

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

**DISTRICT OF COLUMBIA
FISCAL YEAR 2014
MANAGEMENT LETTER REPORT**



**DANIEL W. LUCAS
INSPECTOR GENERAL**

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



April 20, 2015

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

Jeffrey S. DeWitt
Chief Financial Officer
Office of the Chief Financial Officer
The John A. Wilson Building
1350 Pennsylvania Avenue, N.W., Suite 203
Washington, D.C. 20004

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


Dear Mayor Bowser, Chairman Mendelson, and Mr. DeWitt:

I am issuing the enclosed final Government of the District of Columbia Fiscal Year 2014 Management Letter Report, submitted by KPMG LLP (KPMG) as part of our contract for the audit of the District of Columbia's general purpose financial statements for FY 2014 (OIG No. 15-1-17MA). This report sets forth KPMG's comments and recommendations intended to improve internal control or result in other operating efficiencies in the District government.

My office will conduct follow-up on agency actions taken to address the conditions that KPMG identified.

If you have questions or need additional information, please contact me or LaDonia M. Wilkins, Acting Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,


Daniel W. Lucas
Inspector General

DWL/ws

Enclosure

cc: See Distribution List

DISTRIBUTION:

Mr. Rashad M. Young, City Administrator, District of Columbia (via email)
Ms. Brian Kenner, Acting Deputy Mayor for Planning and Economic Development, District of Columbia (via email)
The Honorable Jack Evans, Chairperson, Committee on Finance and Revenue, Council of the District of Columbia (via email)
Mr. John Falcicchio, Chief of Staff, Office of the Mayor (via email)
Mr. Michael Czin, Director, Office of Communications, (via email)
Ms. Nyasha Smith, Secretary to the Council (1 copy and via email)
The Honorable Karl Racine, Attorney General for the District of Columbia (via email)
Mr. Timothy Barry, Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (via email)
Ms. Kathy Patterson, D.C. Auditor, Office of the D.C. Auditor,
Attention: Candace McRae (via email)
Mr. Phillip Lattimore, Director and Chief Risk Officer, Office of Risk Management (via email)
Mr. Steve Sebastian, Managing Director, FMA, GAO, (via email)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives,
Attention: Bradley Truding (via email)
The Honorable Jason Chaffetz, 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: Marianna Boyd (via email)
The Honorable Ron Johnson, Chairman, Senate Committee on Homeland Security and Governmental Affairs, Attention: Patrick Bailey (via email)
The Honorable Thomas Carper, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs, Attention: Holly Idelson (via email)
The Honorable James Lankford, Chairman, Senate Subcommittee on Regulatory Affairs and Federal Management. Attention: John Cuaderes (via email)
The Honorable Heidi Heitkamp, Ranking Member, Senate Subcommittee on Regulatory Affairs and Federal Management, Attention: Eric Bursch (via email)
The Honorable Harold Rogers, Chairman, House Committee on Appropriations,
Attention: Amy Cushing (via email)
The Honorable Nita Lowey, Ranking Member, House Committee on Appropriations, Attention: Shalanda Young (via email)
The Honorable Ander Crenshaw, Chairman, House Subcommittee on Financial Services and General Government, Attention: Amy Cushing (via email)
The Honorable José E. Serrano, Ranking Member, House Subcommittee on Financial Services and General Government, Attention: Shalanda Young (via email)
The Honorable Thad Cochran, Chairman, Senate Committee on Appropriations,
Attention: Ben Hammond (via email)
The Honorable Barbara Mikulski, Ranking Member, Senate Committee on Appropriations,
Attention: Kali Matalon (via email)

Mayor Bowser, Council Chairman Mendelson, and Mr. DeWitt
FY 2014 DC Management Letter Report
OIG No. 15-1-17MA
April 20, 2015
Page 3 of 3

The Honorable John Boozman, Chairman, Senate Subcommittee on Financial Services and
General Government, Attention: Dale Cabaniss (via email)
The Honorable Chris Coons, Ranking Member, Senate Subcommittee on Financial Services and
General Government, Attention: Marianne Upton (via email)
Mr. Paul Geraty, CPA, Public Sector Audit Division KPMG LLP (1 copy)

Government of the
District of Columbia
Fiscal Year 2014
Management Letter

**GOVERNMENT OF THE DISTRICT OF COLUMBIA
MANAGEMENT LETTER
FOR THE YEAR ENDED SEPTEMBER 30, 2014
TABLE OF CONTENTS**

MANAGEMENT LETTER	1
APPENDIX A	A-1
CURRENT YEAR FINDINGS AND RECOMMENDATIONS	A-1
1. <i>Cash and Investments</i>	A-1
2. <i>Disability Compensation</i>	A-9
3. <i>Capital Assets</i>	A-10
4. <i>Grants Management</i>	A-19
5. <i>Loans Receivable</i>	A-21
6. <i>Revenue</i>	A-23
7. <i>Payroll</i>	A-30
8. <i>Financial Reporting</i>	A-33
9. <i>Information Technology</i>	A-34
10. <i>District of Columbia Public Schools</i>	A-59



KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

March 30, 2015

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

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, the budgetary comparison statement, each major fund, and the aggregate remaining fund information of the Government of the District of Columbia (the District), which collectively make up the District's financial statements, as of and for the year ended September 30, 2014, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, 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 in Appendix A to this report. These comments and recommendations, all of which have been discussed with the appropriate members of management as part of the Notification of Findings and Recommendations (NFR) process, are intended to improve internal control or result in other operating efficiencies. The District's written responses to our comments and recommendations are included in Appendix A. The District's written responses to our comments and recommendations have not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly we express no opinion on them.

In addition, we identified certain deficiencies in internal control that we consider to be significant deficiencies and communicated them in writing to management and those charged with governance in our *Independent Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with Government Auditing Standards* dated January 28, 2015.

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.



The purpose of this letter is solely to describe these comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

APPENDIX A: CURRENT YEAR FINDINGS AND RECOMMENDATIONS

1. Cash and Investments

a. Strengthen Controls Over Compliance with the Financial Institutions Deposit and Investment Act of 1997

CONDITION

1. Compliance with Collateral Requirements

We selected a sample of 20 financial institutions (5 from each of 4 months selected) to test completeness and accuracy of the underlying data, the respective bank balance and pledged collateral, used to determine if the District's 102% collateral requirement had been met, and noted the following:

For 2 of 20 financial institutions, the bank balance per the Collateral Monitoring Worksheet did not agree to the balance reported per the corresponding month's bank statement:

Month	Financial Institution	Bank Balance per Worksheet	Bank Balance per Bank Statement	Difference
October 2013	Bank of Georgetown	\$40,000,000	\$40,028,170	\$28,170
February 2014	Premier Bank	\$10,015,455	\$10,012,090	\$3,365

As such, monthly calculations performed by the District to determine compliance with the collateral requirement per the Financial Institutions Deposit and Investment Act were not accurate resulting in increased risk that instances of non-compliance may not be detected. However, we noted no instances of non-compliance with the collateral requirement during our testing.

2. Compliance with Requirement to Invest Excess Funds

We selected a sample of 18 Beginning of Day and End of Day Quick Reports, which are used by the District to prevent and detect non-compliance with the Financial Institutions Deposits and Investment Act – General Deposit and Investment Requirements and the District's Cash and Investment Management Policy. For 4 of 18 reports tested, the "Balance After Position" per the End of Day worksheet did not agree with the "Balance After Position" per the Beginning of Day worksheet, causing the final end of day balance available to be invested to be miscalculated. However, we noted no instances in which excess funds were not invested.

3. *Compliance with Deposit Limitations in Financial Institutions*

We selected a sample of 31 total assets and total deposits amounts across various days and financial institutions in fiscal year 2014 to test completeness and accuracy of underlying data in the Cash Note Reports, which are used by the District to monitor compliance with the Financial Institutions Deposits and Investment Act requirements to limit the concentration of deposits within a single financial institution. During our testwork, we noted the following:

- For 7 of 31 sampled items, we noted the Total Assets values used to perform the daily calculation of Percentage of Deposits held at the Financial Institution of the financial institution's Total Assets were not updated on at least a quarterly basis. For 6 out of 31 sample items, we noted the Total Assets per the Cash Note Reports did not agree to the support provided.
- For 10 of 31 sampled items, we noted the Total Deposits values used to perform the daily calculation of Percentage of Deposits held at the Financial Institution of the financial institution's Total Assets did not agree to the support provided.
- For 1 of 31 sampled items, the Percentage of Deposits held at the Financial Institution of the financial institution's Total Assets was incorrectly calculated.

As such, the daily calculations performed to verify that the District's deposits at a particular financial institution comprise less than 25% of a financial institution's total assets and the District's total deposits are not accurate. Consequently, there is an increased risk that instances of non-compliance may not be detected. However, we noted no instances of non-compliance with the requirement to limit the concentration of deposits in a financial institution.

CRITERIA

Government Auditing Standards (Yellow Book), Appendix I, section A1.08 d., states that management at a State and Local government entity is responsible for “*establishing and maintaining effective internal control to help ensure that appropriate goals and objectives are met; following laws and regulations; and ensuring that management and financial information is reliable and properly reported.*”

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control—Integrated Framework* states:

- “*Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the*

technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

- *Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, standard-setting bodies, or management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate. Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning.”*

Per the Financial Institutions Deposit and Investment Act of 1997, Section 47-351.8, Collateral and Reporting Requirements, “*(a) Except for securities directly purchased without a repurchase agreement and money market funds, an eligible financial institution must at all times provide collateral equal to at least 102% of the District funds held by the eligible financial institution- for deposits and investments that are not fully federally insured.*”

Per the Financial Institutions Deposit and Investment Act of 1997, Section 47-351.3, General Deposit and Investment Requirements, “*(b) The Mayor, or the CFO pursuant to [Section] 47-351.2(c), shall determine what amount of District funds are needed immediately and maintain deposit funds in amounts great enough to satisfy that need. The Mayor, or the CFO pursuant to [Section] 47-351.2(c), shall invest all other funds.*”

Per the Financial Institutions Deposit and Investment Act of 1997, Section 47-351.3, “*(d) The Mayor, or the CFO pursuant to [Section] 47-351.2(c), shall not allow the amount of District funds deposited or placed for the provision of financial services in a single eligible financial institution to exceed the lesser of either-*
(1) Twenty-five percent of the total assets of the eligible financial institution, exclusive of District funds; or

(2) Twenty-five percent of the total District funds available for deposit or investment as of the date of such deposit or placement and as of the end of each fiscal quarter thereafter.”

CAUSE

- The bank balances reported for each financial institution per the monthly Collateral Monitoring Worksheet are not updated consistently on a monthly basis to ensure the amount reported is current and materially accurate.
- Controls over the review and approval of the Beginning and End of Day Quick Reports did not detect the errors identified.
- The District implemented a policy to update the Financial Institution Total Assets values quarterly in July 2014. However, the policy was not in place for the entire year. Further, the District’s controls over review of the Cash Note reports did not detect the differences between the reports and the supporting documentation.

EFFECT

- The failure to accurately update to the Bank Balances reported per the Collateral Monitoring Worksheet could result in unidentified and uncorrected non-compliance with the Financial Institutions Deposit and Investment Act – Collateral and reporting requirements.
- The failure to accurately update the End of Day Quick Reports could result in excess funds not being invested.
- The failure to make accurate and timely updates to the Total Assets and Total Deposits values reported per the Cash Note reports could result in unidentified and uncorrected non-compliance with the Financial Institutions Deposits and Investment Act – General Deposit and Investment Requirements, and the District’s Investment Policy.

RECOMMENDATION

We recommend that the District continue to strengthen controls over the review of the:

- Collateral Monitoring Worksheets to ensure that they are completed at a sufficient level of precision to detect any differences between the supporting documentation and the worksheet;
- Beginning and End of Day Quick Reports to ensure that the Balance After Position is carried forward properly to the End of Day report; and

- Cash Note Reports to ensure that they are performed at a sufficient level of precision to detect any differences between the supporting documentation and the report.

MANAGEMENT'S RESPONSE

- Management concurs with the condition stated in #1 above, however we noted that in both instances noted in Condition #1, the principal balance was captured but not the monthly interest earned (\$31,535 total). In addition, both Premier Bank and Bank of Georgetown over-collateralized the District's funds to include the monthly interest earned. There was no actual risk to the District's funds.

The balance of \$40 million reported on the October 2013 Collateral Monitoring Worksheet for Bank of Georgetown did not include the interest earned amount of \$28,170. However, the financial institution did fully collateralize the District's funds at 112% (which included interest earned net of FDIC coverage of \$250,000). There was no risk to the District's funds. Going forward, the District will drawdown the interest earned from the money market account monthly to reflect the principal only at month end.

With respect to the citing of a \$3,365 difference, the principal amount of the certificate of deposit (CD) held at Premier Bank was reported on the February 2014 Collateral Monitoring Worksheet and not the interest earned. However, Premier Bank did fully collateralize the District's funds at 124% which included the interest earned net of FDIC coverage (\$250,000). There was no risk to the District's funds. Going forward, the District will reflect the interest earned from the CD at month end.

- Management concurs with the issues presented under Condition #2. This condition was identified and reported during the interim audit conducted as of June 30, 2014. The cash management unit updated the beginning and end of day reports. In the process of updating the functionality of these reports the formula used to bring over the beginning day balance to the end of day report was not functioning properly. The formula has been updated and an additional verification formula has been added to the End of Day worksheet.
- Management concurs with the issues presented under Condition #3.
 - a. This condition was noted by the auditors during the interim audit conducted as of June 30, 2014. The cash management unit has implemented a procedure whereby they will update total asset values on a monthly basis for most money funds and financial institutions. For the institutions that do

not provide monthly data, the team will update quarterly and place the support in the month end folder. The procedure has been updated to reflect this update. Also, the team has implemented a procedure whereby the month end reconciliation data that is used to update the account balances in the Cash Note will also be placed in the month end folder. The procedure has been updated to reflect this update.

- b. This condition was noted by the auditors during the interim audit conducted as of June 30, 2014. The team will collect daily and monthly data for the respective accounts and consolidate this data by month in the month end folder. The procedure has been updated to reflect this update.
- c. This was caused by a formulaic error when entering the total balance information. There was not increased risk that instances of non-compliance may not be detected as the error was on the side of caution; it inflated the percentage of DC's deposits as a percentage of the Financial Institution's assets. The team has restructured the report and implemented a review process to check on a monthly basis that the formulas are calculating correctly.

b. Improve Internal Controls over Bank Account Management

CONDITION

During our fiscal year (FY) 2014 testwork over the bank account management process, we noted that the District has begun a clean-up effort to remove all invalid Bank IDs (BIDs) and related balances from the general ledger, and to improve timeliness of cash account reconciliations to address our prior year finding. However, the remediation effort was not fully completed during FY 2014, and the following conditions were identified:

1. Controls over monthly cash and investment account reconciliations were not fully effective during FY 2014. Specifically:
 - For 5 of 40 interim reconciliations tested, the reconciliation was not prepared and reviewed timely, within 45 days subsequent to the month-end general ledger close.
 - For 1 of 40 interim reconciliations tested, the reconciliation was not reviewed timely, within 45 days subsequent to the month-end close.
 - For 8 of 40 interim reconciliations tested, the reconciliations included reconciling items aged greater than 60 days from the date of the reconciliation. We inspected the following month's reconciliations and determined that for 3 of the 8 accounts, all aged reconciling items were not resolved by the following month.

- For 1 of 17 year-end reconciliations tested, we noted that the reconciliation was prepared on January 10, 2015 and reviewed on January 20, 2015. As such, the reconciliation was not prepared and reviewed timely, within 45 days subsequent to the District’s year-end close of November 16, 2014.
 - For 1 of 17 year-end reconciliations tested, we noted an account for the DC Public Charter School Board (DCPCSB) that had a year-end general ledger balance of \$(431,701). As the DCPCSB is not a District entity, the general ledger balance should have been zero.
 - We noted 2 BIDs that were listed as “Open” on the Office of Finance and Treasury’s (OFT) BID listing that were not included in the District’s general ledger, but had a confirmed balance of \$9,465 at year-end.
2. We noted that one of the District’s clearing accounts, the “blank” BID, contained outstanding balances amounting to approximately \$8.7 million as of September 30, 2014 that were not cleared by January 13, 2014 (100 days past the fiscal year-end). We noted the balance was comprised primarily of payroll clearing transactions.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

Per the Office of the Chief Financial Officer’s *Financial Policies and Procedures Manual*, Section 25201000.30 and 25201000.40:

- *“District Government Agencies must record all business activity by the 8th business day of the following month.*
- *Agencies must make the appropriate adjustment in the general ledger for reconciling items that are due to errors/omissions (such as failure to record a transaction on the District’s books) within 60 days of first appearing on the monthly bank reconciliation or within 60 days of account closure.*
- *The agency initiating the cash or investment transaction is responsible for accurately recording the transaction within 24 hours of the actual event.*
- *The Accounting Operations (AO) unit is responsible for performing cash reconciliations within 45 days following the close of the general ledger for the previous month. The Office of Finance and Treasury and the Agency Cluster Controllers are notified within 45 days following the close of the general ledger for the previous month of all reconciling items. If discrepancies are identified and determined to be due to errors/omissions (such as failure to record a transaction on the District’s books), then the reconciliation process is not complete until such time that the errors/omissions is corrected and reflected in the general ledger.”*

CAUSE

- District Agencies are not timely investigating and resolving reconciling items. Additionally, OFOS appears to lack sufficient authority to enforce controls that are in place to ensure that material reconciling items are resolved prior to the issuance of the District's financial statements.
- The District does not have sufficient policies and procedures in place to ensure reconciling items and other adjustments to properly report cash/investments are recorded to the appropriate BID, and that the balance of the suspense account is \$0 at fiscal year-end.

EFFECT

- Inadequate or untimely resolution of reconciling items between the bank and the general ledger could lead to misstatements of cash balances recorded in the financial statements and could increase the District's exposure to fraudulent bank account activity.
- The failure to resolve suspense account balances in a timely manner prevents the District from being able to properly reconcile the District's accounts by BID, which could result in misstatements in cash and investment balances at fiscal year-end.

RECOMMENDATION

We recommend that the District:

- Continue to improve its internal controls to ensure that reconciliations are prepared and reviewed within 45 days following the month-end close, and that all reconciling items are investigated and resolved within a 60 day time period. This includes making the required journal entries to correctly state the general ledger cash and investment balances; and
- Investigate cash and investment balances in the "blank" BID, and reclassify balances to the appropriate BID.

MANAGEMENT'S RESPONSE

Management concurs with the finding. Accounting Operations will continue to enforce the new cash reconciliation procedures with the agencies including meeting the appropriate deadlines. Accounting Operations will also work to eliminate the remaining balance in Bank ID# 999.

2. Disability Compensation

a. Improve Controls over Recording of Tort Claims

CONDITION

During our testwork over tort liabilities (general and auto), we noted that tort claims, related to fiscal year (FY) 2014, were not properly entered into the American Technical Systems (ATS), [the District's third-party claims administration system]. We noted that in FY 2014, tort claims account for \$6.3 million (approximately 5% of the District's total self-insurance liability). Specifically, we noted for 6 of the 30 general and auto tort liability claims tested, the claim amount per the underlying data files submitted to the District's consulting actuary, were incorrectly recorded, thus resulting in a \$380,569 understatement of the initial liability. We noted once the errors were brought to management's attention, they were corrected and the final liability was revised and properly stated as of September 30, 2014.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

The District's internal controls are not operating effectively to ensure that claims are accurately recorded and that data files submitted to the actuary for consideration in calculating the year-end liability related to disability compensation are complete and accurate.

EFFECT

Without adequate internal controls over the financial reporting process for tort liabilities, the reports submitted to the actuary for the calculation of the liability may not be properly prepared and/or reviewed to detect and correct errors in a timely manner.

RECOMMENDATION

We recommend that the District implement formalized policies over the tort liabilities financial reporting process to ensure that:

- Claims are appropriately included in ATS; and
- Claims data is reviewed and reconciled by management prior to submission for the annual actuarial valuation process.

Lastly, management should provide training on these policies to personnel responsible for performing these processes and also perform monitoring procedures to ensure adherence to these policies.

MANAGEMENT'S RESPONSE

Management concurs with finding as noted above.

3. Capital Assets

a. Conduct Physical Inventory of Personal Property Timely

CONDITION

Controls to properly account for personal property capital assets, through completion of a regularly conducted physical inventory count, were not fully designed and implemented for the current fiscal year. The District's policies and procedures require that the Office of the Chief Financial Officer (OCFO) conduct a biennial physical inventory. We noted that during the 4th quarter of FY 2014, a physical inventory was conducted; however, the inventory results were not finalized in time to be reflected in the District's FY 2014 governmental activities statement of financial position.

CRITERIA

According to GASB Statement No. 34 - *Basic Financial Statements—and Management's Discussion and Analysis—for State and Local Governments*, paragraph 19, “*capital assets include land, improvements to land, easements, buildings, building improvements, vehicles, machinery, equipment, works of art and historical treasures, infrastructure, and all other tangible or intangible assets that are used in operations and that have initial useful lives extending beyond a single reporting period. In compliance with GASB No. 34, Governments should report all capital assets, including infrastructure assets, in the government-wide statement of net assets and generally should report depreciation expense in the statement of activities.*”

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

Per the Office of the Chief Financial Officer *Financial Policies and Procedures Manual*, section 10302000.60:

“OFOS will conduct a physical inventory of personal property capital assets biennially (every 2 years) to ensure that adequate care is used in the control and accountability of District assets. The inventory will be conducted based upon the assets listed in FAS as of a given date.”

CAUSE

The personal property physical inventory results were not finalized in time to be reflected in the District’s FY 2014 governmental activities statement of financial position because the District agencies’ review of the inventory variance report was not completed until after the issuance of the District’s FY 2014 financial statements.

EFFECT

Failure to perform timely, periodic inventory counts could result in assets that are not properly identified, tracked and recorded to the general ledger which could result in a misstatement in the District’s capital asset balances.

RECOMMENDATION

We recommend the District enhance current Capital Asset processes to ensure procedures are implemented to include, but not be limited to the following:

- Proper identification, tracking and recording of capital assets to ensure that each inventory item is 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;
- Each inventory record should include an asset identification number, a location number, asset description, cost, fund information, and acquisition date; and
- A physical count should be performed at least annually and results timely finalized to ensure the inventory records and the financial statement balances are complete and accurate.

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

MANAGEMENT’S RESPONSE

Management concurs with the finding. The inventory variance report was not fully reconciled in time to facilitate the auditors review during the testing phase of the engagement. Agencies are reviewing the variances and will determine whether the report is accurate or not. We expect completion of this process by the end of

February 2015. Management would like to state that the inventory covered 68 of 69 agencies (98.6% completion) and that in 2015 we will again perform another inventory.

b. Improve Controls Over Lease Listing

CONDITION

Controls are not operating effectively to ensure that the lease footnote disclosure is complete and accurate based on a complete listing of leases, including new and amended leases in the current year, and that executed lease agreements are recorded timely.

During our testwork over current year lease expenditures and a sample of 14 new or amended operating leases totaling \$9.3 million in fiscal year 2014, we noted the following:

- 1 instance in which a lease amendment was not properly identified as a new amendment in the District's listing of operating and capital facility leases. Therefore, we noted that the District's lease listing is not complete.
- 1 instance in which the lease was signed in a prior fiscal year, but was not included in the District's lease disclosures until the current year.

We noted, however, that the errors identified above did not impact the classification of the leases in the District's financial statements.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

Per GASB Statement No. 62, *Codification of Accounting and Financial Reporting Guidance Contained in Pre-November 30, 1989*, paragraph 213:

“If at its inception a lease meets one or more of the following four criteria, the lease shall be classified as a capital lease by the lessee. Otherwise, it should be classified as an operating lease.

- a. *The lease transfers ownership of the property to the lessee by the end of the lease term*
- b. *The lease contains a bargain purchase option*
- c. *The lease term is equal to 75 percent or more of the estimated economic life of the leased property. However, if the beginning of the lease term falls within the last 25 percent of the total estimated economic life of the leased property,*

including earlier years of use, this criterion shall not be used for purposes of classifying the lease.

- d. *The present value at the beginning of the lease term of the minimum lease payments excluding that portion of the payments representing executor costs such as insurance, maintenance and taxes to be paid by the lessor, including any profit thereon, equals or exceeds 90 percent of the excess of the fair value of the leased property to the lessor at the inception of the lease over any related investment tax credit retained by and expected to be realized by the lessor.”*

CAUSE

The District’s internal controls over financial reporting for leases were not operating effectively to ensure that a complete listing of leases to support the lease footnote disclosure was properly maintained throughout the fiscal year and that executed lease agreements were recorded timely.

EFFECT

Without effective internal controls over the financial reporting process for leases, the lease footnote and related rent expenditures could not be reported completely and accurately.

RECOMMENDATION

We recommend that the District strengthen internal controls to ensure that the lease information reported with respect to the required classification criteria is complete and accurate. These policies should include but not be limited to the following:

- Maintaining complete and accurate records of all leases and amendments; and
- Performing detailed reviews of agency-submitted lease closing packages to ensure completeness and accuracy of the data and to ensure that all expenditures reported relates to current, active leases.

MANAGEMENT’S RESPONSE

Management concurs with the finding; however: a) the lease amendment was not identified as a new amendment because the lease extension was only for three months; b) the lease was not included in the previous year, as the rent commencement date did not occur until fiscal year 2014, although the lease was signed in fiscal year 2013. Please note there were no associated rent expenditures in fiscal year 2013. Currently, in order to further strengthen the internal controls over accounting and financial reporting for leases, the District Department of General Services is currently in the process of developing and implementing a new

database system that helps to track, monitor and report on all leases held by the District.

c. Improve Internal Controls over Construction in Progress (CIP) and Capital Assets

CONDITION

Background. As noted during the fiscal year 2013 financial statement audit, during fiscal year 2014, the District continued efforts to implement uniform District-wide policies and procedures related to recording and classification of capital expenditures and Construction-in-Progress (CIP) activity to ensure timely and accurate financial reporting of depreciable and non-depreciable assets in its government-wide financial statements. Specifically, during fiscal year 2014, the District implemented a database system, Capital Acquisition Booking System (CABS), to provide increased standardization, at the agency level, related to tracking and classifying capital outlay expenditures and support CIP activity. We noted that all District agencies, except those under the Human Support Services cluster, implemented the system as of September 1, 2014, with the expectation for full implementation at all agencies in FY 2015.

We noted, however, that during the current fiscal year, the process for agencies to report CIP activity to the Office of Financial Operations and Systems (OFOS) to facilitate recording in the District's Fixed Asset System (FAS) and general ledger System of Accounting and Reporting (SOAR), continued to be a highly manual process based on agency prepared schedules that are then manually summarized by OFOS utilizing various Microsoft Excel schedules.

Additionally, we found that the majority of capital asset activity continues to only be recorded in SOAR subsequent to year-end for external financial reporting purposes; agencies do not perform timely review and reporting of on-going capital asset activity during the fiscal year. We also found that OFOS lacks proper oversight and on-going monitoring controls to perform timely reviews and reconciliation of capital asset activity thus making the District more susceptible to errors and inconsistencies in financial reporting in the government-wide financial statements.

Current Year Findings

For the current period under audit, the District continues to have deficiencies in the design and implementation of controls related to capital assets.

Specifically related to recording depreciable assets in FAS, controls are not designed effectively in order to complete a timely review of capital asset additions in the FAS system and ensure accurate recording of depreciable assets. As a result of this deficiency, during our testwork over a sample of 25 projects tested as transfers to depreciable assets from CIP in the prior fiscal year and thus, added to FAS in the current year, we noted 2 instances in which projects totaling \$6.7 million identified as not complete as of September 30, 2013, were incorrectly added to FAS in FY 2014. However, we noted in the current year that these assets continue to be in-process and therefore should not be recorded as depreciable assets.

Further, summary schedules prepared by the agencies used by OFOS to accumulate and summarize agency-reported CIP data for financial reporting are not completed timely in order to facilitate a sufficient, detailed review of the activity prior to the schedules being provided for audit. Additionally, the agencies' reported CIP activities continued to only be reconciled to FAS and SOAR at fiscal year-end.

Additionally, as a result of these deficiencies, during our testwork over a sample of 9 projects totaling \$44.8 million transferred from CIP to depreciable assets during fiscal year 2014, and 23 projects totaling \$365.7 million remaining in the CIP as of September 30, 2014, we identified the following errors in the capital asset balances:

- Department of General Services (AM0) – 1 instance in which costs totaling \$12.7 million were incorrectly transferred from CIP to depreciable fixed assets, This was subsequently reclassified from depreciable fixed assets back to CIP subsequent to the project being sampled as part of the audit.
- Office of the Deputy Mayor for Planning and Economic Development (EB0) – 1 project in CIP with an ending balance \$5.4 million, which, based on project status confirmation from the agency, was completed in fiscal year 2011, but not transferred to fixed assets in FY 2014.
- Office of Special Education Transportation (ELC – GO0) – 1 project totaling \$2.9 million in which sufficient documentation to support the ending balance in CIP was not provided. We note, however, based on inspection of the expenditure detail for the project provided by the agency, we determined the project was completed in FY 2012 and thus should be transferred out of CIP.
- Department of Human Services (JA0) – 1 project in CIP with an ending balance of \$18.3 million, related to the Medicaid portion of the District of Columbia Access System (DCAS) that was placed in service on October 1, 2013, was not transferred to fixed assets in FY 2014.

Furthermore, we noted that based on our prior year recommendation, during FY 2014, the District continued remediation efforts over capital asset activity which resulted in the identification of an additional \$22 million in CIP that was transferred to In-Service in FY 2014 that should have been transferred in a prior year.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

According to GASB Statement No. 34, paragraph 19, “*capital assets include land, improvements to land, easements, buildings, building improvements, vehicles, machinery, equipment, works of art and historical treasures, infrastructure, and all other tangible or intangible assets that are used in operations and that have initial useful lives extending beyond a single reporting period. In compliance with GASB No. 34, governments should report all capital assets, including infrastructure assets, in the government-wide statement of net assets and generally should report depreciation expense in the statement of activities.*”

CAUSE

The District has not fully implemented sufficient policies and procedures and related controls, at the agency level, to ensure that costs transferred from CIP are tracked on a project level and that the amounts transferred to depreciable capital assets and costs remaining in CIP are properly supported. Furthermore, the District lacks sufficient processes regarding proper oversight over capital asset financial reporting to ensure complete, accurate, and timely recording of capital assets in the general ledger and FAS.

EFFECT

Without effectively designed and implemented internal controls over the financial reporting process for capital assets, misstatements in capital asset balances may not be prevented or detected in a timely manner. As a result of the findings above, we noted the following uncorrected misstatements to depreciable and non-depreciable assets (in millions):

Financial Statement Line Item	Misstatements		
	Over	Under	Net
Depreciable Fixed Assets	\$6.7	\$(26.6)	\$(19.9)
Construction-in-Progress	\$26.6	\$(6.7)	\$19.9

We noted that management properly recorded the \$22 million of additions to depreciable assets and the \$12.7 million reclassification between depreciable and non-depreciable assets in the government-wide financial statements as of September 30, 2014.

RECOMMENDATION

We recommend that the District strengthen their internal controls over the financial reporting process for capital assets to ensure that capital asset balances are complete and accurate as of the fiscal year-end. This should include, but not be limited to the following:

- Continuing reinforcement and implementation of established District-wide policies and procedures for identifying completed capital projects to ensure that projects are transferred from CIP to depreciable capital assets in the period in which the assets are placed in service.
- Continuing reinforcement and implementation of the established District-wide policies and procedures for identifying capital project expenditures that are non-capital in nature and ensuring such expenditures are expensed in the period incurred.
- Continuing to provide training to District agencies regarding established policies and procedures and the recently implemented CIP database to reinforce appropriate processes and documentation to support determination of classification of capital expenditures and capital project status to ensure timely transfer of completed projects to depreciable capital assets.
- Adhering to existing internal control procedures for the review and approval of agency-reported closing package information to ensure that the closing packages are submitted timely by the agencies and that the reported capital asset data is complete and accurate.
- Maintaining appropriate supporting documentation for all capital expenditures, transfers from CIP to depreciable capital assets, and real and personal property additions and disposals.
- Reinforcing policies and procedures that require management review of entries to record real property assets in FAS, and make corrections as necessary.
- Performing reconciliations of real property balances in SOAR and FAS timely during the fiscal year, rather than after the end of the fiscal year.

We also continue to strongly encourage the District to implement a centralized capital project accounting system that is fully integrated with the District's general ledger that allows capital asset transactions to be tracked at an invoice and project level.

MANAGEMENT'S RESPONSE

Management concurs with the finding, however, the following agencies responded with additional detail:

Office of the CFO:

As of September 30, 2014, the District manages more than \$1.1 billion in net capital assets. The findings as noted by the auditors do not have a material impact on the District's FY 2014 financial statements being that the net adjustment to total Capital Asset is zero. All of the proposed adjustments are reclassifications between different Capital Asset categories. The total Capital Asset balance reported in the District's FY 2014 annual financial statements is accurate.

The District is fully aware of the deficiencies in our aging financial system and is in the process of replacing it with a new system. During the interim, we have implemented compensating measures in an effort to strengthen internal controls. During FY 2014, we revised our Policies and Procedures related to accounting for and reporting on capital assets.. We hired three additional capital asset accountants at OFOS and poured additional resources into educating accountants at the agency level. We also performed interim CIP testing to proactively identify and correct potential problems. The results have been positive. As noted, \$22 million in CIP was identified by the District and properly transferred to in-service during the fiscal year.

The Capital Acquisition Booking System (CABS), mentioned in this report will be fully implemented in FY2015. The system will improve the Capital Asset reporting process for the District because it requires that capital expenditures be analyzed throughout the fiscal year instead of only during the closing process.

Department of General Services (AMO):

We concur with the auditor's finding related to Agency AMO, Department of General Services (DGS). However, DGS management believes the internal controls over capital asset accounting and financial reporting are adequate, because the finding is an isolated incident. DGS managed 187 projects, which includes 431 locations during FY 2014. The audit finding merely represents .5% of total projects managed during FY 2014, .2% of total locations on which capital funding was

expended during FY 2014, 2.7% of the FY 2014 total capital expenditures, and 2% of the total balance of CIP before transfer of completed projects. Additionally, the net effect on depreciation is \$64,000, as the project was substantially complete and occupied in December 2014.

Office of the Deputy Mayor for Planning and Economic Development (EB0):

The project related to the Office of the Deputy Mayor for Planning and Economic Development which is discussed in EB0 the reported condition is related to land improvements associated with the SW Development and Fish Market, which is currently under development, and in anticipation of additional funding and expenditures on the project development, it was assumed that the reclassification from CIP to fixed assets would be done upon the project completion. We will continue to work closely with Project Managers to obtain project completion status and ensure that capital expenditures for completed projects are reclassified from CIP to capital assets in a timely manner.

Office of Special Education Transportation (ELC - GOO):

The expenditures related to this project were transferred out of CIP in January 2015 and the agency has instituted a quarterly review and reconciliation of all CIP balances that will proactively ensure that all appropriate transfers for completed projects from CIP to fixed assets occurs on a timely basis.

4. Grants Management

a. Clean Up Grant Receivable Accounts

CONDITION

In 2008, the District created the Federal and Private Resources Fund (GAAP Fund 400) and posted manual journal entries to reclassify grant receivable account balances from the General Fund (GAAP Fund 100) to GAAP Fund 400. At the time that these transfers were made, the District established temporary grant receivable accounts, referred to as “Dummy Accounts” in the GAAP Funds 100 and 400 to record the transfers.

During our FY 2014 audit, we noted that the District has not implemented sufficient processes to ensure that, at a grant receivable account level within the applicable GAAP funds, grant receivable account balances are properly presented as a result of the reclassification journal entry noted above. Specifically, as part of our testwork over Due From Federal Government we sampled the transactions underlying GAAP Fund 400 grant receivable accounts 71MMD and DUMMY1 outstanding receivable balances and noted that four (4) of the transactions sampled

pertain to 2008 reclassification entries. Based on the sampled transactions, we determined that the grant receivable account balances are presented as unreconciled AR transactions within GAAP Funds 100 and 400.

Specifically, we noted that the amounts represent unreconciled GAAP 400 debit transactions within the specific grant receivable account (e.g., 61MMMD) and the offsetting credit transactions are in the "DUMMY1" grant receivable account; a grant receivable account that was established for posting adjustments. Additionally, we noted the opposite scenario in GAAP Fund 100.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

There is no process in place for the District agencies involved to reclassify the offsetting transactions from the "DUMMY1" grant account receivable to the actual grant account receivable to bring the ending grant accounts receivable balance in these dormant grant account receivable accounts to \$0.

EFFECT

There is no effect at the financial statement level as the offsetting debits and credit related to these transfers net to zero in both GAAP Funds 100 and 400, respectively. However, continuing to maintain these old grant receivable accounts increases the risk for journal entries to be inadvertently posted to these accounts and not be detected.

RECOMMENDATION

We recommend that the district perform a reconciliation and review of all outstanding grants receivable account balances within GAAP Funds 100 and 400 to ensure receivable amounts are properly closed out and presented. The District should reclassify offsetting transactions resulting from the 2008 journal entries in the "DUMMY1" grant receivable account to the respective grant receivable account to bring the ending balances to \$0.

MANAGEMENT'S RESPONSE

No Management Response was provided.

5. Loans Receivable

a. Improve Controls over the Completeness and Accuracy of Loan Activity

CONDITION

The District issues affordable housing loans to borrowers under various local and federally supported programs. Loan principal balances and related allowance for doubtful loan collections are recorded annually based on a reconciliation of the loan balances per Department of Housing and Community Development (DHCD)'s records and the loan balances per the third party loan servicer, AmeriNational Community Services (ACS). The District lacks appropriate policies and procedures to ensure that loans are timely recorded in the financial statements within the Housing Production Trust Fund (HPTF), the General Fund, and the Federal and Private Resources Fund (FPRF).

Specifically, during our testwork over a sample of 25 new loans totaling \$9,783,816 recorded by ACS in FY 2014, we noted that 4 of the loans amounting to \$9,155,043 were disbursed prior to FY 2014 and as such were not recorded on each funds balance sheet in the proper fiscal year.

Additionally, based on an analysis performed by DHCD of all FY 2014 loan expenditures in the HPTF, General and FPRF funds, we noted an additional \$9,944,298, \$215,997 and \$1,593,225, respectively, of new loans that were disbursed in FY 2014, were not recorded in the loans receivable and corresponding allowance for doubtful loan collection balances as of September 30, 2014. However, we noted there was no financial statement impact as these loans are reserved 100%.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

The District has not developed sufficient policies and procedures to ensure that loans are recorded completely and accurately in the funds' general ledger and financial statements and to ensure that new loans are submitted timely to the loan servicer, AmeriNational Community Services, for recordation.

EFFECT

Without effectively designed and implemented internal controls over the recordation process for loans receivable, misstatements may exist in the other long term assets, allowance for doubtful loan collections, and unavailable revenue general ledger and financial statement balances.

RECOMMENDATION

We recommend the District improve current policies and procedures related to the recordation of loans receivable and the related allowance to ensure that loan disbursements and the associated receivables and unavailable revenue balances are properly recorded and reflected in the correct accounting period in the general ledger and financial statements.

MANAGEMENT'S RESPONSE

Management concurs that loans were not timely recorded in the financial statements. DHCD's current post closing administrative instructions describe in detail the required process and procedures for the transmission of loans to the receiver. However, we will take the auditors' recommendations with respect to enhancing policies and procedures under advisement. Accordingly, we will review existing policies and procedures and revise them as deemed necessary and appropriate.

KPMG'S RESPONSE

We have reviewed management's response and our finding remains as noted above.

b. Lack of Retrospective Analysis over Significant Estimates

CONDITION

During our testwork over other long term assets and the related estimate for the allowance for doubtful accounts, we noted the District of Columbia (the District) does not perform a retrospective "look-back" analysis to determine whether the assumptions used in determining the estimate are reasonable. Additionally, management does not have a process in place to review the outcome of accounting estimates included in the prior period financial statements or their subsequent re-estimation for the purpose of the current period.

CRITERA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

The District does not have a process in place to conduct a retrospective "look-back" analysis in order to evaluate the reasonableness of the estimate for the allowance for doubtful accounts.

EFFECT

Failure to perform a retrospective "look-back" analysis of the estimate for the allowance for doubtful accounts could result in misstatements in the financial statements.

RECOMMENDATION

We recommend that the District refine its methodology for estimating the allowance for doubtful accounts to include a retrospective "look-back" analysis in order to evaluate the reasonableness of the methodology.

MANAGEMENT'S RESPONSE

Management concurs with the finding and recommendation of the auditors. We have performed a five year "look back" analysis on the amortized loan population that is based on the total number and outstanding balance of delinquent loans vs. the total number and outstanding balance of amortized loans; however, as recommended, we will work with our loan servicer, AmeriNational, to obtain repayment information, namely, repayments received vs. repayments due, to enable us to perform a more thorough retrospective "look-back" analysis to evaluate the reasonableness of the allowance estimate.

6. Revenue

a. Accelerate Timing of Retrospective Analysis of Estimated Refunds Payable

CONDITION

During our testing of the reasonableness of the District's estimated refunds payable accrual for individual income taxes, we noted management did not perform a timely retrospective review of the prior years' estimated refunds payable liability (performed on January 14, 2015) before their current year calculation of the FY

2014 estimated refund liability. This retrospective review is used to determine the reasonableness and appropriateness of the methodology used to estimate the liability and should be completed before the current year estimate is calculated and recorded to the financial statements. Specifically, management's review identified that the known FY 2012 and FY 2013 estimated refunds payable was over accrued by \$16.123 million and \$15.305 million, respectively. However, as the review was not performed timely, management did not adjust for this in their current year calculation thus potentially overstating the FY 2014 estimated refunds payable by approximately \$19.960 million.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

The District's current policies and procedures for estimating refunds payable do not contain a formal process for reviewing estimated refunds payable against actual refund payments data for accuracy prior to the current year calculation.

EFFECT

Lack of formalized policies and procedures to retrospectively review the accuracy of the accrual could result in incorrect assumptions and considerations being used to estimate the liability, thus resulting in a potential misstatement in the liability.

RECOMMENDATION

We recommend that the District:

- Implement a requirement in its current annual review process to ensure that the retrospective analysis is performed before the current year estimate is recorded to allow for any adjustments that need to be considered for the current year; and
- Perform the retrospective review over five years of data in order to provide a more accurate analysis.

MANAGEMENT'S RESPONSE

Management agrees that the retrospective analysis was done late in the process. Because the methodology for developing the estimate is a legacy practice, during the review there were improvements to the process that were identified. During the

initial phase of revising the methodology, 3 years of actual data will be used. Future retrospective reviews will add one year of data to record, until a 5 year repository of data is available.

b. Improve Process and Controls over Estimating the Real Property Tax Appeals Claims Liability

CONDITION

The District relied upon an improperly compiled report to calculate its estimate of settlement payments from Real Property Tax Appeals claims. Specifically KPMG noted two of twenty-five cases sampled were considered to be “pending” per the report; however, these cases were “closed” as of September 30, 2014 according to the records of the DC Superior Court and shouldn’t have been included in the calculation.

In addition, while an informal review of the prior year accrual is performed, there is no formal retrospective review performed of the prior year liability estimate by the District to ensure that the methodology used to accrue for the contingent liability is reasonable.

CRITERIA

Governmental Accounting Standards Board Codification C50.150 states:

*“State and local governments are subject to many types of claims. Subject to the accounting and financial reporting distinctions of governmental funds, the criteria of paragraphs .151-.168, should be the guidelines for recognizing a loss liability resulting from all claims that result from actions not included in the scope of paragraphs .109-.148 of this section. (See paragraphs .101 and .102.) Those claims include contractual actions, such as claims for delays or inadequate specification on contracts, or for guarantees of the indebtedness of others that are not investment derivative instruments entered into primarily for the purpose of obtaining income or profit, **property tax appeals**, and unemployment compensation claims.”*

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

The District recorded an accrual entry based on pending case information without evaluating the completeness and accuracy of the information. In addition, no retrospective review or look-back analysis was performed to ensure that the methodology used in the prior year was reasonable.

EFFECT

Without performing a review of the case listing prior to the calculation of the accrual, incorrect information can be used to calculate the accrual resulting in a misstatement. Specifically, as of September 30, 2014, the accrual was overstated by \$174 thousand. Additionally, the lack of formalized policies and procedures to retrospectively review the accuracy of the accrual could result in incorrect assumptions and considerations being used to estimate the liability.

RECOMMENDATION

We recommend that the District continue to refine the information used in the estimate by coordinating with the Office of Tax Revenue, the Office of the Attorney General, and the DC Court of Appeals to determine an accurate number of “pending” cases as of the end of the fiscal year. In addition, we recommend that the District perform a formal retrospective review of the methodology used to ensure that it is appropriate based on known actual amounts from prior years to improve the accuracy of the accrual.

MANAGEMENT’S RESPONSE

OTR recognizes the risks associated with overstating year-end accrual estimates related to outstanding claims and judgments in the District’s government-wide financial statements. OTR concurs with the facts of the cause, effect and condition.

The Real Property Tax, Assessment Division on a monthly basis will compare court order petitions against the Superior Court website to determine an accurate number of pending cases.

The Appeals and Litigation Supervisor will perform a formal retrospective review of the methodology used to ensure that it is appropriately based on known actual amounts from prior years utilizing a historical database (Excel) of 3rd level settlements.

- c. **Implement a Process for Reviewing Third-Party Information being Relied Upon to Record Other Revenue Accrual Estimate and Related SSAE 16 Report**

CONDITION

During our FY 2014 testwork over receivables we noted that management does not have a formal process in place to verify the completeness and accuracy of

information provided by a third party for receivable accruals related to parking, camera, and moving violations. The District relied upon the third-party service provider's collections report to estimate receivables at September 30, 2014, without appropriately verifying the information in the reports, possibly overstating accounts receivable and related revenues by \$20,345,690 and overstating long-term accounts receivable and deferred inflow of resources – other by \$57,895,421. The District also failed to obtain and review a current SSAE 16 report covering the fiscal year from the third-party service provider to aid in evaluating the reliability of the information included in the third party collections report.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

The District's current policies and procedures for estimating their receivables accrual for parking, camera, and moving violations do not contain an appropriate amount of precision to verify the completeness and accuracy of the third party data from Duncan Solutions.

EFFECT

Lack of formalized policies and procedures for verifying inputs into a receivable accrual estimate calculation could result in incorrect assumptions and considerations being used to estimate the receivable, thus resulting in a potential misstatement in current and long-term receivables, deferred inflows, and revenue.

RECOMMENDATION

We recommend that the District implement a process for reviewing third party information that is used in their estimates by coordinating with the third party vendor to verify that the information on which they are relying is complete and accurate. In addition, we recommend that the District perform a review of the third party SSAE 16 report that is applicable for the entire fiscal year and implement potential user control procedures.

MANAGEMENT'S RESPONSE

Management concurs with the finding. The Central Collections Unit (CCU) was legislatively established in 2012. The operations began with CCU assuming existing contractual terms and conditions in effect for the prior 5 years. A data management

system needed to be acquired to support the debt management/receivable validation. Unfortunately, CCU is still implementing this essential infrastructure.

To address the establishment of a review process of third party information, CCU will begin to require receipt of a weekly acknowledgment report for new debt placements from both the system of record and the collection contractor. A CCU employee will be assigned to review and reconcile both acknowledgment reports and immediately resolve discrepancies. Going forward, this will allow a validation of the data as accurate and complete as it is placed for collection. When the data management system becomes operational, a third level of validation of data receipt will be performed. CCU will also document the above-stated procedure and incorporate the year-end accrual process.

It must also be noted that the CCU provided KPMG with the calendar year 2013 SSAE 16 report and comfort letter for the gap period. The vendor's auditors will complete the 2014 SSAE 16 report and deliver it in March 2015. CCU will award its new collection contract(s) in March, 2015 and require the SSAE 16 report to conform to the District's fiscal year and not the calendar year. CCU will perform an annual test of the user control procedures for compliance.

d. Improve Controls over Real Property Tax Receivable Accrual Process

CONDITION

During our review of the real property tax receivable we noted that management did not have adequate processes, procedures and internal controls in place to ensure completeness and accuracy of the gross taxes receivable population prior to estimation of the year-end accrual and recordation to the financial statements. During our testwork over net taxes receivable, we identified four exceptions related to the following:

- For one of 17 sampled items tested, we noted that the property was incorrectly assessed as a taxable entity and should have had tax exempt status for FY 2014. The property was obtained after the resident died and his property transferred to the District. At that time the taxes receivable balance should have been removed from the District's financial statements. The impact of this error was a \$142,712 overstatement in taxes receivable.
- For 2 of 17 sampled items tested, we noted that there were collections on the taxes owed to the District that were received and recorded in September 2014. However, the closing module within the Tax Administration System (ITS) did not properly reduce the real property tax receivable balance for each collection received in September 2014 for these two sampled items. The financial impact of these two errors is an overstatement of gross real property tax accounts receivable of \$4,302,216.

- For 1 of 17 samples tested, we noted that the taxpayer received an adjustment to their property tax bill after the initial second half bill had been issued. This change was not captured in the closing module of ITS. The impact on gross real property tax accounts receivable for this exception is an overstatement of \$109,361.

As a result of the above exceptions, management performed an analysis of the gross real property tax accounts receivable population reported on the Revenue Lead Sheet (RLS) as of September 30, 2014 and determined that the above-noted exceptions were caused by errors in the closing module within ITS, specific to real property tax accounts receivable. As a result management's analysis, it was noted that the District's closing module was not properly accounting for the following when calculating the gross real property tax accounts receivable as of September 30, 2014:

- Second half tax bills that had corrected bills or payments after the second half bills were issued were not captured in the closing module. The impact of this error resulted in a net overstatement of gross real property taxes accounts receivable of \$1,837,062.
- Second half bills that received extended due dates with a \$0 balance per ITS as of September 30, 2014, were not captured in the closing module. The impact of this error resulted in a net overstatement of gross real property tax accounts receivable of \$1,610,753.
- Second half bills that received extended due dates and had a balance per ITS as of September 30, 2014, were not captured in the closing module. The impact of this error on accounts receivable was a net overstatement of \$503,386.

The net impact on gross real property tax accounts receivable as of September 30, 2014, is a net overstatement of \$3,951,201. This net overstatement includes the effect of the four exceptions noted in the condition above.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

Management did not have adequate controls designed and implemented to ensure completeness and accuracy of the data used to calculate the gross real property tax accounts receivable balance used in the RLS as of September 30, 2014. Specifically, management did not ensure the logic applied in the ITS closing module was

appropriate, such that the closing report would generate a complete and accurate gross real property tax accounts receivable balance as of September 30, 2014.

EFFECT

As a result of this control deficiency, gross real property tax accounts receivable and unavailable revenues of the General Fund were overstated by \$3,951,201 as of September 30, 2014. There was no financial impact on the allowance for doubtful accounts as the allowance is calculated based on the amount of taxes levied.

RECOMMENDATION

We recommend that the District develop processes and procedures and strengthen its internal controls to address the system limitations of the closing module within ITS. Specifically, we recommend that the District perform an annual analysis of the known amount of the discrepancy caused by the existing ITS closing module and evaluate the financial statement impact each year.

MANAGEMENT'S RESPONSE

OTR concurs that an error was detected in the closing report that resulted in the exclusion of certain real property transactions with second half due dates after September 30th, because the closing program was designed to apply the same logic applicable to self-assessed taxes to real property, a billed tax requiring different treatment under Governmental GAAP. OTR will explore several solutions to correct the process, including modifying the closing program itself, reviewing the application of extended due dates for real property accounts, and subjecting real property accounts receivable to additional review and sampling prior to inclusion in the revenue lead sheet. As a final detective control, OTR will perform additional analysis with regard to properties with bill due dates after the closing date, to ensure that the gross accounts receivable is properly stated. OTR notes that the error was fully mitigated by the conservative allowance reserves for real property accounts receivable in the amount of \$107 million. There was no impact on the financial results due to the finding.

7. Payroll

a. Improve Controls over Compliance with Timesheet Approver Requirements

CONDITION

During our testing over timesheet approvers, the Office of Pay and Retirement Services was unable to provide sufficient documentation, such as the confirmation of completion code, to evidence that authorized timesheet approvers had completed

the required Time and Labor Approver training prior to approval of timesheets in FY 2014. Specifically, 23 of 25 timesheet approvers selected for test work did not appear to have completed the required training.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

Per the District’s policy, *TL [Time and Labor] Approver Training*, “All approvers at the District **MUST** review the time approval lesson. You may review either the tutorial or the video (if available) for each lesson.”

Additionally, “At the end of the lesson, you will be given a **MANDATORY CONFIRMATION OF COMPLETION CODE** to validate that you have participated and completed training. Notification will then be sent to your agency’s representative outlining the date and time of the class that you have completed.”

CAUSE

There was a lack of enforcement of the District’s established internal controls to ensure proper review and approval of timesheets, specifically regarding timesheet approver requirements.

EFFECT

Inappropriate or improper review of timesheets increases the likelihood that errors in submitted timesheets (which could be pay-impacting) are not identified and corrected.

RECOMMENDATION

We recommend that the District adhere to its policies and procedures for Timesheet Approver training.

MANAGEMENT’S RESPONSE

While the District could not produce a certificate or other document to physically validate that Time & Labor (T & L) approver training was completed by the individuals in the sample, this does not mean that the T&L training was not provided to the individuals. In some cases, if individuals viewed the on-line training but did not complete the survey, the database did not capture the training. In other cases, individuals are taught through on-the-job training (OJT), and many in the

sample have been with the District for quite some time, before and during the PeopleSoft implementation when training was provided throughout the District. These persons are keenly aware of the T & L approver tasks.

However, the District will review its current policy and procedures for T & L approver training and within the parameters of available technology and resources, address T & L approver training.

b. Strengthen Management Review of Compensation Payable Accrual Journal Entries

CONDITION

During our testing of compensation payable, we noted the prior year accrual was not fully reversed out, thus resulting in an overstatement of the Compensation Payable and Personnel Service balances at September 30, 2014, of \$17,281,260. Of the total overstatement, \$6,261,076 is related to the General Fund and \$11,020,183 is related to the Federal and Private Resources Fund.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

Controls are not properly designed and implemented to ensure that the prior year accrual is fully reversed out when the general ledger is opened for the new fiscal year. Additionally, reviews over the current year accrual were not effective in identifying the issue.

EFFECT

The General Fund balance of Compensation Payable and Personnel Services was overstated by \$6,261,076 at September 30, 2014.

The Federal and Private Resources Fund balance of Compensation Payable and Personnel Services was overstated by \$11,020,183 at September 30, 2014.

RECOMMENDATION

We recommend that the District implement management review controls over journal entries to include reconciling the current year estimated payroll accrual to

the amount recorded in the General Ledger, such that discrepancies are researched and resolved.

MANAGEMENT’S RESPONSE

Management concurs that there was an unreconciled difference between the GL and the supporting documentation provided for review. The finding states that an overstatement occurred because the reversal of the FY2013 accrual was incorrect. The overstatement was determined by comparing the year-end payroll accrual computed through PeopleSoft using the last pay period for each pay group with the general ledger balance as recorded in SOAR at September 30, 2014. An analysis of GL 1207 indicated that agencies also made manual entries in FY 2014 to account for special payroll items (i.e. retroactive back pay, labor grievances, etc.) that also resulted in a liability being recorded. The entries made by the agencies also contributed to the apparent discrepancy/variance noted by the auditors.

KPMG’S RESPONSE

We have reviewed management’s response and our finding remains as noted above.

8. Financial Reporting

a. Strengthen Management Review of Grant Budget Modifications Entered into SOAR

CONDITION

During our control testing over the grant budget modification process, we noted that for 1 of 20 sampled items tested, the incorrect grant phase was included on the modification that was submitted to the District Council for approval. Specifically, we noted the grant budget modification submitted to the Council for approval indicated a grant phase of “2013”; however, the grant phase entered into the general ledger, SOAR, was “2014”. As a result of our testwork, the Office of Budget and Planning sent a revised modification to the Council for subsequent approval.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

Management did not have proper internal controls in place to ensure that grant budget modification requests sent to the District Council were complete and accurate.

EFFECT

Erroneous or incorrect budget authority may be established for the Agency and improperly recorded in the general ledger system.

RECOMMENDATION

We recommend that the District strengthen policies and procedures to ensure that modifications reviewed and approved by the District Council agree to supporting documentation and are correctly entered in the District's general ledger system.

MANAGEMENT'S RESPONSE

Management concurs with the finding, however we believe that we maintain the proper internal controls to ensure that grant budget modification requests sent to the District Council are complete and accurate.

Periodically, administrative errors may be noted in the information submitted to the Council, for which the corrective action in place is the technical correction process. This process is managed solely within the Office of Budget and Planning, in accordance with District's Home Rule Act and does not require resubmission to the District's Council, as these are administrative changes.

Additionally, the Grant Budget Modification reconciliation process, which is also conducted by OBP staff annually from August 1st to September 30th, involves a detailed review of all administrative and passive grant approvals to ensure that the information is accurately recorded and reported. It should also be noted that while the administrative error cited was discovered by the auditors during preliminary testing, management affirms that OBP's reconciliation and technical correction processes would have detected and corrected the error prior to the closing of the fiscal year.

KPMG'S RESPONSE

We have reviewed management's response and our finding remains as noted above.

9. Information Technology

a. PASS Developer Lack of Segregation of Duties

CONDITION

During FY 2013 testing, it was determined that four individuals with access to migrate changes to production in the Procurement Automated Support System

(PASS) also possessed development responsibilities. Although, procedurally, these individuals were not responsible for migrating their own changes to production, they possessed the logical access to do so and there were no other monitoring or detective controls in place that would have identified whether an individual migrated their own change. Therefore, this represented a weakness in the control environment that persisted into the first quarter of FY 2014.

In December 2013, the Phire change management system was implemented for PASS and systematically enforced segregation of duties between those individuals with development responsibilities and those individuals responsible for migrating changes to production in remediation of this finding. However, a deficiency in the control environment existed from October through December 2013.

CRITERIA

Our internal framework for identifying and testing General Information Technology Controls (GITCs) can be mapped to several commonly accepted information technology risk and control frameworks including those published by the National Institute of Standards and Technology (NIST), Information Systems Audit and Control Association (ISACA), and the International Standards Organization (ISO). For purposes of our reporting of findings for the District of Columbia Government, we have provided below relevant criteria.

The Federal Information Security Management Act (FISMA), passed as part of the Electronic Government Act of 2002, mandates that Federal entities maintain IT security programs in accordance with NIST. The following NIST criteria were considered:

- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995;
- NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009;
- NIST SP 800-64, Security Considerations in the System Development Life Cycle, October 2008; and
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology, September 1996.

The Information Systems Audit Control Association (ISACA) Control Objectives for Information and Related Technology (COBIT®) 4.1, 2007.

CAUSE

Based on a consideration of priorities and limited resources, management had not allocated the resources required to develop and implement controls that mitigate the

risks associated with the condition including, but not limited to, the segregation of program development roles from production administration roles among different individuals and/or other mitigating controls such as monitoring the activities of the individuals with database administrative level access.

EFFECT

For the period of time noted in the condition above, the lack of segregation of duties increased the risk that developers could create and apply changes to the PASS production application outside of defined change management processes that adversely impact application programs and data.

RECOMMENDATION

This issue was remediated in December 2013 and found to be effectively operating for the remainder of FY 2014. Therefore, we recommend that management continue to enforce the logical segregation of duties within the change management process implemented in remediation of the finding above.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

b. Control Deficiencies in UNIX Administration on PeopleSoft and PASS Servers

CONDITION

We noted that the following deficiencies related to users with UNIX/Linux administration privileges on the PeopleSoft and PASS servers continued to exist for a period of time during FY 2014 as described below:

- Direct root login via SSH connections on the PeopleSoft Linux servers was allowed through November 2013.
- At least one of three generic login accounts on four PASS servers and three PeopleSoft servers retained root privileges through February 2014.

While KPMG deemed the items above to be remediated at the points in time noted above, deficiencies existed in the control environment until the time of remediation within FY 2014.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Due to a lack of documented procedures to outline minimum required security settings for servers under the purview of the Enterprise Cloud Infrastructure Services (ECIS) team, the setting to disable direct login to the 'root' account via remote mechanisms was not configured consistently on all in-scope servers.

Additionally, in August 2013, management implemented the three generic accounts noted in the last bullet of the finding above to ensure accounts were available to the ECIS team to perform administrative functions in cases in which individual accounts had not been configured on the servers and to prevent the need to establish and revoke accounts as turnover on this team occurred. However, upon further consideration of the risk associated with these accounts, management replaced them with unique accounts in February 2014.

EFFECT

For the period of time noted in the condition above, the lack of configured settings to require the execution of the switch user or SUDO commands to access 'root' privileges as well as the presence of shared accounts with 'root' privileges could have negatively impacted management's ability to monitor and identify the specific individual performing the activities with these administrative privileges. This could have resulted in unauthorized activity occurring and not being detected.

RECOMMENDATION

This issue was remediated in February 2014 and found to be effectively operating for the remainder of FY 2014. In order to sustain the consistent operation of the controls implemented, we recommend that management document minimum required security settings and access governance protocols for all critical enterprise servers. The suggested document should, at a minimum, include the following:

- Procedures to manage how new accounts are approved prior to creation, periodically reviewed to ensure that the access held by accounts remains restricted to least privilege, and terminated in a timely manner when no longer required to hold access,
- Requirements that strong passwords be enforced for all accounts and compensating controls (such as password rotation or vaulting) be in place to address cases where password expiration and/or account lockout cannot be systematically enforced,
- Requirements that individual accounts be utilized when possible and that system accounts are restricted from being accessed directly when feasible, and

- Procedures to monitor privileged account activity such as reviews of “switch-user” activity on Linux environments.

MANAGEMENT’S RESPONSE

Management concurs with the finding.

c. Deficiencies in PASS Application Access Review

CONDITION

In FY 2013, it was determined that the periodic review of access for the PASS application had been enhanced from an annual review to a semi-annual review. The new semi-annual review focused on the individuals granted the Invoice Manager role, which allowed access to approve invoices for payment. At that time, it was determined that the review did not cover certain critical access rights, including the ability to approve purchase requisitions, set-up new vendors, and modify goods received within PASS.

The first periodic access review in FY 2014, performed in March 2014, was modified to include individuals with access to receive goods on behalf of the District. The second review performed in September 2014 was further enhanced to include access rights to set up new vendors (SOAR Vendor Administrators), approve purchase requisitions and orders (Contracting Officers and Budget Approvers), and change passwords within the PASS system. While this condition was deemed remediated as of the completion of the September 2014 periodic review of access, which was effectively designed, a deficiency in the control environment existed for the first 11 months of the year until the point of remediation.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Prior to remediation, considering the decentralized nature of the PASS user population, management did not deem certain critical access rights within the applications to pose a significant enough risk to warrant deploying resources in a manner that would enable a more comprehensive and timely periodic review of access process to be performed.

EFFECT

By not performing a review of user accounts that covers the access rights listed above, there is an increased risk 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 the user to process purchase requisitions and orders or make changes to the vendor master file(s) outside of defined approval processes.

RECOMMENDATION

The deficiencies identified as a result of the periodic review of access were remediated as part of the performance of the September 2014 periodic review of access. We recommend that management continue to perform this review process as designed on a semi-annual basis.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

d. SOAR Developer Segregation of Duties

CONDITION

During FY 2013 testing, it was determined that both members of the SOAR Production Support team were granted access to develop and migrate application program changes into production, as well as administer the database. According to management, this access was authorized, as these individuals were responsible for developing "low-impact" SOAR changes. This combination of responsibilities and access levels represented a control weakness in segregation of duties.

Development responsibilities were removed from these individuals in July 2014, enforcing segregation of duties between development and production administration, in remediation of the finding above. However, a deficiency in the control environment existed from the beginning of FY 2014 through the point of remediation in July 2014, approximately 9 months of the fiscal year.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Prior to remediation, based on a consideration of priorities and limited resources, management had not allocated the resources required to develop and implement segregation of duties controls that mitigate the risks associated with the condition including, but not limited to, the segregation of program development roles from production application and database administration roles among different individuals and/or other mitigating controls such as monitoring the activities of the individuals with administrative level access.

EFFECT

For the period noted in the condition above, the lack of segregation of duties controls increased the risk that developers could create and apply changes to application programs, data, and/or the configurations of the underlying database schema within the production environment without management's awareness/approval. This could have an adverse effect on the availability or processing/data integrity of the application.

RECOMMENDATION

We recommend that management continue to enforce the segregation of duties implemented as part of the remediation of this finding.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

e. DOCS and WEBBS Password Settings are Not in Compliance with DOES Requirements

CONDITION

During FY 2013 testing for the District Online Compensation System (DOCS) and the web interface, Web Enabled Benefit System (WEBBS), it was noted that the application level password configurations did not comply with requirements set forth in DOES's password policies (i.e., the D.C. Department of Employment Services (Office of Information Technology) User Account and Password Management Standard). Specifically, the minimum password length was set to five characters (whereas policy require the setting to be between 6 and 8 characters), and required settings for password complexity, password expiration, and account lockout after unsuccessful login attempts were not enforced.

During FY 2014, no changes were made to address the condition above, and therefore, this represents an unremediated finding from FY 2013.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Due to system limitations, upon implementation of DOCS and WEBBS, the password parameters were not set in accordance with the current DOES Password Management Policy for password-based authentication. Subsequently, due to resource limitations and efforts required, the password parameters have not been updated since implementation to reflect the current password policy requirements.

EFFECT

Weakly configured password settings increase the risk that unauthorized users could access sensitive system functions, which could negatively impact the confidentiality, integrity and availability of application data.

RECOMMENDATION

We recommend that management enforce strong password settings in accordance with the D.C Department of Employment Services, Office of Information Technology, User Account and Password Management Standard in remediation of the finding above.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

f. DOCS and DUTAS Application Administrator Access

CONDITION

In our FY 2013 testing, it was determined that the DOCS application security administrator and two DUTAS administrators also possessed either developer or business end user responsibilities. While management had deemed their access appropriate to perform these functions, the lack of segregation of duties between these functions, in addition to the fact that a compensating control to mitigate the risk associated with this specific condition had not been designed and implemented by management, represented a weakness in the internal control environment for these two applications.

Upon review in July 2014, it was determined that security administration for DOCS was appropriately restricted and segregated. However, the two DUTAS administrators retained access to their conflicting functions as developers. As a result, this control deficiency has not been fully remediated from FY 2013.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Based on a consideration of priorities and limited resources, management has not yet allocated the resources required to develop and implement segregation of duties controls that mitigate the risk associated with the condition. This includes, but is not limited to, the segregation of program development from production application administration roles among different individuals, and/or other mitigating controls such as monitoring the activities of the individuals with administrative level access. Specifically, the developers noted with access to administer security to DUTAS are the only two Office of Information Technology (OIT) personnel currently aligned to support the DUTAS system.

EFFECT

For the period of time noted in the condition above, the lack of segregation of business end user responsibilities from production system administration roles increases the risk that security changes are made outside of defined approval processes to manage such security changes.

The lack of segregation of program development roles from production system administration roles increases the risk that certain data or configuration changes could be made directly within the applications, by-passing established change control procedures. Such changes, if not authorized, tested, and properly implemented, could have adverse effects on the availability or processing/data integrity of the application.

RECOMMENDATION

We recommend that management limit the access of those with development responsibilities for DUTAS to read-only within the production application. If resource limitations dictate that this is not feasible, processes should be implemented to periodically review any changes deemed critical by management, including changes to security, that are made by those with development responsibilities within the production environment. This review should be performed in a controlled and consistent manner (at least quarterly) by someone without access to make the changes subject to the review. The review should be formally documented and consist of the reviewer tying back any cases in which changes were made by these IT support personnel to upfront approval documentation that would have approved the change to be made.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

g. Batch Job Monitoring for PASS

CONDITION

Logs or other relevant evidence of automated task completion (for both successful and failed tasks) was not available prior to February 1, 2014, as automated tasks were manually monitored prior to this time. As a result, KPMG could not conclude on the operating effectiveness of management's control: "PASS automated task failures are evaluated and remediated in a timely manner" during the period from October 1, 2013 through January 30, 2013. While this control has been remediated as of February 2014, a deficiency in the control environment existed during the period above.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

At the time of upgrade to the PASS system in September 2013, management began to utilize the automated task scheduler within PASS to support batch processing for the application. During stabilization, these jobs were manually monitored by IT support personnel, and management did not consider the risk of unresolved job failures to warrant further documentation to support this process until automated alerting mechanisms were configured in February 2014.

EFFECT

Without job processing completion logs, management's ability to research specific issues and general trends in support of the overall administration of the PASS system could be limited.

RECOMMENDATION

We recommend that management continue to follow currently implemented processes to produce and store e-mailed logs of job successes and failures and to track through to remediation via incident tickets any cases in which automated tasks fail within PASS.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

h. Terminated Employees in SOAR and PASS

CONDITION

Until April 2014, a significant portion of accounts belonging to separated employees were captured as part of downstream access review processes. This indicated that the proactive process to communicate and remove access of terminated employees in a timely manner upon termination was not consistently performed. Specifically, access was revoked, but not within a timely manner (more than 14 days after separation), for 10 out of 15 separated SOAR users and 5 out of 15 separated PASS users that were selected for testing. Additionally, 12 PASS users that separated prior to April 2014 were also determined to possess active access to the application at the time of review in July 2014.

In April 2014, the access termination processes for SOAR and PASS were modified to include automated access revocation triggered by the processing HR termination records for PASS and the consistent, timely communication of separations from Human Resources to the security administrator for SOAR. The controls were reviewed in April 2014 and were determined to be effectively designed. However, a deficiency existed from October 2013 through April 2014.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

For the period noted in the condition above, Agency Security Officers (ASOs) did not consistently receive timely notification from management regarding the separation of employees within their agency, and therefore, these ASOs were unable to take the appropriate steps necessary to have the access of the separated individuals revoked in a timely manner.

EFFECT

Without consistently following the process for timely communication of and removal of system access for separated employees, the risk exists that a separated person with malicious intent, or another person with knowledge of the separated person's logon credentials, may be able to use the account to alter the integrity of application data contained within applications such as SOAR and PASS.

RECOMMENDATION

We recommend that management continue to execute the control activities implemented as part of the remediation of the finding above.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

i. CFO\$olve Database Password Configurations

CONDITION

In reviewing password settings configured for the CFO\$olve environments during FY 2013 testing, it was determined that settings for the database and operating system passwords deviated from the Office of the Chief Financial Officer (OCFO)/Office of Chief Information Officer (OCIO) Password Policy in minimum length, complexity, account lockout, and password expiration.

These password settings were updated to comply with the aforementioned policy in September 2014. However, a deficiency in the control environment existed from the beginning of FY 2014 through the point of remediation in September 2014, which was almost 12 full months.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Although the OCFO/OCIO Password Management Standard requires strong password configurations, management has not defined processes to periodically monitor adherence to control and configuration standards.

EFFECT

Weakly configured database and operating system password settings increase the risk that unauthorized users can access sensitive system functions, which can negatively impact the confidentiality, integrity and availability of application data.

RECOMMENDATION

Management should perform a periodic review of key security configurations within the systems under the OCFO Password Management Standard to ensure compliance with this policy.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

j. Monitoring of Privileged UNIX Access

CONDITION

While processes to review a series of authentication attempts to highly privileged accounts (including SSHD and SUDO logins) onto the servers supporting PASS and PeopleSoft were implemented in FY 2014, these processes were not comprehensive and did not include all PASS and PeopleSoft servers, and did not account for switch-user (SU) commands. Further, SU logs were not available for the entirety of FY 2014. As a result, the inability of management to monitor these privileged activities on the servers supporting PeopleSoft and PASS represents a weakness in the internal control environment.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

OCTO security policies have not been designed to require monitoring of SU activity. Rather, security procedures have emphasized the preventative control of changing the password to privileged system accounts at the time of separation of the one of the individuals with knowledge of the password.

EFFECT

Without processes to monitor switch-user activity, the risk is increased that unauthorized activity performed in the system under these accounts is not detected in a timely manner, thereby negatively impacting the confidentiality, integrity and/or availability of financial data.

RECOMMENDATION

Management should document and adhere to access governance protocols for all critical enterprise servers. These protocols should include procedures to monitor privileged account activity through quarterly reviews of “switch-user” activity on Linux environments. These reviews should be conducted by individuals with knowledge of the appropriateness of the individuals accessing the privileged accounts on these servers. Additionally, actions constituting suspicious activity should be defined and further investigated when identified.

MANAGEMENT’S RESPONSE

Management concurs with the finding.

k. PASS Access to Change Passwords

CONDITION

In reviewing users with access to change user passwords within PASS, it was determined that 9 contractors possessed access after either separating from the entity or changing their role within the entity, which no longer required that they have access to perform this function.

All of these individuals required access to perform this function at the time of initial hire, and this issue was deemed remediated on September 4, 2014 when their access was revoked. Additionally, management implemented a process to review access as it relates to this function on a quarterly basis in October that was reviewed and deemed effective. However, as access was held when no longer required until it was revoked on September 4, 2014, a deficiency in the control environment existed from October 2013 through the September 2014.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

For the contractors that transferred to a different role or left the entity, the process to revoke access to PASS at the time of transfer or termination did not execute due to management oversight.

Additionally, the periodic review for PASS was not designed to include users with access to change passwords within PASS, and as a result, these users were not detected as no longer requiring these levels of access.

EFFECT

Accounts possessing access to change passwords when no longer required to hold this level of access increases the risk that changes will be made to a user's password outside of defined help desk processes allowing an individual to operate under the account of the individual for whom the password was changed. This inhibits the ability of authentication controls to ensure that the user account operating in the system is utilized only by the account owner.

However, in assessing the risk posed by this deficiency, it was determined that none of the individuals noted in the observation above made changes to user passwords after the point in time in which they transferred or became separated.

RECOMMENDATION

As documented within the condition above, a quarterly periodic review of users with access to change passwords for PASS was implemented in October 2014. We recommend that this process continue in the future as to address the risk that contractors retain privileged access rights within PASS when no longer required.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

I. BARTS Application Administrator Access

CONDITION

Upon reviewing individuals with administrative access to the Budget and Reporting Tracking System (BARTS) application, it was determined that one individual retained access to administer the BARTS application when not commensurate with his role as Agency Director. Management had approved this access to be retained in a backup capacity, but it was no longer utilized or necessary to support operations at the time of review.

Upon review on September 22, 2014, it was determined that the individual noted above was removed from the BARTS application in remediation of the finding above. However, a deficiency in the control environment existed from the beginning of FY 2014 through the point of remediation on September 22, 2014.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Until the point of remediation, management did not consider the risk introduced by the level of access held by the Agency Director to necessitate revocation of the access held.

EFFECT

For the period noted in the condition above, the lack of segregation of business owner responsibilities from production system administration roles increased the risk that security changes were made outside of defined approval processes to manage such security changes.

RECOMMENDATION

Management should continue to perform periodic reviews of BARTS access, including the access of security administrators, to ensure that access remains commensurate with user job responsibilities and remains restricted based on the principle of least privilege.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

m. BARTS Operating System, Database Administrative Access, and Database Password Configurations

CONDITION

During FY 2013 testing, it was determined that:

- Due to limitations associated with use of Windows SQL Server 2000 as the BARTS database management system, minimum password configurations could not be enforced for the "sa" generic account.
- Eight system and generic accounts with active access to administer the operating system were no longer required to be active.

On June 6, 2014, management implemented a manual, semi-annual rotation of the password for the "sa" account in remediation of the first point in the finding above. Additionally, on September 26, 2014, management revoked the administrative access for the system and generic accounts that no longer required these privileges when remediating the second point in the finding above. However, these deficiencies existed in the control environment from the beginning of FY 2014 through the points at which they were remediated.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Due to considerations of the risk along with resource limitations, management had not implemented formal policies and procedures for monitoring accounts with privileged access and ensuring that system and generic accounts that no longer required privileged access had been disabled or deleted timely.

Additionally, due to system limitations, management cannot enforce system password complexity at the database level. Prior to the time of remediation, management had not deemed the risk sufficient enough to warrant a manual process to rotate the passwords for database accounts in compensating for the lack of configurable controls to secure these passwords.

EFFECT

For the period of time noted in the condition above, the existence of dormant accounts that no longer required access to the operating system or database increased the risk that these accounts could have been accessed by individuals without authorization to do so. Additionally, accounts without strong controls over

their related login credentials increased the risk that the accounts could have become compromised. In both cases, these accounts could have been utilized to manipulate application programs and data in an unauthorized manner.

RECOMMENDATION

Management should continue to execute control processes to periodically rotate the password to the “sa” account. Additionally, management should implement processes to periodically review administrator access on the BARTS database and operating system to ensure that access remains appropriately restricted to those accounts requiring access as part of their user or system job responsibilities.

MANAGEMENT’S RESPONSE

Management concurs with the finding.

n. DOCS Wage Modification Access

CONDITION

During FY 2013 testing, it was determined that 25 of 41 users had the ability to add or modify wage information per their system access rights within the District Online Compensation System (DOCS) application when it was not required to fulfill their job responsibilities.

On July 15, 2014, management implemented changes to the access structures within the DOCS application to remediate this finding. These changes restricted access to only the appropriate individuals who needed access to update wage information in order to fulfill their job responsibilities. However, this deficiency existed in the control environment from the beginning of FY 2014 through the point of remediation on July 15, 2014.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Historically, system limitations have prevented management from configuring access within DOCS to separate access privileges required to modify eligibility parameters and wage data. During FY2013 and FY2014, management was in the process of reconfiguring the application to address this limitation so that privileges enabling the modification eligibility parameters could be assigned separately from

privileges enabling the modification of wage information. The process was completed on July 15, 2014.

EFFECT

For the period noted in the condition, there was an increased risk that the users referenced could apply changes to client wage information within the DOCS application that inappropriately influences monetary eligibility for unemployment benefits payments outside of defined approval processes.

RECOMMENDATION

Management should continue to perform periodic reviews of access for DOCS users to ensure that access remains appropriately restricted based on user job responsibilities.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

o. Terminated Employees in DOCS

CONDITION

Upon reviewing the timeliness of access revocation for a sample of eight DOCS terminated users, it was determined that two users did not have their access removed within the expected period of one week from the date of termination. In both cases, access was held for more than one month after termination, at which time it was revoked as part of management's semi-annual periodic review of access. Although access was revoked, the lack of timely removal of access of terminated employees indicates a weakness within the control environment.

It was noted that neither of the two users identified above logged into the system after their termination dates.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

The DOCS Security Officer did not consistently receive timely notification from Human Resources and the terminated employees' supervisors regarding the separation of employees, and therefore, the DOCS Security Officer was unable to

take appropriate steps necessary to have the access of the separated individuals revoked in a timely manner.

EFFECT

Without consistently following the process for timely communication and removal of system access for separated employees, the risk exists that a separated employee or another person with knowledge of the separated employee's logon credentials, may be able to use the account to alter the integrity of application data contained within the DOCS application.

RECOMMENDATION

Management should re-emphasize the established process for communicating separations and removing separated employees' user access to the DOCS application with all parties responsible for control performance to increase the consistency with which the process is followed. This should include the terminated employees' supervisors and Human Resources representatives. Further, timeliness requirements for the communication of terminated employees to the DOCS Security Administrator should be formally documented within policies and procedures governing these applications and communicated to all relevant parties.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

p. Journal Entries Segregation of Duties within the System of Accounting Reporting (SOAR)

CONDITION

As part of our FY 2013 evaluation of controls over segregation of duties related to the System of Accounting and Reporting (SOAR), it was determined that 519 accounts, including individuals and system accounts, had access to both enter/post and approve/release journal entries. In addition, it was determined that management had not implemented a detective control after the journal entry approval to confirm the adherence to the segregation of duties policy requiring a journal entry to be prepared and reviewed by separate individuals.

Similar controls were reviewed during our FY 2014 audit procedures and it was determined that management reduced the number of accounts with access to both enter/post and approve/release journal entries to 69. Additionally, a quarterly review process was implemented to validate that a documented approval outside of SOAR was present for any entries appearing to have been entered/posted and

approved/released by the same person within the system. The first review covered FY 2014 Q4 (July 1 - September 30). This review was completed, and all entries appearing to have been entered/posted and approved/released by the same person were determined to have had a documented approval by a separate individual outside of the system, in remediation of the finding above. However, a deficiency existed within the control environment until the completion of the first review in October 2014.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Historically, system limitations prevented management from configuring access within SOAR to separate the privileges to enter/post and approve/release journal entries. Additionally, prior to FY 2014, management had not established policies and procedures to require manual reviews of journal entries applied within the SOAR system to compensate for the additional risk posed by the segregation of duties risk.

EFFECT

Without system enforcement of the segregation of duties between entering/posting and approving/releasing journal entries (or compensating controls to identify if the segregation of duties risk is exploited resulting in journal entries being applied outside of defined approval processes), there is an increased risk that unauthorized or inaccurate journal entries could potentially be entered/posted and approved/released and remain undetected by management.

RECOMMENDATION

Management should continue to execute control processes implemented as part of the remediation of the finding above. Additionally, management should monitor control performer adherence to the procedure on a periodic basis.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

q. DCAS Access Review

CONDITION

A periodic review of system user access within the District of Columbia Access System (DCAS) (including the Curam and Connecture applications) has not been performed.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Due to resource limitations and the effort required for the initial periodic review of access, management has not yet completed the first periodic review.

EFFECT

By not performing a review of user accounts on a regular and timely basis, there is an increased risk 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 the ability to use various functions to alter the integrity of application data.
- A separated person or another person with knowledge of this active user account, may be able to use this account to alter the integrity of application data.

RECOMMENDATION

We recommend that management complete a periodic access review of the user accounts within DCAS. This review should be:

- Performed at a controlled frequency determined by management;
- Performed by an individual with sufficient knowledge of the user access requirements who is not responsible for administering access and who does not individually possess the access level that is being reviewed;
- Based on a comprehensive system-generated report of user accounts from DCAS (including Curam and Connecture); and
- Formally documented and signed by the reviewer.

- Access modifications requested as a result of the review should be verified to ensure that they are proper and executed in accordance with controls provisioning access.

We also recommend that the DCAS Access Control Policy be updated to reflect these control activities.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

r. DCAS Password Settings

CONDITION

Upon inspection of the minimum password configuration requirements at the application, database, and operating system layers for District of Columbia Access System (DCAS), the following deviations from the DCAS Identification and Authentication policy were identified:

- **Application Layer** – The DCAS password policy requires three maximum failed login attempts; the actual maximum account lockout attempts configuration was set to five. In addition, the DCAS password policy requires a maximum password age of 90 days; the actual maximum password age configuration allowed 180 days.
- **Database Layer** – The DCAS password policy requires three maximum failed login attempts; the actual maximum account lockout attempts configuration was set to ten. In addition, the DCAS password policy requires a maximum password age of 90 days; the actual maximum password age configuration allowed unlimited password age. Finally, the DCAS password policy requires a minimum password length of eight characters with password complexity enforced; the actual configuration does not require minimum password length nor password complexity.
- **Operating System Layer** – The DCAS password policy requires a maximum password age of 90 days; the actual maximum password age configuration allowed unlimited password age. In addition, the DCAS password policy requires a minimum password length of eight characters with password complexity enforced; the actual configuration required a minimum password length of five characters and no password complexity.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Due to lack of management oversight, required password parameters outlined within the DCAS Identification and Authentication Policy (DCAS-IA-01) have not been consistently applied to the application, operating system, and database layers for the system. Additionally, there has not been a process implemented to monitor and remediate deviations using defined security policies.

EFFECT

Noncompliance with the DCAS Identification and Authentication policy as it relates to password settings increases the risk that unauthorized users could access sensitive system functions, which could negatively impact the confidentiality, integrity, and availability of application data.

RECOMMENDATION

We recommend that management enforce strong password settings across all three layers (application, database, and operating system) in accordance with the DCAS Identification and Authentication Policy (DCAS-IA-01). In cases where password expiration settings cannot be enforced systematically due to system limitations or operational inefficiencies, we recommend that management apply a manual password rotation on a periodic basis where the change is formally documented. Additionally, management should implement procedures to monitor and remediate deviations from defined security policies.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

s. Linux Administration for DCAS

CONDITION

During the assessment of users with administrative access for the Linux servers supporting the District of Columbia Access System (DCAS) environment in FY 2014, it was determined that:

- For one of four sampled Linux servers hosting DCAS (Curam and Connecture), direct root login via remote Secure Shell (SSH) connections has been allowed.

- A review of the Switch User (SU) system log activity which captures login activity on the administrative accounts, including root, has not been formally documented.
- For the servers supporting the DCAS environment, 17 individuals held super user do (SUDO) access to root privileges which allows them to run a command or program as root. 15 of the 17 users with these elevated privileges were initially approved as part of the stabilization efforts, but no longer required this level of access. At the time of our review, the SUDO access to root privileges for those 15 users was not commensurate with job responsibilities.

CRITERIA

See NIST and ISACA Criteria previously described at pages A-35.

CAUSE

Due to the lack of formal standards that require the disablement of direct root login via remote SSH connections and the lack of procedures to require review of SU activity, these controls and processes were not consistently implemented during FY 2014.

Finally, due to resource limitations, as well as system stabilization and development efforts, management did not follow the DCAS Access Control Policy (DCAS-AC-01) least privilege access and the accounts noted in the third bullet of the finding above were not removed when access was no longer required.

EFFECT

The failure to timely remove access belonging to employees who no longer need it increases the risk that unauthorized activity performed in the system is not prevented, thereby negatively impacting the confidentiality, integrity and/or availability of financial data. Further, the lack of configured settings to require the execution of the switch user or SUDO commands to access 'root' privileges and lack of SU log review increase the risk that unauthorized activity performed in the system is not detected in a timely manner.

RECOMMENDATION

We recommend that management:

- Disable the capability for individuals with knowledge of the root password to directly login to 'root' account via remote login protocols such as SSH.

- Develop formal hardening guidelines and supporting procedures for managed servers that outline required settings to be configured consistently. Control performers should be trained on these guidelines and procedures.
- Implement a process, including defined documentation requirements, to review the SU activity log on a periodic basis. The reviewer should be independent, but have knowledge of the appropriateness of the events within the SU activity log, and should be independent and without SU access. The review should be completed and documented on a periodic basis determined by management.
- Revoke the logical access rights of accounts that possessed access to SUDO to root privileges when no longer required.
- Implement a process, including defined documentation requirements, to review accounts with SUDO access to root privileges on a periodic basis. The reviewer should be independent, but have knowledge of the appropriateness of individuals with this level of access, and should be independent and without significant system access. Control performers should be trained on this procedure as well as the procedures for removing access of separated personnel.

MANAGEMENT'S RESPONSE

Management concurs with the finding.

10. District of Columbia Public Schools

a. Ineffective Controls Over Administrative Premium Pay

CONDITION

DCPS' personnel costs and benefit expenditures totaled \$603,970,966 in FY 2014. During our testing of 145 payroll disbursements totaling \$490,841, we identified 17 employees who received additional pay. For 1 of the 17 employees, DCPS could not provide supporting documentation for the entire amount of the disbursement. Specifically, we noted that a disbursement in the amount of \$3,406 included administrative premium pay for the employee in the amount of \$136. However, DCPS could not provide supporting documentation to evidence that the employee was eligible to receive the additional pay.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

DCPS controls were not operating at the appropriate level of precision to ensure that the administrative premium payment (APP) data recorded in PeopleSoft was properly supported. The controls were designed for the school principal to request and review the “administrative premium” or “request for extra duty” sheet for the APPs entered into PeopleSoft by the schools. However, the principal did not ensure that the supporting documentation was provided before the APP was entered into PeopleSoft.

EFFECT

APP transactions entered by the schools without proper supporting documentation could increase the risk that inaccurate transactions will occur and not be detected in a timely manner. This could ultimately lead to improper payments being made to employees and misstatements of payroll expenditures.

RECOMMENDATION

We recommend that DCPS adhere to internal controls currently in place to ensure that all APP supporting documentation is prepared and reviewed prior to entry in PeopleSoft. In addition, we recommend that DCPS continue to provide guidance and training to ensure that the appropriate documentation is retained consistently at all schools to support the APP transactions.

MANAGEMENT’S RESPONSE

Management concurs with the finding. With the adoption of electronic approval of time and attendance, records are being maintained in the respective school/department. We will continue to provide guidance for record maintenance at trainings for principals and business office managers in which the OCFO participates.

b. Ineffective Review of Retro Pay Accrual

CONDITION

DCPS’ personnel and benefit expenditures totaled \$603,970,966 in FY 2014. During our testing of a sample of 145 payroll disbursements, we identified 44 employees who were approved for a 3% cost-of-living increase in October 2014. The increase was retroactive to October 1, 2013; however, DCPS did not record an accrual for the amounts due as of September 30, 2014 for 27 of the 44 employees.

CRITERIA

Yellow Book, Appendix I, section A1.08 d and COSO Internal Control—Integrated Framework as previously described on pages A-2 and A-3 of Appendix A.

CAUSE

DCPS controls were not operating at the appropriate level of precision to ensure the completeness of the payroll accrual calculation. Specifically, the review performed over the retro payment accrual estimate did not detect the omission of several groups of employees that were due a retro payment from the payroll accrual calculation.

EFFECT

Without effective controls surrounding the review of the calculation of the accrued retro pay, there is an increased risk that payroll expenditures could be misstated. Specifically, there was an understatement of payroll expenditures of \$49,136 related to the transactions we tested. The current year total estimated misstatement related to amounts owed but unpaid was \$937,645.

RECOMMENDATION

We recommend that DCPS develop and implement a formal process to review the union retro payment payroll accrual to ensure that all employees eligible to receive a retro payment are properly accrued and that payroll expenses are accurately stated in the general ledger.

MANAGEMENT'S RESPONSE

Management concurs with the finding. We acknowledge that we failed to recognize those employees that were inactive as of October 1, 2013. As we develop our Policy and Procedure Manual, we will include this process to ensure it is consistently followed.