing up data to the offsite storage facility; and
- Periodically restoring backup media to help ensure recoverability of data.

Management should provide training to those responsible for performing these procedures and monitor to ensure adherence to the policy.

i. We recommend that management establish a formalized procedure that defines the minimum requirements that each ASO must follow when they conduct periodic application user access reviews for their respective agencies, including appropriate review and approval by the designated business owner for each agency. We recommend that this include, at a minimum, procedural and documentary requirements for:

- Mandatory review steps, follow-up procedures as a result of any inappropriate access identified, retention of the PASS user access listings reviewed by the ASOs and the modifications of user access that occurred as a result of the review;
- The consideration of users' ongoing need to retain PASS access and segregation of duties considerations; and
- A tracking mechanism to ensure that each DC Government Agency using PASS, including IT support roles, is included in the periodic application user access review.

These requirements should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

j. We recommend that management institute formal policies and procedures for PASS production job monitoring that, at a minimum, include consideration for the following:

- Implementation of monitoring processes to ensure that PASS production jobs complete in a timely manner. In consideration of limited resources, management should prioritize monitoring activities to focus on production jobs that are most critical to the business processes supported by PASS.

- Implementation of remediation procedures for resolving failed PASS production jobs in a timely manner.

- These policies and procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

k. We recommend that management remove the logical access permissions which allow the five individuals referenced in this condition above to possess the ability to migrate PASS application changes into production through the Serena Dimensions change management tool.

   Additionally, we recommend that management institute a formal periodic review process to determine whether users with the ability to migrate PASS application changes into production through Serena Dimensions require this access in order to perform their job responsibilities. In support of the recommended remediation, management should develop and formally document procedures for performing reviews that address mandatory review steps, follow-up procedures for any exceptions identified, and documentation generation and retention requirements. These procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

Management Response:

a. Management concurs with the facts of this finding.

b. Management concurs with the facts of this finding.

c. Management concurs with the facts of this finding.

d. Management concurs with the facts of this finding. The District agrees that separation between developers and administrators is an important internal control and must be maintained for the reasons stated above. However, in February/March of 2010, 2 of 4 technical resources resigned from the Procurement Application Services team. This critical loss of personnel required the District to have the remaining developer temporarily assist with administration. Without this assistance, PASS would not have been able to support the District's procurement business processes. The District has since filled these positions and restored separation between development and application administration functions.

e. Management concurs with the facts of the finding.

f. Management concurs with the facts of this finding.

   Root Access: - The Unix AIX servers are going to be decommissioned by the end of this month, January 2011, and we have already restricted the direct root logins on the scheduled build for the Linux Servers. The existing Solaris environment will undergo the same procedure by the end of Feb 2011.

   Oracle access: - The Unix Team will discuss in-depth details regarding DB access with application DBA's to restrict direct logins for all application IDs unless there are dependencies identified.

   Root password policy: - Implementation of the new process to change the passwords every 90 days is underway for the upcoming production Linux environment.

g. Management concurs with the facts of this finding.

h. Management concurs with the facts of this finding.

   - We already periodically (daily) back up all the PeopleSoft and pass servers.
   - As soon as the new datacenter is live, backup data will be replicated to that facility, and data at that facility will be replicated back to ODCI.
   - Restores will be performed any time the application owners request it.

i. Management concurs with the facts regarding the initial exclusion of two agencies in the FY2010 annual review process. Henceforth, the agency reports will be updated monthly to reflect the addition of new agencies to ensure that all agencies are included in the annual security review. In addition there will be mandatory retention of PASS user access listings before and after the PASS application access review process.

j. Management concurs with the facts of this finding. The installed version of Ariba (v8.2.2) does not have facilities to alert application administrators when a task succeeds or fails. In FY11, the District plans to implement Ariba 9, which has notification facilities. Further, the District plans to migrate Ariba Tasks and Integration Events to the UC4 platform to achieve robust job monitoring.

k. Management concurs with the facts of this finding. Action performed to remove the QA-Team and QA-Lead roles to have the ability to migrate PASS applications. Management agrees to have a formal periodic review as to whether users who have access to migrate the PASS application releases to production do require this access or not.

6. PeopleSoft

We noted the following deficiencies in the general IT controls environment supporting the PeopleSoft application:

a. During discussions with management, we were informed that two infrastructure changes were implemented into production without prior approval from the OCTO CAB. These changes resulted in temporary service outages to DC IT networks and systems.

   1) Management has indicated that these changes were not malicious in nature and that the individuals who implemented the changes were unaware of the impact of implementing the changes directly into the production IT environment. Management also noted that the changes had no impact on the integrity of processing or data of the in-scope applications.

   2) Management informed us that they plan to implement an automated change monitoring system that will be installed on production infrastructure environments for purposes of automatically capturing and reporting changes to further strengthen the infrastructure change management process.

b. Management has not updated its policy that defines the minimum password configuration requirements for DC IT systems in over six years. Further, inquiry and inspection procedures performed by the audit team indicate that the policy was not effectively communicated to responsible personnel. Specifically, we noted the following:

   1) The OCTO Password Management Policy, dated September 2004, does not require that systems be configured to automatically lock out user accounts after a predefined number of invalid log-on attempts;

   2) Inquiry of four individuals at the management level who have responsibility for implementing password security parameters for in-scope applications informed us that they were neither aware of nor able to locate the OCTO Password Management Policy document; and

   3) We noted various inconsistencies between the requirements outlined in the OCTO Password Management Policy and configurations set within the in-scope applications and their supporting databases and operating systems.

c. Management does not monitor PeopleSoft generic user accounts with elevated/super user privileges, 253 of which were created during the period October 1, 2009 to August 26, 2010, to resolve help desk and production support issues and then subsequently deleted after their use.

d. Management does not periodically review PeopleSoft application access to ensure that user access permissions remain commensurate with employee job responsibilities.

According to management, user accounts that have been assigned select PeopleSoft user access roles (i.e., Human Resources and Time and Approver) are reviewed periodically to determine whether they belong to separated employees. However, this review process does not include all PeopleSoft user access roles, and it does not include consideration of the appropriateness of users' access rights in relation to their current job responsibilities.

e. Management does not periodically review physical access to the OCTO ODC1 and ODC2 facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications.

f. The weekly script used to identify and remove PeopleSoft application access privileges for terminated users was not executed during the period of July 16, 2010 through October 18, 2010. During this timeframe, no other procedures were in place for the identification and timely removal of access rights for terminated PeopleSoft application users.

g. Management was unable to provide documented user access requests and the corresponding supervisory authorizations that were associated with the access permissions configured within the system for 23 of 40 PeopleSoft users selected for testing.

   Management has indicated that although documentation evidencing the access request and supervisory approval was unavailable for the users noted above, the corresponding access granted was nevertheless authorized in consideration of job responsibilities and the users' need-to-know.

h. During our test work over PeopleSoft application program change management, we noted the following conditions:

   1) For thirteen (13) of sixteen (16) PeopleSoft application program changes selected for testing, management was unable to provide sufficient evidence that quality assurance and/or user acceptance testing was performed prior to implementing the application changes into production.

   2) For nine (9) of sixteen (16) PeopleSoft application program changes selected for testing, management was unable to provide evidence of approval from the OCTO CAB including approval from the PeopleSoft Program Manager.

i. During our test work over physical access to the OCTO ODC1 and ODC2 facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications, we noted the following conditions:

1) Management was unable to provide the physical access request form for 1 of 3 employees selected for testing, who were granted physical access to the ODC1 and ODC2 computer rooms during fiscal year 2010; and

2) We compared a list of separated employees for the period of October 1, 2009 through September 9, 2010, to ODC1 and ODC2 physical access listings generated on September 27, 2010, and identified 4 active physical access badges belonging to individuals who no longer worked for the District.

j. During our test work over operating system administrator access and infrastructure change management for PeopleSoft and PASS, we noted the following conditions:

1) UNIX operating system administrators have the ability to and typically logon directly to the 'root' user account, which allows these individuals to perform operating system administration functions under a generic user account. Additionally, no process has been established for the review of the actions performed by this super user account.

2) Oracle database administrators currently utilize generic user accounts to perform database administration functions. No process has been established for the review of the actions performed by these generic user accounts.

3) Management does not have a formalized process in place for periodically changing the password for the 'root' operating system privileged user account or generic privileged accounts with access privileges to perform Oracle database administration functions.

k. For the period June 1, 2010 through September 30, 2010, management did not adhere to the formal process in place to rotate backup tapes for the PeopleSoft and PASS applications, operating systems, databases, and their data to an offsite storage facility.

Recommendations:

a. We recommend that management periodically communicate existing OCTO change management procedures to the individual control performers. During these communications, management should ensure that the control performers are, at a minimum, aware of the following concepts:

- Recording the nature of each change being applied;

- Evaluating the impact and risk of each change relative to objective rating criteria;

- Obtaining approval/approving (and documenting such approvals of) changes;

- Validating the functionality/system impact of each change via pre-production testing in a model environment or post-implementation confirmations; and

- Further, management should monitor control performer adherence to the procedures on a periodic basis. Management should also continue with their plans to implement an automated change monitoring system that will be installed on production infrastructure environments for purposes of capturing and reporting changes made to production systems.

b. We recommend that management develop and implement a process to review, update, and communicate the OCTO Password Management Policy to responsible individuals on a periodic basis to help ensure it remains current. We further recommend that this policy include, at a minimum, requirements for the following password configuration settings:

- Minimum password length;

- Password aging and update requirements;

- Password complexity (e.g., at least one number, letter, and special character);

- User account lockout after a predefined number invalid logon attempts; and

- Password history/reset restrictions.

In support of the recommended remediation, management should reconfigure existing password configuration settings at the application, operating system and database level, where applicable, in accordance with the revised OCTO Password Management Policy. Finally, we recommend that management monitor adherence to the policy on a periodic basis.

c. We recommend that management perform a review to determine the minimum access permissions required to perform help desk/production support activities and, based on the results of this review, establish requirements for help desk/production support access configuration to be followed on a going-forward basis. To the extent that elevated/super user privileges are required for certain support tasks, management should at a minimum, establish procedural and documentary requirements for:

- Periodically reviewing detailed audit logs associated with the use of generic user accounts and, for any inappropriate activities identified, conducting research/resolution activities as needed.

- Periodically reviewing a selection of temporary generic user account creations and tracing them back to valid requests (i.e., documented help desk tickets and/or authorized system change requests).

These requirements should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

d. By not performing a review of user accounts on a regular basis to determine whether access levels are appropriate for a given user's job responsibilities and to verify that all user accounts belong to current employees, the risk exists that:

   - Employees may have access to the system that does not correspond with their current job responsibilities and/or may present a conflict of interest. This access could allow a person to advertently or inadvertently use various functions to alter the integrity of application data in an unauthorized manner.

   - Should an active user account of a separated employee be present within the application, the separated person, with malicious intent, or another person with knowledge of this active user account, may be able to use this account to alter the integrity of application data contained in an unauthorized manner.

   By not instituting formalized user access review documentation requirements, the risk is increased that reviews will be performed and documented inconsistently and management and other interested parties will not have reliable audit trails of review activities for later investigation and/or evaluation of the individuals performing the reviews.

e. We recommend that management establish a formalized process for performing periodic reviews of physical access to the ODC1 and ODC2 Data Centers to determine whether individuals who have such access still require it to perform their job responsibilities. The process should include requirements for documenting the review, including the modification of any inappropriate physical access privileges identified during its performance.

   This process should be recorded in a formal policy or procedure document and provided to and discussed with control performers. Further, management should monitor adherence to the process on a periodic basis.

f. It was noted that the execution of the weekly termination script in the PeopleSoft production environment was resumed on October 18, 2010. We recommend that management monitor the performance of this script on a periodic basis to ensure that the application access permissions for terminated PeopleSoft users are identified and removed on a timely basis. If additional issues are identified related to the functionality of the script, management should implement alternative procedures for the timely identification and removal of terminated application users.

g. We recommend that management update the existing user access management policies and procedures for the PeopleSoft production application, where applicable. These updates should include, at a minimum, requirements for PeopleSoft access requests that include clearly articulated role assignments, as well as the corresponding supervisory authorizations.

   Management should communicate and provide training on these user access management policies and procedures to the control performers and periodically monitor to ensure adherence to the procedures.

h. We recommend that management adhere to the established PeopleSoft HCM Release Board Standard Operating Procedures, which document the required testing and approval before a change can be made to the PeopleSoft production application.
   Management should provide training on these procedures to control performers and periodically monitor to ensure adherence to the procedures.

i. We noted that management has established a formalized procedure for requesting physical access to the ODC1 and ODC2 computer rooms, which requires documented access requests and authorization from the Mainframe Security Manager. This existing procedure should be provided to and discussed with control performers within the OCTO organization. Further, management should monitor adherence to the procedure on a periodic basis.
   We recommend that management establish timeliness requirements for the communication of employee separations and disablement/removal of the related physical access rights. This process should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor adherence to the procedure on a periodic basis.

j. We recommend that management establish and implement formalized operating system and database security policies that, at a minimum, include consideration for following:

   - Configuring the UNIX operating system to prevent users from logging on directly to the 'root' user account.

   - Implementing a formal process that requires users to logon using their unique user accounts before executing the switch user (SU) or 'SUDO' command to access the 'root' account, thus establishing an audit trail of administration activity performed.

   - Periodically reviewing 'SU' or 'SUDO' logs and, for any inappropriate activities identified, conducting research/resolution activities as needed.

   - Implementing a formal process that requires database administrators to use unique user accounts when performing their daily administration responsibilities.

- Implementing a formal process that requires password for the 'root' user account to be changed on a periodic basis.

These requirements should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

k. We recommend that, upon completion of the transition to the new OCTO data center, management ensure that backup and offsite tape rotation processes implemented include, at a minimum,

- Periodically backing up the PeopleSoft and PASS applications, operating systems, databases and stored data;
- A schedule for backing up data to the offsite storage facility; and
- Periodically restoring backup media to help ensure recoverability of data.

Management should provide training to those responsible for performing these procedures and monitor to ensure adherence to the policy.

Management Response:

a. Management concurs with the facts of this finding.

b. Management concurs with the facts of this finding.

c. Management concurs with the facts of this finding. In FY 2011, the District plans to centralize PeopleSoft security functions and establish processes to create and deactivate these user accounts when needed. Processes will also be established that minimize the use of these accounts.

d. Management concurs with the facts of this finding. PeopleSoft security is not currently centralized, and no one agency or group currently holds this responsibility. In FY 2011, the District will establish a centralized PeopleSoft security team responsible for completing these application access reviews.

e. Management concurs with the facts of this finding.

f. Management concurs with the facts of this finding. As noted above, the weekly termination script was repaired on October 18, 2010 and the backlog of terminations was cleared on or about that date. The District made reasonable efforts to complete manual processing of the terminations when the problem was found, but the available resources

allocated to processing the terminations manually were insufficient to complete the unusually large number of terminations that occurred during the period.

g. Management concurs with the facts of this finding. PeopleSoft security is not currently centralized, and no one agency or group currently holds this responsibility. In FY 2011, the District will establish a centralized PeopleSoft security team responsible for creating documentation describing these access authorization guidelines.

h. Management concurs with the facts of this finding. The District will ensure that all PeopleSoft changes adhere to the established Release Board Standard Operating Procedures or other configuration management guide if written. The District has begun implementation of the Agile software development methodology within the HR Application Services team, which will bring additional structure to the PeopleSoft migration path and ensure that all parties that must approve changes to PeopleSoft are notified timely and with the proper documentation.

i. Management concurs with the facts of the finding.

j. Management concurs with the facts of this finding.

Root Access: - The Unix AIX servers are going to be decommissioned by the end of this month, January 2011, and we have already restricted the direct root logins on the scheduled build for the Linux Servers. The existing Solaris environment will undergo the same procedure by the end of Feb 2011.

Oracle access: - The Unix Team will discuss in-depth details regarding DB access with application DBA's to restrict direct logins for all application IDs unless there are dependencies identified.

Root password policy: - Implementation of the new process to change the passwords every 90 days is underway for the upcoming production Linux environment.

j. Management concurs with the facts of this finding. See Management's response below:

1) We already periodically (daily) back up all the PeopleSoft and pass servers.

2) As soon as the new datacenter is live, backup data will be replicated to that facility, and data at that facility will be replicated back to ODCI.

3) Restores will be performed any time the application owners request it.

7. SOAR

We noted the following deficiencies in the general IT controls environment supporting the SOAR application:

a. During discussions with management, we were informed that two infrastructure changes were implemented into production without prior approval from the OCTO CAB. These changes resulted in temporary service outages to DC IT networks and systems.

   Management has indicated that these changes were not malicious in nature and that the individuals who implemented the changes were unaware of the impact of implementing the changes directly into the production IT environment. Management also noted that the changes had no impact on the integrity of processing or data of the in-scope applications.

   Management informed us that they plan to implement an automated change monitoring system that will be installed on production infrastructure environments for purposes of automatically capturing and reporting changes to further strengthen the infrastructure change management process.

b. Management has not updated its policy that defines the minimum password configuration requirements for DC IT systems in over six years. Further, inquiry and inspection procedures performed by the audit team indicate that the policy was not effectively communicated to responsible personnel. Specifically, we noted the following:

   1) The OCTO Password Management Policy, dated September 2004, does not require that systems be configured to automatically lock out user accounts after a predefined number of invalid log-on attempts.

   2) Inquiry of four individuals at the management level who have responsibility for implementing password security parameters for in-scope applications informed us that they were neither aware of nor able to locate the OCTO Password Management Policy document.

   3) We noted various inconsistencies between the requirements outlined in the OCTO Password Management Policy and configurations set within the in-scope applications and their supporting databases and operating systems.

c. Management does not periodically review physical access to the OCTO ODC1and ODC2 facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications.

d. One of the three users with the ability to add, disable, or modify bank information within the SOAR application, no longer required this access to perform their job responsibilities.

Management has indicated that for the user noted above, the SOAR application access permissions were authorized on a temporary basis to assist with a bank reconciliation project. However, documentation evidencing the access request and supervisory approval could not be provided.

e. We compared a list of separated employees for the period of October 1, 2009 through September 9, 2010 and a SOAR access list generated on August 30, 2010, and identified 120 active accounts belonging to individuals who no longer worked for the District. We then inspected the mainframe access listing generated on August 18, 2010, and determined that of the 120 individuals noted above:

    1) 30 users did not have associated mainframe access, and therefore these accounts could not be used to access the SOAR application.

    2) 90 users still had associated mainframe access, of which 75 user accounts were revoked or inactivated by the mainframe security software due to 90 consecutive days of inactivity. Of the remaining 15 accounts, one user account had a 'last logon' date after their separation date.

f. We noted deficiencies in the design of management's existing process to periodically review SOAR application user access permissions. Specifically, the following was noted relating to the adequacy of the periodic review process:

    1) Two of seven DC Government Agencies selected for testing were not included in the FY2010 annual review process.

    2) SOAR application user access listings distributed to each ASO for review did not include all of the application access rights each user was potentially assigned. For example, the specific SOAR screens each user can access, including the associated update capabilities, were not included in the packages provided to ASOs.

    3) Of three ASOs interviewed, two stated that they did not document the results of their reviews. One ASO stated that he did not look up individual access permissions within SOAR.

g. Management has not instituted a formalized process to periodically review access to update and install mainframe database system software. As a result, we noted the following instances in which such access was not assigned based on least privilege and need-to-know security concepts:

    1) Three of 15 users with the ability to update the mainframe datasets for DB2 database system software supporting the SOAR and TAS applications did not require such access to perform their job responsibilities.

2) 55 of 57 users with the ability to update the mainframe datasets for ADABAS database system software supporting the ACEDS application did not require such access to perform their job responsibilities.

h. During our test work over physical access to the OCTO ODC1 and ODC2 facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications, we noted the following conditions:

1) Management was unable to provide the physical access request form for 1 of 3 employees selected for testing, who were granted physical access to the ODC1 and ODC2 computer rooms during fiscal year 2010.

2) We compared a list of separated employees for the period of October 1, 2009 through September 9, 2010, to ODC1 and ODC2 physical access listings generated on September 27, 2010, and identified 4 active physical access badges belonging to individuals who no longer worked for the District.

Recommendations:

a. We recommend that management periodically communicate existing OCTO change management procedures to the individual control performers. During these communications, management should ensure that the control performers are, at a minimum, aware of the following concepts:

- Recording the nature of each change being applied;
- Evaluating the impact and risk of each change relative to objective rating criteria;
- Obtaining approval/approving (and documenting such approvals of) changes; and
- Validating the functionality/system impact of each change via pre-production testing in a model environment or post-implementation confirmations.

Further, management should monitor control performer adherence to the procedures on a periodic basis. Management should also continue with their plans to implement an automated change monitoring system that will be installed on production infrastructure environments for purposes of capturing and reporting changes made to production systems.

b. We recommend that management develop and implement a process to review, update, and communicate the OCTO Password Management Policy to responsible individuals on a periodic basis to help ensure it remains current. We further recommend that this

policy include, at a minimum, requirements for the following password configuration settings:

- Minimum password length;
- Password aging and update requirements;
- Password complexity (e.g., at least one number, letter, and special character);
- User account lockout after a predefined number invalid logon attempts; and
- Password history/reset restrictions.

In support of the recommended remediation, management should reconfigure existing password configuration settings at the application, operating system and database level, where applicable, in accordance with the revised OCTO Password Management Policy. Finally, we recommend that management monitor adherence to the policy on a periodic basis.

c. We recommend that management establish a formalized process for performing periodic reviews of physical access to the ODC1 and ODC2 Data Centers to determine whether individuals who have such access still require it to perform their job responsibilities. The process should include requirements for documenting the review, including the modification of any inappropriate physical access privileges identified during its performance.

   This process should be recorded in a formal policy or procedure document and provided to and discussed with control performers. Further, management should monitor adherence to the process on a periodic basis.

d. We noted that the SOAR user access permissions for the individual referenced in the condition above were removed as of September 28, 2010. We recommend that management institute a formalized process for tracking SOAR user access permissions that are assigned on a temporary basis to ensure that the access permissions are removed at the conclusion of the time period for which they were authorized. In support of the recommended remediation, management should develop and formally document procedures for performing periodic user access reviews that address mandatory review steps, follow-up procedures for any exceptions identified, and documentation generation and retention requirements. These procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

e. We recommend that management establish timeliness requirements for the communication of employee separations/transfers and disablement/removal of the related user access. This process should be documented in a formalized

policy/procedure that is provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

f. We recommend that management establish a formalized procedure that defines the minimum requirements that each ASO must follow when they conduct periodic application user access reviews for their respective agencies, including appropriate review and approval by the designated business owner for each agency. We recommend that this include, at a minimum, procedural and documentary requirements for:

- Mandatory review steps, follow-up procedures as a result of inappropriate access identified, and documentation generation and retention requirements;
- The consideration of users' ongoing need to retain SOAR access and segregation of duties considerations; and
- A tracking mechanism to ensure that each DC Government Agency using SOAR is included in the periodic application user access review.

These requirements should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

g. We recommend that management remove the logical access permissions which allow the individuals referenced in the condition above to update and install mainframe database system software. Management should also perform a review of all individuals with this privileged access and ensure that each individual requires this access to perform his or her job responsibilities.

Additionally, we recommend that management institute a formalized, periodic review process to determine whether users with the ability to update and install mainframe database system software require this access in order to perform their job responsibilities. In support of the recommended remediation, management should develop and formally document procedures for performing reviews that address mandatory review steps, follow-up procedures for any exceptions identified, and documentation generation and retention requirements. These procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

h. We noted that management has established a formalized procedure for requesting physical access to the ODC1 and ODC2 computer rooms, which requires documented access requests and authorization from the Mainframe Security Manager. This existing procedure should be provided to and discussed with control performers within the OCTO organization. Further, management should monitor adherence to the procedure on a periodic basis.

We recommend that management establish timeliness requirements for the communication of employee separations and disablement/removal of the related physical access rights. This process should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor adherence to the procedure on a periodic basis.

Management Response:

a. Management concurs with the facts of this finding.

b. Management concurs with the facts of this finding.

c. Management concurs with the facts of this finding.

d. Management concurs with the facts of this finding. Management does not have a process in place for the identification and removal/disablement of temporary user access permissions in SOAR, once access is no longer required. This finding is in regard to the opening and closing of Bank Identification Number (BIDs) in SOAR. This access is limited to OFT's Banking and Operations group.

e. Management concurs with the facts of this finding. A review of the payroll activity for the 9 individuals listed as terminated and determined to have accessed the District Financial System, revealed that 8 of these individuals were terminated in their primary or secondary job classifications but remained employed by the District of Columbia in another classification. There was only one employee that was terminated in the Payroll System but was still active in SOAR. SOAR Security Access is always terminated immediately on notification from Agency Personnel or the Agency Human Resources. To further enforce compliance with the exit policy, we will continue to discuss adherence with the District of Columbia Human Resource Agency and coordinate a more effective process to terminating departing associates from all related user access.

f. Management concurs with the facts of this finding. Agency reports will be updated monthly to reflect the addition of new agencies so that all agencies are included in the annual review process.

   Agency security officers have been provided access to the SOAR standard security reports (DAFR 7240 and DAFR 7270). These readily available reports contain all of the security data for each user including profile and screen level access rights.

   A standardized reporting form will be provided to each ASO. The form will guide them through a consistent and thorough process requiring them to review and report on essential elements in their agency's SOAR security profiles. The ASO will be required

to complete and submit the form for annual assessment and corrective action if necessary at the central level.

Periodic agency visits will be carried out to ensure adherence to the SOAR access policies and procedures. These site visits are to confirm that user financial application access is authorized and valid.

g. Management concurs with the facts of this finding.

h. Management concurs with the facts of the finding.

8. TACIS

We noted the following deficiencies in the general IT controls environment supporting the TACIS application:

a. Management did not perform periodic user access reviews to determine whether TACIS access is commensurate with employee job responsibilities for any of the departmental units that use TACIS with the exception of the Office of Internal Affairs (OIA).

   According to management, a monthly review of TACIS user access is performed for OIA employee accounts; however, this review is not documented consistently. Specifically, for two of three months selected for testing, management was unable to provide evidence of the user access review.

b. Contractor-provided developers were granted administrative levels of access to TACIS for the express purpose of providing on-going support of the performance and availability of TACIS, including the ability to migrate changed TACIS program code into production without any preventative impedance provided by other change mitigating controls placed into operation by management.

   Specifically, both (two) developers had administrative access to the production version of the TACIS application. The administrative access level in question – 'ALLACCES' – provides users to which it has been assigned the ability to perform all TACIS business functions; create and delete user accounts and add and modify application privileges associated with user accounts.

   Further, one of the two developers referenced above has knowledge of the 'root' password for the HP-UX operating system; this access level provides these users administrative privileges to both the operating system and the database layers supporting TACIS.

c. Management manually logs program changes as well as the dates that program change testing and approval occurred on a Microsoft Excel spreadsheet; however, there is no additional documentary evidence of program change testing and approval prior to the migration of changes to production.

d. Management has not designated its backup and tape rotation processes of the TACIS application, operating system, and database and its data with sufficient priority. As a result, backup tapes were not rotated offsite for five of eight weeks selected for testing.

e. Twenty five (25) TACIS accounts whose access was created or modified in fiscal year 2010 were selected for testwork; for 2 of 25 user accounts selected for testing, management was unable to provide documentation to support the supervisory approvals.

   Management has indicated that although documentation evidencing the supervisory approval was unavailable for the two users noted above, the corresponding access

granted was nevertheless authorized in consideration of job responsibilities and the users' need-to-know.

f. During our test work over physical access to the Metropolitan Police Department (MPD) data center, which hosts the TACIS application, we noted the following conditions:

   1) Management does not perform a periodic review of physical access to the MPD data center to determine whether individuals' physical access assignments remain commensurate with employee job responsibilities.

   2) For both (two) employees granted access to the MPD data center in fiscal year 2010, management was unable to provide e-mails documenting the access request and supervisory approvals. Management has indicated that although documentation evidencing the access request and supervisory approval was unavailable for the two employees noted above, the corresponding access granted was nevertheless authorized in consideration of job responsibilities and the employees' need-to-know.

   3) We compared a list of separated employees for the period of October 1, 2009 through September 9, 2010 to a MPD data center physical access listing generated on September 27, 2010, and identified three (3) physical access badges belonging to individuals who no longer worked for the District. Management has indicated that the physical access badges for two (2) of the separated employees noted were set to 'inactive' status; however, documentation could not be provided to support the actions performed.

g. Management did not formally document and track to resolution the TACIS application incidents reported to the IT Help Desk during fiscal year 2010. Management has indicated that they are establishing incident management procedures that include the recording of TACIS application issues into the Remedy Help Desk system; however these procedures were not in place during fiscal year 2010.

Recommendations:

a. We recommend that management institute a formalized, periodic review process to determine whether TACIS user access remains commensurate with employee job responsibilities for all of the departmental units that use TACIS.

   In addition, management should develop and formally document procedures for performing reviews that address mandatory review steps, follow up procedures for any exceptions identified, and documentation generation and retention requirements. Management should provide training on this policy to those responsible for performing these procedures and monitor to ensure adherence to the policy.

b. We recommend that management develop and implement change management processes and controls that establish one or more of the following:

- Organizational and logical segregation of program development roles from production system administration roles among different individuals; and

- Implementation of one or more independently operated monitoring controls over the activities of the developers (and other individuals) with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.

c. We recommend that management develop and implement a formalized change management policy and procedures for the TACIS production application, operating system, and database. We recommend that these include, at a minimum, procedural and documentary requirements for:

- The completion of a formal change request form;

- Proper authorization of the change prior to initiation of the work;

- The preparation of test plans and results to determine whether the change is operating as required; and

- Formal approval of the change prior to migration to production.

Management should provide training on this policy to those responsible for performing these procedures and periodically monitor to ensure adherence to the policy.

d. We recommend that management develop and formally document backup and tape rotation policy and procedures for the TACIS application, operating system, database and stored data. We recommend that these include, at a minimum, procedural and documentary requirements for:

- Periodically backing up the TACIS application, operating system, database and stored data to backup tape media;

- Periodically taking inventory of backup tape media;

- A schedule for rotating backup tape media to an offsite facility and for the duration of storage at the facility;

- Maintaining signed logs of backup tape media rotations to an offsite facility; and

- Periodically restoring backup tape media to help ensure recoverability of data.

Management should provide training on this policy to those responsible for performing these procedures and monitor to ensure adherence to the policy.

e. We recommend that management develop and formally document the access management policy and procedures for the TACIS production application. We recommend that these include, at a minimum, procedural and documentary requirements for:

- Requesting, approving and configuring user accounts; and
- Periodic reviews of user access performed in consideration of users' ongoing need to retain TACIS access and segregation of duties considerations, and the configuration of any updates required as a result of inappropriate access identified during the review process.

Management should provide training on this policy to those responsible for performing these procedures and monitor to ensure adherence to this policy.

f. We recommend that management develop and formally document the physical access management policy and procedures for the MPD Data Center. We recommend that these include, at a minimum, procedural and documentary requirements for:

- Requesting, approving and configuring physical access to the MPD Data Center;
- Timely disablement/removal of physical access rights during instances of employee separations; and
- Performing periodic reviews of access in consideration of users' ongoing need to retain physical access to the MPD Data Center, and the modification of any updates required as a result of inappropriate access identified during the review process.

These procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

g. We noted that management is establishing incident management procedures that include the recording of TACIS application issues into the Remedy Help Desk system. As management develops these procedures, we recommend that, at a minimum, these procedures include consideration for the following:

- Formally documenting and tracking TACIS application incidents that are reported to the help desk;

- Establishing a formalized service level agreement (SLA) that addresses the resolution of TACIS application incidents reported to the IT help desk, within a defined time period that is acceptable to TACIS application owners; and

- Monitoring TACIS application incidents reported to the IT help desk to ensure they are remediated within the timeframes outlined in the SLA.

Management should provide training on these incident management procedures to those responsible for performing these procedures and monitor to ensure adherence to the policy.

Management Response:

a. Management concurs with the facts of this finding. We will develop standard operating procedures (SOP) for TACIS user access to include implementation of quarterly review of user access commensurate with the employee's job responsibilities, obtain the appropriate authorization, and maintain documentation to support user access in accordance with the District's records retention period.

   Management will ensure employees are trained on the SOP and will monitor adherence to the same.

b. Management concurs with the facts of this finding. We will coordinate with the MPD IT Division to develop and implement change management policy and procedures to incorporate segregation of duties for program development roles from production system administration roles, and monitoring controls.

c. Management concurs with the facts of this finding. We will coordinate with the MPD IT Division to develop and implement formal change management policy and procedures for the TACIS production application, operating system and database. The policies and procedures will incorporate training and policy monitoring.

d. Management concurs with the facts of this finding. We will coordinate efforts with the MPD IT Division to develop and properly document the backup and tape rotation policy and procedures for the TACIS application, operating system, database and stored data in accordance with industry standards on a phase basis.

e. Management concurs with the facts of this finding. We will develop SOPs for TACIS user access to include implementation of quarterly review of user access commensurate with the employee's job responsibilities, obtain the appropriate authorization, and maintain documentation to support user access in accordance with the District's records retention period.

   Management will ensure employees are trained on the SOP and will monitor adherence to the same.

f. Management concurs with the facts of this finding. The MPD IT Division is in the process of developing policies and procedures to document guidelines for the physical access of the Data Center, which will incorporate physical access rights, approval process for access, training of control performers, and performance of periodic review of user access.

g. Management concurs with the facts of this finding. We will coordinate the MPD IT Division to establish and implement policies and procedures for the TACIS incident management process to track application incidents to include remediation timeframes, training for Help Desk staff, and policy monitoring.

9. TAS

We noted the following deficiencies in the general IT controls environment supporting the TAS application:

a. During discussions with management, we were informed that two infrastructure changes were implemented into production without prior approval from the OCTO CAB. These changes resulted in temporary service outages to DC IT networks and systems.

   Management has indicated that these changes were not malicious in nature and that the individuals who implemented the changes were unaware of the impact of implementing the changes directly into the production IT environment. Management also noted that the changes had no impact on the integrity of processing or data of the in-scope applications.

   Management informed us that they plan to implement an automated change monitoring system that will be installed on production infrastructure environments for purposes of automatically capturing and reporting changes to further strengthen the infrastructure change management process.

b. Management has not updated its policy that defines the minimum password configuration requirements for IT systems in over six years. Further, inquiry and inspection procedures performed by the audit team indicate that the policy was not effectively communicated to responsible personnel. Specifically, we noted the following:

   1) The OCTO Password Management Policy, dated September 2004, does not require that systems be configured to automatically lock out user accounts after a predefined number of invalid log-on attempts;

   2) Inquiry of four individuals at the management level who have responsibility for implementing password security parameters for in-scope applications informed us that they were neither aware of nor able to locate the OCTO Password Management Policy document; and

   3) We noted various inconsistencies between the requirements outlined in the OCTO Password Management Policy and configurations set within the in-scope applications and their supporting databases and operating systems.

c. Office of Tax and Revenue (OTR) management has established a formalized process which requires a quarterly review to determine whether TAS application user access remains commensurate with employee job responsibilities. However, the review for the 2nd quarter of the calendar year was not completed until mid-September 2010, two-and-a-half months after the review was supposed to be performed. Additionally, users that have been granted security administration privileges to the TAS application via the Administration Security Administrator (ASA) roles are not reviewed as a part of this quarterly process.

d. Management does not periodically review physical access to the OCTO ODC1 and ODC2 facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications.

e. There is no requirement for an individual's manager or director within OTR to authorize the Integrated Tax System (ITS) profile request form, which is used to request access permissions within the TAS application. Currently, authorization of the ITS profile request form can be provided by the OTR agency security officer responsible for configuring the requested access within the application.

f. We noted the following exceptions when we conducted procedures to determine whether TAS program changes were tested before they were implemented in the production environment:

    1) Management was unable to provide documentation to support the completion of testing activities for 2 of 40 application changes selected for testing.

    2) Quality Assurance (QA) testing and the approval for migration to production was performed by the same individual for 2 of 40 application changes selected for testing. Although it is normally required, the individual who approved the changes was not an end user.

g. During our test work over access to migrate TAS application changes to production, we noted the following condition:

    1) 2 of 18 users with the ability to migrate TAS application changes into production did not require this access to perform their job responsibilities.

    We inspected the last login dates of the mainframe accounts belonging to the two users described above and determined that their last logon dates were April 1, 2009, and April 14, 2009, respectively.

h. Management has not instituted a formalized process to periodically review access to update and install mainframe database system software. As a result, we noted the following instances in which such access was not assigned based on least privilege and need-to-know security concepts:

    1) Three of 15 users with the ability to update the mainframe datasets for DB2 database system software supporting the SOAR and TAS applications did not require such access to perform their job responsibilities.

    2) 55 of 57 users with the ability to update the mainframe datasets for ADABAS database system software supporting the ACEDS application did not require such access to perform their job responsibilities.

i. Management was unable to provide documentation to support the access permissions configured within the system and the corresponding supervisory authorization for 1 of 5 mainframe users selected for testing.

j. Although management has established a service-level agreement (SLA) for "Severity level 1" incidents, which include basic hardware diagnostics and password resets, that are submitted to the OCFO help desk, there is no equivalent SLA in place that specifies the time by which TAS application issues are to be remediated by the Tax Systems Group (TSG). Additionally, there is no formal monitoring process in place to ensure that TAS application issues reported to the OCFO help desk are resolved.

k. During our test work over physical access to the OCTO ODC1 and ODC2 facilities, which host the SOAR, TAS, PeopleSoft, PASS, ACEDS, DOCS, and DUTAS applications, we noted the following conditions:

   1) Management was unable to provide the physical access request form for 1 of 3 employees selected for testing, who were granted physical access to the ODC1 and ODC2 computer rooms during fiscal year 2010.

   2) We compared a list of separated employees for the period of October 1, 2009 through September 9, 2010, to ODC1 and ODC2 physical access listings generated on September 27, 2010, and identified 4 active physical access badges belonging to individuals who no longer worked for the District.

Recommendations:

a. We recommend that management periodically communicate existing OCTO change management procedures to the individual control performers. During these communications, management should ensure that the control performers are, at a minimum, aware of the following concepts:

   - Recording the nature of each change being applied;
   - Evaluating the impact and risk of each change relative to objective rating criteria;
   - Obtaining approval/approving (and documenting such approvals of) changes; and
   - Validating the functionality/system impact of each change via pre-production testing in a model environment or post-implementation confirmations.

   Further, management should monitor control performer adherence to the procedures on a periodic basis. Management should also continue with their plans to implement an

automated change monitoring system that will be installed on production infrastructure environments for purposes of capturing and reporting changes made to production systems.

b. We recommend that management develop and implement a process to review, update, and communicate the OCTO Password Management Policy to responsible individuals on a periodic basis to help ensure it remains current. We further recommend that this policy include, at a minimum, requirements for the following password configuration settings:

   - Minimum password length;
   - Password aging and update requirements;
   - Password complexity (e.g., at least one number, letter, and special character);
   - User account lockout after a predefined number invalid logon attempts; and
   - Password history/reset restrictions.

   In support of the recommended remediation, management should reconfigure existing password configuration settings at the application, operating system and database level, where applicable, in accordance with the revised OCTO Password Management Policy. Finally, we recommend that management monitor adherence to the policy on a periodic basis.

c. We recommend that management take measures to ensure that subsequent quarterly TAS user access reviews are completed in a timely and comprehensive manner. Such measures may include, but are not limited to:

   - Documenting policies and procedures that outline the specific time requirements for completing user access reviews, including the modification of application privileges to remove any inappropriate access levels identified during reviews, and assign accountability for the performance of these reviews. Policies and procedures should be communicated to, and discussed with, control performers.
   - Monitoring the control performer's adherence to the policies and procedure on a periodic basis.
   - Ensuring that all user accounts and their assigned user classes are included within the review performed.

d. We recommend that management establish a formalized process for performing periodic reviews of physical access to the ODC1 and ODC2 Data Centers to determine whether individuals who have such access still require it to perform their job responsibilities.

The process should include requirements for documenting the review, including the modification of any inappropriate physical access privileges identified during its performance.

This process should be recorded in a formal policy or procedure document and provided to and discussed with control performers. Further, management should monitor adherence to the process on a periodic basis.

e. We recommend that management update existing user access processes to require that only managers or directors can authorize access requests for individuals they supervise. The existing TAS security procedure document should be updated to reflect this requirement.

f. We recommend that management update existing application change management policies and procedures to require that documentation of testing results is completed prior to migrating application changes into production. These requirements should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor adherence to the procedure on a periodic basis.

g. We recommend that management remove the logical access permissions which allow the two individuals referenced in this condition above to possess the ability to migrate TAS application changes into production. Management should also perform a review of all individuals with this privileged access and ensure that each individual requires this access to perform his or her job responsibilities.

   Additionally, we recommend that management institute a formalized, periodic review process to determine whether users with the ability to migrate TAS application changes into production require this access in order to perform their job responsibilities. In support of the recommended remediation, management should develop and formally document procedures for performing reviews that address mandatory review steps, follow-up procedures for any exceptions identified, and documentation generation and retention requirements. These procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

h. We recommend that management remove the logical access permissions which allow the individuals referenced in the condition above to update and install mainframe database system software. Management should also perform a review of all individuals with this privileged access and ensure that each individual requires this access to perform his or her job responsibilities.

   Additionally, we recommend that management institute a formalized, periodic review process to determine whether users with the ability to update and install mainframe database system software require this access in order to perform their job

responsibilities. In support of the recommended remediation, management should develop and formally document procedures for performing reviews that address mandatory review steps, follow-up procedures for any exceptions identified, and documentation generation and retention requirements. These procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

i. We noted that management has established a formalized procedure for mainframe user access management, which requires documented access requests from applicable ASOs. This existing procedure should be provided to and discussed with control performers. Further, management should monitor adherence to the procedure on a periodic basis.

j. We recommend that management institute formal policies and procedures to monitor open TAS application incidents reported to the OCFO Help Desk that are forwarded to the TSG and to ensure that they are remediated within a defined time period that is acceptable to TAS application owners.

   These policies/procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

k. We noted that management has established a formalized procedure for requesting physical access to the ODC1 and ODC2 computer rooms, which requires documented access requests and authorization from the Mainframe Security Manager. This existing procedure should be provided to and discussed with control performers within the OCTO organization. Further, management should monitor adherence to the procedure on a periodic basis.

   We recommend that management establish timeliness requirements for the communication of employee separations and disablement/removal of the related physical access rights. This process should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor adherence to the procedure on a periodic basis.

Management Response:

a. Management concurs with the facts of this finding.

b. Management concurs with the facts of this finding.

c. Management concurs with the facts of this finding. The liability was booked in compliance with OCP regulations and FY 2009 closing instructions provided by OFOS. Costs were incurred by the DMV in August, 2009, and encumbered in PO276964. The DMV was unable to modify the purchase order for full payments prior to the closing

submission date for FY 2009. Due to an oversight, the payment was not submitted to OFOS for approval.

d. Management concurs with the facts of this finding.

e. Management concurs with the facts of this finding. The current TAS user access authorization policy and process, as established by OTR and OCIO does not mandate that a user's supervisor or manager be required to provide authorization for user access. This authorization has been delegated, by the Agency Director, to the agency security officer role.

   OCIO does agree that adding a supervisory authorization will add another layer of control over the user authorization process and will work with OTR to modify the current policy and process to require this additional approval step.

f. Management concurs with the facts of this finding. OCIO management concurs with this finding and is pleased to inform that this issue has since been resolved. The application change management workflow has been updated to ensure that the same user can no longer provide QA acceptance and production approval of any change. Furthermore, the process of relying on business end user for QA activities has been discontinued. All QA operations are being performed by the OCIO QA staff, independent of the end user or developers.

g. Management concurs with the facts of this finding. OCIO concurs with this finding. This issue is related to the role of Super ASAs as currently outlined in the system security profiles for TAS. OCIO agrees that Super ASAs do not require the ability to migrate code changes into production. OCCIO will analyze and change the TAS security profiles to remove the production migration capability from the super ASA profile.

h. Management concurs with the facts of this finding.

i. Management concurs with the facts of this finding.

j. Management concurs with the facts of this finding. Help desk tickets related to TAS are not always easily resolved and often represent requests for service rather than system breaks. Many of these issues require a formalized SDLC approach which includes analysis, design, development and testing. OCIO management currently meets with TAS application owners' senior management on a bi-weekly basis to prioritize all TAS development and maintenance. In this meeting the administration directors discuss all TAS owner issues and decide which TAS issues are to be resolved by the OCIO and in what order. This includes all system issues including user requests / held desk ticket open issues. A formalized reporting process combined with a rigorous SDLC methodology is then utilized to track the implementation of the prioritized enhancements and fixes to the system and to keep system owners informed and a separate help desk

incident management process is followed for minor incidents outside of the SDLC process.

To specifically ensure the critical help desk ticket open issues are discussed in the bi-weekly meetings or via the help desk issue management process, the OCIO management will institute a formalized reporting mechanism to bring critical help desk ticket open issues to the bi-weekly prioritization meeting for discussion and prioritization or address non-critical issues with the help desk incident management process. The TAS application owners and Help Desk managers will then prioritize these help desk ticket open issues in the context of all other user request/issues. These procedures will be documented and put in place by May 31, 2011.

k. Management concurs with the facts of the finding.

Section II – Non-EDP Comments

During our audit of the fiscal year 2010 basic financial statements, we have noted deficiencies within various accounting and financial reporting processes. We have broken down these deficiencies by process below along with both our recommendation for remediating the deficiency as well management's response.

1. Fixed Assets, including Leases

We noted the following deficiencies in the fixed assets process, including leases:

a. During our observation of the fixed asset inventory count, we noted the following:

1) The District employed a service organization for completing the fiscal year 2010 inventory count. However, we noted that the District did not adequately monitor the performance of the service provider to ensure the physical count was performed appropriately.
2) Physical count procedures were not adequately planned prior to the performance of the physical count. The District was unable to provide a copy of the inventory instructions, nor was a physical observation schedule provided to the service organization or District agencies that outlined the planned inventory observation locations and dates.

During the UMC inventory count observation, we noted the following:

1) Inventory cutoff was not established prior to the physical count; we observed inventory items being moved within and between the storerooms.

2) For fifty-two (52) items tested during inventory re-counts, twenty (20) items did not agree with the inventory count recorded.

3) We identified instances where the physical count was recorded inaccurately (e.g. 6 items were recorded on the count sheets, when 60 items should have been recorded).

4) We observed entire boxes of product that were counted and recorded as individual units when the count should have recorded the number of individual units within each box.

5) While performing floor-to-list counts, we observed items that should have been counted that were not included in the physical count and were subsequently not recorded on the inventory count sheets.

During the MPD inventory count observation, we noted the following:

1) Ten (10) of ten (10) items selected from the Fixed Asset System (FAS) Inventory listing could not be located at MPD.

2) Items that were originally located at the MPD as documented on the FAS Inventory Listing had been moved to a different location; however, the accounting department was not notified when these items were moved.

3) For 8 out of 10 items selected at MPD to trace from the inventory floor back to the FAS Inventory Listing, could not be agreed to the FAS report. We also observed that property numbers attached to the inventory items selected could not be matched to the FAS report.

b. During performance of our test work over infrastructure assets transfers from construction in progress, we identified the following:

1) Management was unable to validate he estimated average project life cycle employed by the Department of Transportation. The capitalization methodology was established in FY 2002, based on the assumption that infrastructure projects average 24 months in duration. Annually, amounts expended for new infrastructure projects are recorded as construction-in-process. The balance is moved to fixed assets at the end of the second fiscal year to match the end of the 24 month cycle for average project cycle.

c. During performance of our testwork over real property exchanges, we identified the following:

1) We requested documentation supporting the valuation of the Reservation 13 and Old Naval Hospital property that the District obtained through property exchanges with the Federal government. We determined that the District had no formalized policy to obtain an independent, third party valuation for highly complex or non-routine fixed asset transactions to validate the District's own fair valuation calculation. We also identified that the St. Elizabeth's property transferred out of the District was not included in disposals for FY 2010 resulting in a known difference of $5.7M.

Recommendations:

a. We recommend the District enhance current fixed asset policies to ensure procedures are implemented to include, but are not limited to the following:

1) Proper identification, tracking and recording of fixed assets to ensure that each inventory item should be tagged with the corresponding identification number and held at the location number on record. Any changes such as relocation or disposal should be updated in the record.

2) Each inventory record should include an asset identification number, a location number, asset description, cost, fund information, and acquisition date.

3) A physical count should be performed at least bi-annually to ensure the inventory records and the financial statement balances are complete and accurate.

District personnel responsible for performance of these procedures should be training on the enhanced policies. In addition, the District should implement a monitoring process to ensure adherence to these policies.

b. We recommend that the Department of Transportation enhance its fixed asset policies and procedures to ensure that infrastructure project milestone data is maintained in a consistent, readily accessible manner.

   In addition, we recommend that the District enhance its fixed asset policies and procedures to include clearly stated guidelines for capitalization of infrastructure assets. This enhancement should include assumptions made for use of estimates employed, and a stated period for which estimates are considered valid, after which time the assumptions and estimates will be reviewed and updated as necessary.

c. We recommend that the OFOS enhance its fixed asset policies and procedures. These policies should include but are not limited to the following:

   1) Proper documentation is maintained for each fixed asset transaction, including asset valuation.

   2) Policies which require use of third party specialists for non-routine exchange transactions which require calculations involving the fair value measurements.

   3) Procedures for proper management level review involving significant and non-routine transactions.

Management Response:

a. Management concurs with the facts of this finding. For future inventory counts, OFOS will provide the agencies with proper procedures in order to determine an accurate count and will monitor the performance of the selected vendor in order to ensure agreement with the final count tallied.

b. Management concurs with the facts of this finding. We agree that KPMG was unable to verity the validity of the estimated project life cycle and with KPMG's recommendation that the District Department of Transportation ensure that infrastructure project milestones be maintained in a consistent readily accessible manner.

Steps will be taken to improve collection and recordation of infrastructure project milestones as part of the currently on-going general ledger replacement being undertaken by the District. The District is currently updating all policies and procedures. Changes in assumptions and estimates employed, and stated period for which estimates are considered valid will be included based on discussions in FY 2011.

c. Management concurs with the auditor's recommendation with respect to point one and three. Management does not agree with the recommendation of point two specifically calling for the use of an independent third party for measurements of fair value. Per DC law Sec. 10-1011(a)(1)(G), an inventory of real property under the executive control of the mayor shall include "the current assessed value of the property and any improvements..." Management believes that since the Office of the Chief Assessor is responsible for determining the assessed value (based on FMV) of real property in the District, that responsibility also extends to any fair market valuation needed and that such value determined by the Chief Assessor or his representatives substantiates what is set forth in the law and therefore no additional outside party is needed.

KPMG response:
We have read the District's response and consider our finding to be appropriate as presented. We believe that for a real property valuation of this size (~$250M), an independent third party appraisal is appropriate.

2. Debt
We identified the following deficiencies in the debt process:

a. During our testwork over derivative instruments held by the District, we identified that an inappropriate method used to determine hedge effectiveness was utilized by the District for 1 of the five derivatives held. The District has been relying on a third party service provider to determine hedge effectiveness and valuation. Additionally, the methods employed by the District's third party service provider results in the District not determining the hedge effectiveness appropriately under newly implemented GASB Statement No. 53.

Recommendation:

a. We recommend that the District:

   1) Adequately review third party service provider work regarding valuation and determination of hedge effectiveness.

Management Response:

a. Management concurs with the facts of this finding. Management concurs that for 1 out of its 5 derivative instruments, the appropriate method was not used to test hedge effectiveness in accordance with the new GASB 53 requirements.

   Management does not concur that the Condition noted above was brought about due to ineffective monitoring of the work performed by a third party service provider. Given that this was a new requirement, the District, in conjunction with the third party service provider, sought guidance from the auditors prior to the actual audit to seek to determine/verify whether the appropriate methods were being employed to comply with the new GASB 53 requirements. It was reasonable for management to conclude that the facilitation of direct communication between the third party, the auditors and the District about the calculation methodologies in advance of the audit represented an effective monitoring process for ensuring that the proper methodologies would be employed to comply with this new requirement.

   Management does not concur that the District may be relying on erroneous data from its third parties. The issue here was not the veracity of the data being relied upon, but was that for 1 of the 5 instruments, there was lack of clarity as to the proper calculation method to be used to test hedge effectiveness. The District knew that the third party had sought clarity on this from the auditors, and therefore thought the issue was being handled appropriately. In addressing effect, however, it should also be noted that these hedges were put in place well before the existence of the new GASB 53 requirements, and as such, the District employed other policies and methods to determine the prudence and effectiveness of the hedges; and, as verified by the application of the appropriate testing methods for all of the hedges by the third party and by the auditors, they all have in fact been functioning as effective hedges over the life of their existence and in FY 2010.

KPMG response:
We have read the District's response and consider our finding to be appropriate as presented.

3. Human Resources

We noted the following deficiencies in the Human Resources process:

a. The District has not developed or implemented policies and procedures to ensure the completeness and accuracy of the disability claims data that is provided to third party actuaries for purposes of determining the valuation of the District's disability compensation liability. We identified the following exceptions during our testwork over disability compensation claims data:

   1) Uniformed (FEMS and MPD) Worker's Compensation:

      - For eighteen (18) of a sample of forty-one (41) claims (FEMS) and 4 of 25 claims (MPD) selected, we noted that members were earning disability

compensation in excess of both the MPD's 1,376 maximum allowable hours and FEMS maximum allowable 512 hours.

- The District does not maintain supporting documentation for Worker's Compensation payments that are classified in the 100 series. This includes (but is not limited to) health care deductions, life insurance deductions, and compensation for missed work. Their supporting documentation is in the form of manual system notes recorded in the Via One System at the time the claim was filed by the District employee.

2) Tort Liability:

- The District has not developed sufficient policies and procedures to estimate tort liability reserves. In three (3) of fifty (50) sample items tested, we noted that the DC Office of Risk Management (DCORM) accrued additional reserves for possible settlement of the claim for which no documentation supporting the additional reserves was provided.

- We identified two (2) of a sample of twenty (25) claims tested for general tort liability claims were incorrectly classified as general tort liability claims and should have been reported as automobile claims as the claims representatives opened duplicative claims in two separate cases.

- For eight (8) of a sample of (25) general claims selected and three (3) of a sample of twenty five (25) auto liability tort claims tested no supporting documentation for the claims was provided.

b. During our performance of procedures related to District management's review other post employment benefit (OPEB) actuarial assumptions and final projections report, we identified that the District currently performs a limited and insufficient review of the underlying participant data provided by the District to its actuaries in order to estimate the District's OPEB liability at year end. This review is critical to ensure the completeness and accuracy of the claims data submitted to the actuaries.

Further, the District's Department of Human Resources (DHR) engages an actuary to provide a valuation of the liability for OPEB for District retirees. DHR has not adequately documented the rationale behind the actuarial assumptions established by the District.

Recommendations:

a. We recommend that management implement formalized policies over the disability compensation processes to ensure:

1) Documentation to support claims is proper maintained.

2) Claims data is reviewed and reconciled by management prior to submission for the annual actuarial valuation process.

3) Management level reviews are implemented to ensure disability compensation maximum allowable hours are not exceeded.

4) Develop consistent and standard policies for application when establishing Tort liability reserves.

Management should provide training on these policies to personnel responsible for performing these processes and monitor to ensure adherence with these policies.

b. We recommend that management develop and implement policies and procedures over a formal review process to ensure that the actuarially determined liabilities and disclosures in the financial statements are fairly presented in accordance with U.S. generally accepted accounting principles. This review process should be complete so as to include guidance related to the underlying participant data, assumptions utilized in the actual calculations and the propriety of the mathematical calculations.

Management Response:

a. Management concurs with the facts of this finding. Management concurs with the facts of this finding

While the ORM agrees with the general thrust of this finding, additional context and explanation must be provided regarding two of the auditor's statements. First, ORM disagrees with the statement that "[the] District does not maintain supporting documentation for Worker's Compensation payments that are classified in the 100 series." It is not accurate that ORM does not maintain any documentation for these payments, which generally include indemnity payments to workers' compensation claimants and deductions for health and life insurance benefits. In most cases, the primary documentation that ORM adjusters use when accepting a workers' compensation claim is the claimant's pay stub, which is then used to calculate the claimant's indemnity and other benefits. In many of the cases included in the auditor's sample, the original pay stub was available in the claim files; however, the payment in question did not match exactly the original pay stub documentation. This is because, over time, payments change depending on circumstances, including COLA increases or other adjustments in benefits. These changes are tracked over time with additional documentation and in the notes section of the claim files. It should also be noted that many of the cases where the auditor was unable to locate files were older cases where the date of injury was before 2005, when ORM began using electronic case files and improved its record-keeping practices. In addition, documentation may have been lacking because some older files may have been transferred from several other agencies, which used procedures different from the current documentation process currently

implemented by ORM. Nonetheless, ORM agrees with the auditor's recommendation that it should improve its documentation of payments in these circumstances.

ORM also agrees with the auditor's findings regarding its tort liability program. It should be noted, however, with respect to those cases in the sample where "no supporting documentation for the claims was provided," that the reason can often be attributed to the fact that little to no work had been done on the claim due to the program's significant resource constraints. ORM's two adjusters assigned to torts claims have caseloads of approximately 730 claims each, which makes it unrealistic to expect that all of the almost 1600 pending tort claims will include supporting documentation at any given time.

b. Management concurs with the finding and will follow the recommendation.

4. Procurement

We identified the following deficiencies in the Procurement process:

a. The District was not able to provide all the supporting documentation for three (3) of the seven (7) construction contracts selected for testing. More specifically:

   1) DRES (Department of Real Estate Services)

      - For two (2) contract files (CDFA-2008-C-0124-M01 & POAM-2005-C-0009-RS), the solicitation and evaluation documents were not available for review; therefore, we could not determine whether the contracts were competitively bid.

      - Also for one (1) contract (POAM-2005-C-0009-RS) the Determination and Finding for price reasonableness and Contractor responsibility, the Council approval and Office of the Attorney General legal review for when the contract was awarded in 2005, was not available for review.

   2) DDOT (Department of Transportation)

      - For one (1) contract file, the excluded parties' printouts were not available for review. Therefore, we could not determine whether the required research to determine whether the Contractor was debarred or suspended was performed.

b. During our testing over direct vouchers, one (1) transaction out of a sample of twenty-five (25) related to a prior year expenditure and initiated by the Department of Motor Vehicles was not approved by OFOS (Office of Financial Operations and System) prior to disbursement.

c. During our review of large procurements over $100,000, we identified several contracts with missing supporting documentation:

   1) Two (2) contracts were not available for review:

      - DCTO-2009-C-0232
      - DCAM-2007-C-7001

   2) The pre-award process documents were not available for review. Specifically, there was no evidence of competition for one (1) contract (POAM-2005-C-0044-03-CA).

   3) For two (2) contracts (DCAM-2007-C-2103 and DCTO-2009-C-0161) there was no evidence that the District performed a search to determine whether the vendor was debarred or suspended from conducting business with the District.

   4) The supporting documents provided for one (1) contract related to the FY 2009 contract that had expired.

5) The authorization for DC participation in a cooperative agreement with the contractor and the State of Virginia was not available for review.

d. We reviewed twenty five (25) transactions for fifteen (15) procurement purchase cardholders from fifteen (15) agencies and identified the following:

1) For one (1) cardholder, the transactions were not approved timely by the Approving Official;

2) For one (1) cardholder, the invoice was not available to support the transaction on the P-card statement;

3) For one (1) cardholder, the supporting documentation for the transactions on the P-card statement was not available for review; and

4) For 9 out of the 15 P-card statements requested, the Pending review/approve report was not available for review. Therefore, we could not determine whether the Approving Official is performing the monthly reconciliation and approval.

e. We requested a complete population of purchase orders issued during fiscal year 2010: the first dataset was pulled from the PASS data warehouse whereas the second was pulled from the production database. The system query from the production database returned a listing of purchase orders, which was missing 657 purchase orders found in the data warehouse database. 10,286 PO found in the data warehouse database were not found in the dataset pulled from the production database.

After three attempts and a 3-month delay, the District was able to explain the differences observed in the queries and rewrite a query to pull a complete population of purchase orders.

Also based on certain data routines we ran as part of our audit, we identified the following other data quality observations for a number of transactions:

1) No unique payment identification number;

2) Data files with missing fields (e.g., Vendors missing or incomplete address information);

3) Payments with missing check numbers; and

4) Duplicate Vendor identification number.

Recommendations:

a. We recommend that management implement a transition process to ensure all contract files are accounted for when there is turnover in the agencies' procurement team.

b. We recommend that all agencies be reminded that until a revised regulation is adopted into law, the standing law or regulation should be followed.

c. We recommend that the District implement appropriate controls to ensure compliance with relevant procurement laws and regulations in the Procurement Practices Act.

d. We recommend that the P-card Program office hold Agencies accountable for non-compliance with the District's P-card policies and procedures.

e. We recommend that the District enhance the training of PASS users to ensure they develop their ability to create system query to generate the desired reports within the system imposed limitations in a timely manner.

   We also recommend that system controls be implemented in PASS to prevent users from entering incomplete/duplicate data in the system.

Management Response:

a. Management concurs with the facts of this finding. In FY 2011, after evaluating transaction volumes and the extent of audit coverage across procurement thresholds (i.e. Single Audit, CAFR, ad hoc reviews by District Government investigative and oversight entities), OCP prioritized its limited resources to strengthen compliance in the area of Competitive Small Purchases ($5K $\geq$ $100K), as these on average represent more than fifty percent (50%) of transactions District-wide.

   As part of this training and in addition to real case examples, OCP has circulated a Quick Reference Guide (QRG) citing applicable sections of Title 27 DCMR and other codified procurement regulations, policies and procedures with the goal of identifying what the procurement professional must evidence within her/his contract file in order 10 be compliant.

   Corollary, given the relative success of this training, OCP is in the process of developing comparable models for transactions which are typically greater than $100K i.e. Invitation for Bids (IFBs) and Request for Proposals (RFPs).

   While tangible results might not be immediate, we expect that periodic training/ refreshers and regular compliance reviews will strengthen the control environment and ultimately improve compliance outcomes in subsequent fiscal years.

b. Management concurs with the facts of this finding. The liability was booked in compliance with OCP regulations and FY 2009 closing instructions provided by OFOS. Costs were incurred by DMV in August, 2009 and encumbered on PO2076964. DMV was unable to modify the purchase order for full payments prior to the closing submission date for FY 2009. Due to an oversight, the payment was not submitted to OFOS for approval.

c. Management concurs with the facts of this finding. In FY 2011, after evaluating transaction volumes and the extent of audit coverage across procurement thresholds (i.e. Single Audit, CAFR, ad hoc reviews by District Government investigative and oversight entities), OCP prioritized its limited resources to strengthen compliance in the area of Competitive Small Purchases ($5K ≥ $100K), as these on average represent more than fifty percent (50%) of transactions District-wide.

   As part of this training and in addition to real case examples, OCP has circulated a Quick Reference Guide (QRG) citing applicable sections of Title 27 DCMR and other codified procurement regulations, policies and procedures with the goal of identifying what the procurement professional must evidence within her/his contract file in order to be compliant.

d. Management does not concur with the facts of this finding. Agency response: According to the findings stated the District does agree that in 9/ 15 cases, Purchase Card policies and procedures are not being followed consistently by all District agencies. However, within the authority granted per the Purchase Card policies and procedures, this audit finding refers to program oversight and surveillance reporting that is currently the responsibility of each Agency Review Team (ART).

   Recommendation: The OCP Credit Card Program Management Office (PMO) will increase the monthly review of ART submissions after due date and issue a pre-suspension warning letter/email for agencies that are delinquent with monthly ART report submissions and Pnet approvals.

e. Management does not concur with the facts of this finding. After an extended period of requirements gathering and testing, the District delivered a complete set of purchase orders formatted to KPMG's specification issued by PASS in FY 2010 on 1/11/2011. Further, the District explained all differences between this complete dataset and the dataset generated by OCP on 1/11/2011. Attached to this response are emails confirming both of these facts. The District disagrees with the auditors finding that data is characterized as "missing". The District and the auditor went through an iterative process to ensure that the auditor's data files contained the required fields. However, the fact that it took an extended period of time to understand and extract the auditor's data does not indicate there is missing data in the PASS database. The PASS database is complete and intact with absolutely no missing data.

The District disagrees with characterizing the requirements gathering phase as a "three-month delay". The District exerted reasonable efforts to deliver to the auditor what was requested in a reasonable amount of time. The auditor also took time necessary to analyze and understand the data, contributing to the extended audit period.

The District disagrees with the "data quality observations" the auditor reported above. Specifically:

1) *No unique payment identification number* – PASS does not contain payment information, and this was explained to the auditor at the beginning of this engagement. Therefore, PASS contains no payment identification number of any kind. However, PASS has a unique constraint on the *Voucher ID* field. It is not possible for PASS to generate the same *Voucher ID.* This was tested again and found to be completely operational. On 2/22/2011, the District requested evidence from the auditor that might prove that this constraint is inoperative, but the auditor did not respond to the District.

2) *Data files with missing fields (e.g., Vendors missing or incomplete address information)* – PASS is designed with several required and optional fields, as per requirements captured form OCP and OCFO. Not all fields will be populated with data. This was explained to the auditor at the beginning of the engagement. However, PASS enforces the selection of a vendor and mail code for all Vouchers sent to SOAR. It is not possible to generate a Voucher without this data. This function was tested and found to be completely operational. On 2/22/2011, the District requested evidence from the auditor that might prove that this constraint is inoperative, but the auditor did not respond to the District.

3) *Payments with missing check numbers* – As mentioned to the auditor at the beginning of this engagement, and mentioned again above, PASS does not contain payment data or check number. It is unclear why this NFR mentions this data element.

4) *Duplicate Vendor identification number* – SOAR is the system of record for all vendor information. PASS only copies vendor information from SOAR. If there are duplicate vendor identification numbers, SOAR should be enhanced to prevent this from occurring. The District recommends assigning this specific finding to OFOS for additional review.

Finally, the District disagrees with the two recommendations above. As evidenced by the fact that the District was able to provide a complete dataset, and was able to explain why there were differences in the different extracts obtained by the auditor, additional training is not necessary.

The District also disagrees with the recommendation that PASS is enhanced to prevent users from entering incomplete/duplicate data in the system. The District successfully

demonstrated to another team on the auditor's staff, over a series of several days, the functionality of the system and all constraints and validations requested by the auditor. In addition, the auditor is also unable to provide any evidence to the contrary that PASS validations and constraints were somehow violated.

5. Medicaid and Grants Management

We identified the following deficiencies in the medicaid and grants management process:

a. During testwork over the medicaid accrual, we identified that the methodology developed by the District's Department of Healthcare Finance (DHCF) does not consider the additional reimbursement of Medicaid costs by the federal government under the American Recovery and Reinvestment Act (ARRA).

   In FY 2010, the District received additional federal reimbursement equal to 9.29% of eligible Medicaid costs under ARRA. This additional reimbursement was in effect throughout FY 2010 and will be phased out in 2011. In prior years, DHCF accrued based on the Federal Medical Assistance Percentage (FMAP). In FY 2010, this amount was 70% for the District of Columbia. With the enhanced FMAP under ARRA, the District could receive up to 79.29% reimbursement for eligible Medicaid costs. This increase in reimbursement was not considered in the calculations for the Medicaid accrual.

b. Public provider entities and private providers who submit costs through annual cost reports are required by the Medicaid State Plan to subject the cost reports to an audit. During testwork over the medicaid accrual, we noted delays in the issuance of audited cost reports.

   KPMG notes that the most recent audited cost reports for DCPS, CFSA, and DMH are 2007, 2007, and 2008 respectively.
   KPMG notes that the year of the most recent audited report for the cost based hospital Specialty Hospital of Washington (SHW) – Hadley is 2004, the most recent audited report for Riverside Hospital is 2006, and the most recent audited cost reports for SHW Capitol Hill and Psychiatric Institute of Washington are 2007.

c. The District is required by GASB No. 24 to record revenues and expenditures in the financial statements related to the value of Food Stamps. We noted in its testwork over the Food Stamps revenue and expenditures entry that the District does not retain source documentation from its service provider to support the amounts in the entry.

d. During testwork over the medicaid accrual, we noted that DHCF double-counted a liability in the amount of $4.7 million by recording the HMO Advantage lawsuit as a liability amount and also disclosing it in the contingent liabilities footnote as a "reasonably possible" case.

e. During testwork over the medicaid eligibility, we noted that 47 of 65 Medicaid provider files did not contain evidence of current licensure status. Licensure status and a written agreement are documentary evidence for whether a provider is eligible to receive reimbursement under the medicaid program.

f. During testwork over the deferred revenue at the Office of the State Superintendent for Education (OSSE), we noted that a portion of the balance could not be supported. Further, OSSE personnel indicated that the balance was under internal review because of the likelihood that amounts within the balance were improperly classified as deferred revenue.

g. We identified the following deficiencies regarding participant eligibility at the following programs:

1) Medicaid:

We noted incomplete supporting documentation in 6 of 65 files. We reviewed the files for the Medicaid application, Waiver Program application, and/or the recertification form. In several instances, the most recent recertification form was not included in the file. In other instances, the forms were included, but the supporting documentation (e.g., income verification, or updated identification) was not included.

2) Temporary Assistance for Needy Families (TANF):

We identified 14 of the 58 case files did not include the required documentation to support the TANF application and/or the recertification.

Specifically, we noted the following:

Seven instances in which the case file does not include adequate supporting documentation to show eligibility for TANF.

Seven instances in which the case file does not include documentation of recertification to continue TANF eligibility.

3) Food Stamps:

We identified that 12 of 65 case files did not include the required documentation to support the Food Stamps application or the recertification.

Specifically, we noted the following:

Three instances in which the case file does not include required supporting documentation for eligibility.

Ten instances in which the case file does not include documentation of recertification to continue Food Stamps eligibility

h. During testwork over Temporary Assistance for Needy Families (TANF) beneficiary eligibility, we identified that IMA was unable to locate 6 of 65 case files.

Recommendations:

a. We recommend that DHCF adjust the Medicaid accrual amounts to reflect the additional reimbursement from the federal government under ARRA.

b. We recommend that the District improve coordination and communication between the District and its providers in order to reduce the lag between the submission of cost reports and the audits of those reports.

c. We recommend that the District retain the monthly reports – or at a minimum the summary page from the reports – as a part of its records for the Food Stamps program.

d. We recommend that the District disclose the HMO Advantage lawsuit in the footnotes to the CAFR, as the likelihood of loss has been deemed "reasonably possible." Since the liability is deemed "reasonably possible", and not "probable", the District should not include the amount in the Medicaid accrual, in accordance with SFFAS No. 5.

e. We recommend that DHCF improve its process for maintaining current licensure information for Medicaid providers.

f. We recommend that OSSE remove the balances for financial reporting purposes until the issue is resolved.

g. We recommend that the District implement policies and procedures to improve the beneficiary case file management. KPMG notes that the District is in the process of scanning beneficiary files in order to make the file management system electronic.

h. We recommend that the IMA reinforce current policies and procedures in order to improve the case file management process.

Management Response:

a. Management concurs with the facts of this finding. Management agrees that the enhanced Federal Medical Assistance Percentage (FMAP) that is available as a result of the American Reinvestment and Recovery Act (ARRA) was not incorporated in the calculation of the Medicaid accrual.

   Management does not agree that an effect of the exclusion is to overstate the amount due to providers. All of the Medicaid accrual calculations are made on a gross (local and federal funds combined) basis. DCHF determines how local and federal funds are used to fund that accrual as the final calculation. Excluding the enhanced FMAP from the calculation affects how the accrual is funded – local versus federal – but not total amount due to providers.

Accurately determining the impact of the enhanced FMAP on the Medicaid accrual would add complexity with little gain in accuracy. DHCF forecasts Medicaid provider payments, and by extension the accrual, based on provider type (inpatient hospital, nursing home, physician, home health, etc.). However, payments for care for beneficiaries who became eligible for Medicaid as a result of eligibility expansions that occurred after the passage of ARRA are not considered qualified expenditures. For the District, this means the spending for the approximately 35,000 childless adults up to 133% of the federal poverty level who became Medicaid eligible July 1, 2010 as a result of the District exercising the early option in federal health care reform would have to be excluded from the accrual calculation. Although most of these beneficiaries are enrolled in managed care, a few hundred are not, and they could use services from any provider type. The upshot is that the accrual calculation for each of the approximately 35 provider types would require an additional determination of what portion was attributable to these childless adults versus the other Medicaid beneficiaries.

Determining the effect of the enhanced FMAP would also require a series of assumptions about when the amounts accrued will actually be paid out to providers. This is because the actual FMAP enhancement for qualified spending depends on the date of payment. The availability of enhancements appears in the chart below.

Payment Date Range	FMAP Enhancement
10/1/2010 - 12/31/2010	9.29%
1/1/2011 - 3/31/2011	6.47%
4/1/2011 - 6/30/2011	4.58%
After 6/30/2011	0.00%

For the most institutional providers, DHCF would have to make assumptions about when each provider would be paid. For the non-institutional providers, DHCF would have to make assumptions by provider-type about how much of the accrual amounts would be paid in each of the periods above.

To avoid the complexity and assumptions described above, DHCF used the District's regular FMAP of 70% in determining how the Medicaid accrual should be funded.

b. Management does not concur with the facts of this finding.

1) District of Columbia Public Schools:

Audit reports for FY 2007 were received Jan. 23, 2011. Fieldwork for the audits of FY 2008 is in process. The FY 2009 cost reports were submitted Oct. 29, 2010.

2) Child and Family Services Administration:

Audit reports for FY 2006 and 2007 were received Jan. 14, 2011. Fieldwork for the audits of FY 2008 is in process. The FY 2009 cost report is expected March 31, 2011.

3) Department of Mental Health:

The final Notice of Program Reimbursement, based on the audited FY 2008 cost report, was issued Oct. 19, 2010. Field work for the audit of FY 2009 is in process. The FY 2010 cost report is due Feb. 27, 2011.

4) Private Providers:

Audits of Specialty Hadley have been hampered by the provider's inability to obtain records from the previous ownership. DHCF has decided to approach the provider with a proposal to resolve the 2005 and 2006 audits. The 2007 and 2008 audits are in process and management believes these audits will be completed within the current year.

Specialty Capitol Hill appealed the audit results issued for 2006 and 2007 and is in the process of responding to DHCF's request for additional documentation. The 2008 audit has been begun.

Refiled 2009 cost reports for both Specialty Hadley and Specialty Capitol Hill were obtained Jan. 19, 2011 and DHCF intends to initiate audits this year. 2010 cost reports are due May 20, 2011 and DHCF intends also to initiate audits this year.

Riverside Hospital closed in fiscal 2008 and field work is being completed on the remaining years. An exit for the combined 2007-2008 closing audit is expected in February, 2011. Management believes this audit will be completed within the current year.

Auditors are completing field work for the 2008 Psychiatric Institute of Washington audit and DHCF expects to have this audit completed within the current year, and to initiate audits of 2009 and 2010.

Management believes it is reasonably timely by industry standards in completing public provider audits. Completion of the District's annual CAFR audit is necessary to prepare final adjustments before cost reports can be completed. Given efficient preparation and filing of cost reports, the time required to complete audit work, hold exit conferences and resolve outstanding issues is likely to extend beyond September 30th of each year. Management believes in the case of private providers that it is making reasonable progress in dealing with unique problems attendant upon change of ownership and termination of participation. In the case of P.I.W., the District has a long and consistent relationship with the provider and believes it will successfully recover any amounts deemed due upon audit, either through settlement or retention of claims payments.

c. Management concurs with the facts of this finding and responds that this is not a Department of Human Services finding. [The Department of Human Services (DHS)] recognizes that the hard copy of the documentation was not available during the time of the audit; however, [DHS] is not the recipients of these statements. The Office of Finance and Treasury (OFT) was not in the practice of retaining the summary statement since they are available on line through JP Morgan Chase Manhattan Bank. However, JP Morgan only has the statements live on line for a period of three months and then they archive this information after the three month period. The monthly statements were subsequently retrieved from JP Morgan for FY 2010. [DHS] contacted OFT and going forward they will print out and retain the monthly summary report from the online system of recordation.

d. Management concurs with the facts of this finding. The Government of the District of Columbia FY 2010 Close Instructions for Topic 11 Commitments and Contingencies (page 170) requires agencies to, in part, "...report each contingent liability with a maximum (worst case) potential loss of $50,000." The Department of Health Care Finance (DHCF) complied with that instruction by reporting the $4.7 million claim before the Contract Appeals Board from HMO Advantage.

   DHCF believes it is probable that the District will have to pay HMO Advantage when this action is finally resolved. Since it is a requirement that agencies pay their liabilities, the District has consistently accrued for this $4.7 million claim on the Medicaid agency's books as part of the Medicaid accrual.

e. Management concurs with the facts of this finding. Provider Services will conduct periodic spot audits to ensure that the provider licensure on file mirrors the license information displayed on the "provider eligibility/specialty" tab within the Medicaid Management Information System.

f. Management concurs with the facts of this finding. The OSSE OCFO came under new management in October 2009, and inherited these large deferred revenue balances, which date back to FY 2007. The agency is engaging an external auditor to complete a comprehensive review of all deferred revenue balances. We expect that this review will be complete in time for any corrective action required to be completed before the close of FY 2011.

g. Management concurs with the facts of this finding. During FY 2010. DHS undertook the Document Imaging Management System (DIMS) initiative, which is expected to improve the accuracy of eligibility determination and efficiency of locating documents within IMA. The DIMS process entailed several phases and tasks including transferring records of clients who visited other IMA Service Centers back to the appropriate Center, so that the records would be prepared for the DIMS scanning process. Due to space limitations, not all files and records could be transferred and this contributed to the challenge of locating records and documents in time for review by the auditors. Additionally, the agency experienced an approximate 40% increase in applications since

2009, and a reduction in staff and ongoing vacancies since 2007-2010, which has also contributed to a number of records/documents not being properly filed. To address this issue, DHS moved the Case Record Management Unit under one supervisor who reports to the Deputy Administrator for Program Operations to ensure consistency and accountability of staff. In addition. DHS established a business process that requires scanning, tagging, and indexing of documents upon receipt, rather than allowing documents to compile and scan at a later date.

Scanning of records started January 1, 2011. All existing documents and records should be scanned within the next two years. Moreover, DHS began scanning all new documents upon receipt from customers as of January 1. 2011. DHS is confident that as the process of scanning of records and documents becomes more proficient future deficiencies in case documentation will be avoided.

h. Management concurs with the facts of this finding. During FY 2010, DHS undertook the DIMS initiative, which is expected to improve the accuracy of eligibility determination and efficiency of locating documents within IMA. The DIMS process entailed several phases and tasks including transferring records of clients who visited other IMA Service Centers back to the appropriate Center, so that the records would be prepared for the DIMS scanning process. Due to space limitations, not all files and records could be transferred and this contributed to the challenge of locating records and documents in time for review by the auditors. Additionally, the agency experienced an approximate 40% increase in applications since 2009, and a reduction in staff and ongoing vacancies since 2007-2010, which has also contributed to a number of records/documents not being properly filed. To address this issue, DHS moved the Case Record Management Unit under one supervisor who reports to the Deputy Administrator for Program Operations to ensure consistency and accountability of staff. In addition, DHS established a business process that requires scanning, tagging, and indexing of documents upon receipt, rather than allowing documents to compile and scan at a later date.

Scanning of records started January 1, 2011. All existing documents and records should be scanned within the next two years. Moreover, DHS began scanning all new documents upon receipt from customers as of January J 1, 2011. DHS is confident that as the process of scanning of records and documents becomes more proficient future deficiencies in case documentation will be avoided.

6. Revenue

We noted the following deficiencies in the revenue process:

a. During our testing of tax refunds, we identified that OTR issued 374 refunds to individuals and businesses outside of the United States (excluding those issued to an Army Post Office (APO), Armed Air Forces (AA), or the Armed Forces Europe (AE)). Based on our discussions with management, we identified that the District does not perform a detailed review of refunds being paid out to these individuals and businesses if the refunds are below a threshold dollar value of $10,000.

b. We identified that management has not performed adequate verification and validation procedures surrounding the methodologies used for setting the allowance for various types of tax receivables as the allowance percentages have not been formally re-examined since FY 2004.

c. During our testwork performed at OTR–the Revenue Accounting Administration (RAA), we identified that 15 of the 27 monthly Bank to SOAR to ITS reconciliations selected for testing included significant reconciling items which were not corrected or input into ITS. We observed that ITS is not capable of applying information to a taxpayer account when information from the deposit does not match 100% of the data fields within ITS. These unreconciled items are listed in ITS as unposted / suspended deposits and are not matched to the taxpayer account.

Recommendations:

a. We recommend that the OTR Revenue Accounting Administration review 100% of all tax refunds being issued to foreign addresses to ensure the validity and accuracy of the refund being provided.

b. The Office of Tax and Revenue should reassess the reserve percentages applied to determine the Allowance for Doubtful Accounts for non-RPT Taxes Receivable on an annual basis, at minimum, by performing a look-back analysis of actual collections of receivables. Additionally, management should identify and consider other relevant factors, such as the state of the economy, in its analysis.

c. We recommend the following:

   1) We recommend that OTR establish and implement reconciliation procedures that require reconciling items identified between SOAR and ITS to be updated and corrected within ITS within 30 days of identification.

   2) In addition, OTR should prepare an annual reconciliation of SOAR to ITS to ensure that all reconciling items identified throughout the fiscal year have been updated and are properly reflected within ITS.

Management Response:

a. Management concurs with the facts of this finding. OTR recognizes the risk of unauthorized or fraudulent refunds across the entire taxpaying population. Although we concur with the facts of the finding, we do not concur with the conclusion or the recommendation.

   Of more than 265,000 tax refunds issued annually (249,000 individual income), only 609, or 0.23%, went to any foreign address, including an APO, AA, or AE address indicating a member of the US military deployed overseas. The dollar value of the refunds identified in the finding totals less than $300,000. As a percentage of the total population, these kinds of refunds do not represent a material risk in our opinion.

   In order to address the risk of unauthorized refunds, OTR has implemented a suite of controls, which includes:

   1) Establishment of a specialized Refund Control Unit, charged with ensuring that refunds meet defined documentation and approval criteria;

   2) A tiered review process, which requires multiple sign-offs and certifications based on various established dollar thresholds and refund type;

   3) A signature control process to ensure that sign-offs are original and appropriate based on dollar thresholds;

   4) The use of systemic reports to sample employee work, particularly as it relates to adjustment activity;

   5) A feedback loop and regular refresher training on control responsibilities and requirements for properly documenting refunds; and

   6) Clearly documented procedures for processing a refund, and for reviewing a refund to ensure that it is properly authorized and documents, based on established thresholds.

   Due to resource constraints, OTR has defined a risk appetite for refunds below certain dollar thresholds. Management will continue to look at opportunities to refine the current control structure and to identify additional review criteria that can further mitigate risk, but we believe that the current structure provides the best control available for the very large universe of refund activity.

b. Management concurs with the facts of this finding. OTR agrees that the reserve percentages used to calculate the allowance for doubtful accounts have not been reviewed on an annual basis. However, management does recognize the risk of potential misstatement of accounts receivable, and believes that the current allowance reserves are appropriately conservative. The current calculation reserves 50% of accounts receivable in the first year for most tax types (excluding real and person property). This rate increases annually until after the fourth year, the reserve rate for these accounts receivable reaches 100%.

   Additionally, although an analysis of delinquent receivables collections has not been performed recently, a review process is in place that, in combination with the allowance for doubtful accounts, ensures that OTR has fairly and conservatively estimated the true value of its receivables. This process involves testing and close review of accounts receivable balances in order to systemically identify balances that are erroneous due to processing errors or other systemic issues.

   Management will develop procedures for reviewing the allowance rates on a yearly basis. The review will take into account collection rates, the economy and other relevant factors.

c. Management recognizes the risk of inaccurate taxpayer account information in the Integrated Tax System (ITS), caused by suspended transactions. The current monthly reconciliation process is an important part of the overall system of controls designed to ensure that the high volume of taxpayer account transactions in ITS is recorded accurately, which also includes the active working of the suspense queue in the Returns Processing Administration (RPA).

   It should be noted that taxpayer error is often a root cause for the variances, and clarification can often be determined only with the aid of the taxpayer, the taxpayer can be identified. Additionally, the automated transfers between accounts may require that bank/SOAR to ITS reconciliations are done to include multiple deposit accounts and multiple taxpayer accounts in order to identify all of the related activity.

   Management recognizes the opportunity to improve the reconciliation process, and is in the beginning stages of reengineering the process to ensure that reconciling items are resolved in month over month and annual reports. Some variance will always exist, because some payments are applied to taxpayer accounts that are not in ITS, such as payments received via the real property custodial account intended for Business Improvement District payments, and payment for non-ITS tax types.

7. Financial Reporting

We noted the following deficiencies in the financial reporting process:

a. Although agencies may not record any transaction in the general ledger without OFOS approval after the last week in November, the District did not close its FY 2009 general ledger in SOAR until the end of July 2010 when all transactions that were coded for FY 2009 were entered in the system.

b. Based on the testing performed over manual journal entries, we made the following observations relating to the District's manual journal entry data in SOAR:

   1) A number of journal entries included in the manual entry population did not include a description because the current system of record does not require for journal entries to include a description of the transaction.

   2) A number of manual journal entries included in our population had over 1,000 lines. we determined that the current system of record allows for a maximum of 99,999 lines to each journal entry.

Recommendations:

a. We recommend that the new system of record being implemented by the District include a more timely and efficient closeout process that would prevent any changes to the general ledger after the CAFR issuance.

b. As the District implements a new system of record, we recommend that the District implement policies and procedures that will ensure the production of high quality auditable data. Specifically, we recommend that:

   1) The transaction description field be required for all journal entries.

   2) The maximum number of lines allowed for a journal entry be reduced from 99,999 to a more reasonable number to allow for an effective review and investigation by the District in the event a journal entry needs to be researched.

Management Response:

a. Management concurs with the facts of this finding. The OFOS agrees that the general ledger should be complete and officially closed in the system in a more timely manner before July. However, we do not agree that when the financial audit is complete the system should not allow users to make changes to the financial system. As with most tasks / events, a reasonable time period is normally allowed for a final review and / or reconciliation of information after the task / event occurred. During the District's closing process several entries are recorded in the system at a high level and then after

the publication of the CAFR, the detailed entries are recorded and the high level entries are reversed in the system. Examples of such entries are the fund balance reservation at the agency and grant level, the elimination of the Intra District revenue and expenditure transactions at the agency and object code level and other CAFR related entries that were recorded in the system at a high level.

Although there is always the chance for users to post transactions to the incorrect fiscal year, access to the system for post CAFR reconciliation is restricted to two highly skilled employees in the Financial Control and Reporting Division of OFOS. The OFOS has been successful for the last 10 years in controlling this task and the District's books have always reconciled to the information published in the CAFR.

The OFOS will strive to complete the final CAFR review and reconciliation process in the system in a timely manner.

b. Management concurs with the facts of this finding. Management responded as follows:

1) The current financial system does not require a transaction description. I have contacted our technical staff to determine the level of effort that is needed to make this field a required field for all journal entries. Additionally, the suggestion to require a description on journal entries has been added to the requirements for the new financial system.

2) A restriction on the number of journal entries in one batch would be difficult to change in the current environment. All the interfaces would need to be changed. The most significant change would create partial position of payroll batches. There are agencies that have 30,000 summary entries to post expenses to the General Ledger. If this were changed it would create monumental research problems. While the change to the current system is not likely, this suggestion has been added to the requirements for the new financial system.

Section III – University of the District of Columbia

During our audit of the basic financial statements, we noted deficiencies at the University of the District of Columbia related to controls over third party servicers, compliance with investment policy, the financial reporting process, and the payroll process. In the pages that follow, we have broken down these deficiencies by area below along with both KPMG's recommendation for remediating the deficiency noted as well management's response to the noted deficiency.

1. Third Party Servicers

We noted the following deficiency related to controls over the lack of monitoring third party servicers:

a. Management does not obtain and review reports performed in accordance with Statement on Auditing Standards No. 70, *Service Organizations* (SAS No. 70 reports) or perform alternative procedures over the controls in place at third-party service providers that impact the University's financial reporting. Specifically, the SAS No. 70 reports of investment fund managers (Stanford Bernstein & JPMorgan) are not reviewed to ensure that controls which impact the processing of University's investment transactions are properly designed and operating effectively.

   In addition, there are not sufficient procedures in place to ensure that transactions processed by Tuition Management Systems (TMS), a third-party service provider are complete and accurate. TMS collects and remits tuition payments to the University on the behalf of the University's students who are on a payment plan. TMS does not have a SAS No. 70 review performed. The University does not perform alternative procedures to ensure that controls at TMS impact the processing of tuition payment transactions are properly designed and operating effectively.

Recommendations:

a. We recommend that Management review the SAS No. 70 report of its investment fund managers, JPMorgan and Stanford Bernstein to ensure that controls which impact the processing of the investment transactions are properly designed, in place and operating effectively and that user controls are appropriately identified.

   We also recommend that the University perform alternative procedures, such as testing controls in place at TMS or requiring TMS to obtain a review in accordance with SAS No. 70 to ensure that management can properly monitor the design and operating effectiveness of controls over the processing of tuition payment transactions.

Management Response:

a. Management concurs with this finding.

   UDC and the Office of Finance and Treasury (OFT) staff will look to engage a third party investment consultant to assist in the review and oversight of external investment

managers. This engagement will include policy compliance, as well as review of SAS 70 for managers.

In addition, management will review and document the consultant's work to make sure it is in compliance with SAS 70.

2. Compliance with Investment Policy

We noted the following deficiency related to compliance with investment policy:

a. During our testing of mutual fund investments in, we noted that the University's mutual fund investment in Bernstein International Value II portfolio (SIMTX) had an overall two-star rating from Morningstar during fiscal year 2010 which is not in compliance with the *University of the District of Columbia Endowment Fund Investment and Spending Policy* (Investment Policy). Per the Investment Policy, all mutual funds must maintain at least a three-star rating from Morningstar. The market value of SIMTX is $3.2 million or 9.2% of the total investment portfolio of $35 million as of September 30, 2010.

Recommendation:

a. We recommend that management periodically review its investment portfolio, including the fund managers' purchase decisions to ensure compliance with all Investment Policy requirements.

Management Response:

a. Management concurs with this finding.

UDC and the Office of Finance and Treasury (OFT) staff will be engaging in a RFP in FY 2011 to replace underperforming managers and managers not meeting mutual fund ratings. UDC and OFT staff will also engage a third party investment consultant to assist in investment reviews and portfolio compliance during the fiscal year. At this stage management is comfortable with the existing exposure to the Bernstein fund and will document the policy violation to the Investment Advisory Board.

3. Financial Reporting

We noted the following deficiencies in the Financial Reporting process:

a. During our audit, we noted that the University did not have adequate and effective internal controls in place over the financial reporting process as follows:

1) Preparation and management review of the financial statements

The University did not submit a complete and accurate set of financial statements for audit in accordance with the agreed-upon financial reporting timeline.

Specifically, the University submitted draft financial statements for audit that did not include a statement of cash flows, as required by generally accepted accounting principles (GAAP). In addition, we noted that many of the notes to the financial statements, specifically cash and cash equivalents, accounts receivable, grants and contracts receivable, and capital assets, did not agree to the amounts on the face of the statements. Management informed us that the initial version of the financial statements submitted for audit was incomplete and subsequently provided a revised draft of the financial statements. However, we noted that certain balances included in the subsequent draft of the financial statements still did not agree to the face of the financial statements. In addition, we noted that while a statement of cash flows was provided, the cash and cash equivalents balance on the statement of net assets did not agree to the ending cash and cash equivalents balance on the statement of cash flows. In addition, we noted that although the management's discussion and analysis included the amounts and percentages of change from the prior year, it did not sufficiently describe the reasons for significant changes from the prior year in accordance with GAAP.

2) Inadequate account review and analysis

We noted that several accounts included amounts which could not be adequately supported by management. Specifically, we noted that management was aware that the year-end accounts receivable balance included approximately $3.4 million related to amounts that were carried over from a prior year system conversion. As this amount could not be adequately supported by management and does not represent valid future claims, it does not meet the definition of a valid receivable.

In addition, the year-end grants and contract receivable balance included approximately $384 thousand in receivables that have been outstanding for over nine years and could not be adequately supported and were not reserved for in the allowance for doubtful accounts. Management did not perform an aging analysis to determine the ongoing collectability and validity of these receivable balances.

Lastly, the year-end deferred revenue balance included approximately $133 thousand of deferred revenue that remained deferred for over nine years and could not be adequately supported. Management did not perform an analysis to ensure that the amounts were valid.

3) Lack of Controls over Accounting for Capital Assets

During our testing of capital assets, we noted certain individually significant items that were not properly capitalized. As a result, management performed an analysis over the operating expense and capital asset accounts and noted an additional $14 million that were erroneously recorded as operating expenses. In addition, during our testing of capital assets, we noted $2.4 million of capital assets with fiscal year 2009 in-service dates that were included as fiscal year 2010 capital asset additions.

These errors represented 16.3% of the fiscal year 2010 capital additions of $14.7 million.

4) Calculation of the allowance for doubtful accounts

During our year-end testing of the methodology and calculation of the allowance for doubtful accounts related to student accounts receivable, we noted that the calculation did not use the correct accounts receivable balance as of September 30, 2010. Specifically, management erroneously used the amount of $15,838,793 instead of the correct amount of $12,302,951, resulting in an overstatement in the calculation for the allowance for doubtful accounts.

Recommendations:

a. We recommend that management implement policies and procedures to require the following:

1) Thorough review of financial statements prior to submission for audit;

2) Thorough review and analysis of account detail and balances;

3) Performance of routine aging analysis of outstanding receivables to assess collectability;

4) Review and analysis of expenses to ensure the appropriate accounting treatment (i.e., capitalized or expensed) and to ensure capital assets are recorded in the proper fiscal year; and

5) Thorough review and approval over the calculation of the allowance for doubtful accounts.

Management Response:

a. See Management's response below:

1) Preparation and management review of the financial statements

Management concurs with this finding.

Management understands the composition of the three basic financial statements as required by generally accepted accounting principles (GAAP). However, in order to meet the CAFR submission deadline that was established by the University and agreed to by all parties (12/22/2010), UDC management submitted "the Balance sheet" and "Statement of Revenue, Expenses and Changes in Net Assets", while still working on "the Statement of Cash Flows" and updating "Foot notes". Management

embarked on this strategy to speed up the audit and give the auditors a head start in order to meet the established deadline.

In order to prevent such inconsistent submission of the Financial Statement in the future, management will work closely with its auditors to set timelines that both meet the City's CAFR deadline and also provide enough time for audit work.

2) Inadequate account reviews and analysis

Management concurs with this finding.

UDC has set-up sufficient amount as allowance for doubtful accounts to allow for possible write-off in the event that any receivable is deemed uncollectible. Also, management will conduct routine aging analysis to determine probability of collections.

3) Lack of controls over Accounting for Capital Assets

Management concurs with this finding.

Prior to FY 2010, all capital related transactions were handled by the DC Department of Real Estate for all District agencies including UDC. Fiscal year 2010 is the first year that UDC procurement and real estate division assumed the management of capital assets. Because this has been a new function for UDC procurement division, it was not captured in the Fixed Asset Module. However, all these capital expenditures stays as expenditures in the income statement.

To ensure that all capital assets are timely and properly identified and capitalized, the new Banner financial system that was implemented in FY 2011, will allow UDC to set up construction project correctly in the proper asset class as they are processed.

4) Calculation of the allowance for doubtful accounts

Management concurs with this finding.

Management has added a second level approval path that will be conducted by the controller and will also serve as a quality control measure. This will ensure that this situation does not recur.

4. Payroll Process

During our year-end testwork over the payroll process, we noted the following deficiency:

a. During our testing of payroll expense, we noted one payroll transaction amounting to $43,915 of the ninety-eight payroll transactions selected that was incorrectly charged to the University's payroll register.

   Specifically, we noted that the transaction related to an employee who retired from the Office of Chief Financial Officer (OCFO) in October 2009. Upon retirement, the employee received a retirement incentive award in the amount of $15,000, and was also entitled to a severance payment of twenty-six weeks of regular pay. The retirement incentive award payment was contingent upon the employee not being employed by the Government of the District of Columbia for a period of five years. As the employee was hired into an adjunct faculty position by the University in January 2010, the employee properly repaid the award amount. The credit for the repayment was erroneously recorded in the University's payroll register instead of the appropriate agency (OCFO). The employee received the remainder of his OCFO severance payment in the amount of $43,915.35 in February 2010. The credit for the severance payment was also erroneously recorded in the University's payroll register.

   In addition, during our testing of the time and attendance (T &A) process, we noted that for three of the sixteen non-salaried employees selected, the T&A form was not properly signed by the authorizing supervisor.

Recommendation:

a. We recommend management implement controls to ensure amounts included in the University's payroll expense represent true and valid expenses of the University.

   In addition, we recommend that the University ensure all T&A forms for non-salary employees are signed by both the employee and supervisor in accordance with the University's existing policy.

Management Response:

a. Management concurs with this finding.

   Management has instituted the following controls to eliminate such oversight:

   Budget Analyst assigned to specific program will conduct bi-weekly review of the University's 485 Payroll Report. This will include analysis of payroll charges by program and employees receiving payments. This process will also enable the analysts to identify excessive payments that did not receive prior approval by UDC finance department prior to payment.

   A second level review will be conducted by Specific Program owners, to identify legitimate program employee charges. This will ascertain that only current employees working within that program are getting paid.

The final and third level review will be conducted by the Budget Director, who will sign off on all 485 Payroll Reports, to make sure the above reviews are properly conducted, and all adjustments, if needed are made within a reasonable time frame.

Section IV – Other Matters to be Communicated

1. Failure to claim expenses under Medicaid

In January 2009, the Child and Family Services Agency (CFSA) suspended billing for Medicaid services under billing strategies for Targeted Case Management and Rehabilitative Services. The Agency ceased billing Medicaid in order to address potential disallowances for insufficient documentation and services which are not allowable under the Medicaid program. As a result of the suspension in billing to Medicaid some of CFSA's costs were shifted to other grants for reimbursement; however a large portion of the costs are now absorbed completely by the District.

KPMG is unable to estimate a dollar amount of unbilled Medicaid costs for FY 2010; but the information that is available indicates that the unbilled amount at CFSA could be significant. To demonstrate this point: in FY 2010 CFSA billed Medicaid for $298,000 related to clinic services. In FY 2008, CFSA wrote off $32.0 million in accounts receivable that it had previously billed to Medicaid for reimbursement.

The District has initiated several process-improvement programs in order to rebuild the billing strategies at CFSA but until the strategies are fully implemented, the District will continue to incur costs which may have been reimbursable under Medicaid.