

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

DISTRICT OF COLUMBIA

**Independent Auditors' Report on
Internal Control and
Compliance Over Financial Reporting
Fiscal Year Ended September 30, 2011**



**CHARLES J. WILLOUGHBY
INSPECTOR GENERAL**

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



February 10, 2012

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

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

Dear Mayor Gray and Chairman Brown:

In connection with the audit of the District of Columbia's general purpose financial statements for fiscal year 2011, KPMG LLP submitted the enclosed final Independent Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters (OIG No. 12-1-02MA).

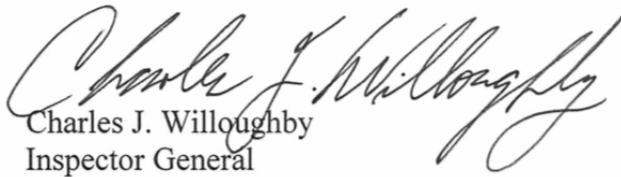
This report identifies two significant deficiencies. A significant deficiency adversely affects the District's ability to initiate, authorize, record, process, and report financial data. The significant deficiencies identified in the report are weaknesses in the following areas: (1) General Information Technology Controls and (2) Procurement and Disbursement Controls.

I am pleased to report progress relative to the financial management of the District of Columbia in comparison to last year's report of five significant deficiencies and, for the third consecutive year, the audit of the city's financial statements has revealed no material weaknesses.

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

If you have questions or need additional information, please contact Ronald W. King, Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,


Charles J. Willoughby
Inspector General

Enclosure

CJW/ws

cc: See Distribution List

DISTRIBUTION:

Mr. Allen Y. Lew, City Administrator, District of Columbia (via email)
Mr. Victor L. Hoskins, Deputy Mayor for Planning and Economic Development,
District of Columbia
The Honorable Muriel Bowser, Chairperson, Committee on Government Operations,
Council of the District of Columbia (via email)
The Honorable Jack Evans, Chairperson, Committee on Finance and Revenue,
Council of the District of Columbia District of Columbia (via email)
Mr. Brian Flowers, General Counsel to the Mayor (via email)
Mr. Christopher Murphy, Chief of Staff, Office of the Mayor (via email)
Ms. Janene Jackson, Director, Office of Policy and Legislative Affairs (via email)
Mr. Pedro Ribeiro, Director, Office of Communications
Mr. Eric Goulet, Budget Director, Mayor's Office of Budget and Finance
Ms. Nyasha Smith, Secretary to the Council (1 copy and via email)
Mr. Irvin B. Nathan, Attorney General for the District of Columbia (via email)
Dr. Natwar M. Gandhi, Chief Financial Officer (1 copy and via email)
Mr. William DiVello, Executive Director, Office of Integrity and Oversight, Office of the
Chief Financial Officer (via email)
Ms. Yolanda Branche, D.C. Auditor
Mr. Phillip Lattimore, Director and Chief Risk Officer, Office of Risk Management (via email)
Ms. Jeanette M. Franzel, Managing Director, FMA, GAO, Attention: Norma J. Samuel (via email)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives,
Attention: Bradley Truding (via email)
The Honorable Darrell Issa, Chairman, House Committee on Oversight and Government
Reform, Attention: Howie Denis (via email)
The Honorable Elijah Cummings, Ranking Member, House Committee on Oversight and
Government Reform, Attention: Yvette Cravins (via email)
The Honorable Trey Gowdy, Chairman, House Subcommittee on Health Care, the District of
Columbia, the Census and the National Archives, Attention: Anna Bartlett (via email)
The Honorable Danny Davis, Ranking Member, House Subcommittee on Health Care, the District
of Columbia, the Census, and the National Archives, Attention: Yul Edwards (via email)
The Honorable Joseph Lieberman, Chairman, Senate Committee on Homeland Security and
Governmental Affairs, Attention: Holly Idelson (via email)
The Honorable Susan Collins, Ranking Member, Senate Committee on Homeland Security
and Governmental Affairs, Attention: Daniel Jenkins (via email)
The Honorable Daniel K. Akaka, Chairman, Senate Subcommittee on Oversight of
Government Management, the Federal Workforce, and the District of Columbia,
Attention: Benjamin Rhoadside (via email)
The Honorable Ron Johnson, Ranking Member, Senate Subcommittee on Oversight of
Government Management, the Federal Workforce, and the District of Columbia
The Honorable Harold Rogers, Chairman, House Committee on Appropriations, Attention:
Cornell Teague (via email)

The Honorable Norman D. Dicks, Ranking Member, House Committee on Appropriations,
Attention: Laura Hogshead (via email)
The Honorable Jo Ann Emerson, Chairman, House Subcommittee on Financial Services and
General Government, Attention: John Martens (via email)
The Honorable José E. Serrano, Ranking Member, House Subcommittee on Financial
Services and General Government, Attention: Laura Hogshead (via email)
The Honorable Daniel K. Inouye, Chairman, Senate Committee on Appropriations,
Attention: Charles Houy
The Honorable Thad Cochran, Ranking Member, Senate Committee on Appropriations
The Honorable Richard Durbin, Chairman, Senate Subcommittee on Financial Services and
General Government, Attention: Marianne Upton (via email)
The Honorable Jerry Moran, Ranking Member, Senate Subcommittee on Financial Services
and General Government, Attention: Dale Cabaniss (via email)
Mr. John E. Reagan, III, CPA, Public Sector Audit Division KPMG LLP (1 copy)



GOVERNMENT OF THE DISTRICT OF COLUMBIA

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*

September 30, 2011



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

**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***

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

We have audited the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, budgetary comparison statement, each major fund, and the aggregate remaining fund information of the District of Columbia (the District) as of and for the year ended September 30, 2011, which collectively comprise the District's basic financial statements and have issued our report thereon dated January 25, 2012. Our report referred to the cumulative effect of a change in an accounting principle due to the passage of legislation affecting property tax revenues. Our report also referred to the adoption of a new accounting standard effective October 1, 2010. We conducted our audit 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. The financial statements of the District of Columbia Water and Sewer Authority and District of Columbia Housing Financing Agency, discretely presented component units of the District, were not audited in accordance with *Government Auditing Standards*.

Internal Control over Financial Reporting

Management of the District is responsible for establishing and maintaining effective internal control over financial reporting. In planning and performing our audit, we considered the District's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinions on the basic financial statements, but not for the purpose of expressing an opinion on the effectiveness of the District's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the District's internal control over financial reporting.

A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be deficiencies, significant deficiencies, or material weaknesses. We did not identify any deficiencies in internal control over financial



reporting that we consider to be material weaknesses, as defined above. However, we identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies and that are described in Appendix A to this report. A significant deficiency is a deficiency, or combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the District's basic financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* and which are described in finding 2011-02 in Appendix A to this report.

We noted certain matters that will be reported to management of the District in a separate letter.

The District's responses to the findings identified in our audit are described in Appendix A. The status of the significant deficiencies and instances of noncompliance identified in the fiscal year 2010 audit are described in Appendix B to this report. We did not audit the District's responses described in Appendix A or the status of the prior year deficiencies and instances of noncompliance described in Appendix B and, accordingly, we express no opinion on them.

This report is intended solely for the information and use of the Mayor, the Council, the Office of the Inspector General, District management, the U.S. Government Accountability Office, the U.S. Congress, and federal awarding agencies and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

January 25, 2012

Appendix A – Significant Deficiencies in Internal Control Over Financial Reporting

Finding 2011-01 – Weaknesses in the District’s General Information Technology Controls

Background:

General Information Technology Controls (GITCs) provide the foundation for a well-controlled technology environment that supports the consistent processing and reporting of operational and financial data in accordance with management’s directives. Our audit included an assessment of selected GITCs in four (4) key control areas: Access to Programs and Data, Program Changes, Program Development, and Computer Operations. During our assessment, we noted that, while the District made progress and remediated certain GITC findings identified during our prior year audit, pervasive GITC-related issues continue to exist.

The GITC environment is undergoing significant transition during fiscal year 2011. The District is currently in the process of modernizing its District-wide System of Accounting and Reporting. As a result, certain deficiencies previously identified will continue to exist, as they will not be remediated until the new system is implemented. Additionally, the District has already remediated other GITC deficiencies during fiscal year 2011. However, as these remediation efforts did not take place until fiscal year 2011 was well under way, the conditions continued to exist during part of the fiscal year and thus are included in this year’s report.

Our fiscal year 2011 findings included the following:

Access to Programs and Data

Conditions:

1. Failure to consistently restrict privileged and general user access to key financial applications in accordance with employee job responsibilities or segregation of duties considerations.
2. Inconsistent performance and documentation of both physical and logical user access administration activities, including the approval of new user access and access changes, periodic review of user access rights, including whether user access is commensurate with job responsibilities, and timely removal of user access upon employee termination.
3. Use of generic accounts to perform system administration or end user functions within key applications without adequate monitoring controls over such activities.
4. Failure to update the policy that defines the minimum password configuration requirements for the District’s Information Technology (IT) systems in approximately seven years. Further, inquiry and inspection procedures performed indicate that the policy was not effectively communicated to responsible personnel. Specifically, we determined:
 - a. The Office of the Chief Technology Officer (OCTO) Password Management Policy, last revised in November 2004, does not require that systems be configured to

- automatically lock out user accounts after a predefined number of invalid log-on attempts.
- b. There were various inconsistencies between the requirements outlined in the OCTO Password Management Policy and configurations set within certain applications and their supporting databases and operating systems.
 - c. There is potentially confusing language around the scope of the policy, which indicates it is to include “all District Government agencies and all users of DC Government computing equipment” when, in fact, the Office of the Chief Financial Officer (OCFO) is not under the direction of this policy.

Program Changes

Conditions:

1. Failure to institute well-designed program change policies that establish procedural and documentation requirements for authorizing, developing, testing, and approving changes to key financial applications and related infrastructure software¹ in the production environment.
2. Inconsistent adherence to established program change management procedures, including instances in which changes made to the system were not approved, tested or documented appropriately per the established procedures.
3. Failure to consistently restrict developer access to the production environments of key financial applications in accordance with segregation of duties considerations or, if not feasible, implement independent monitoring controls to help ensure changes applied to the production environment are authorized.

Program Development

Conditions²:

1. Failure to consistently follow and provide documentation for system development life cycle policies for authorizing, developing, testing, and approving system developments to key financial systems.
2. Failure to consistently restrict developer access to the production environments of key financial applications in accordance with segregation of duties considerations or, if not feasible, implement independent monitoring controls to help ensure changes applied to the production environment are authorized.

¹ Infrastructure changes refer to software changes and updates applied to underlying operating systems and databases supporting the key financial applications.

² Systems Development findings are specific to the Banner application at the University of the District of Columbia in FY 2011.

- Usage of generic accounts during the implementation to apply changes to the application, operating system, and underlying database with no evidence of monitoring of these generic accounts.

*Computer Operations
Conditions:*

- Failure to establish a monitoring process for identifying and addressing production job failures in several systems.
- Failure to retain system-generated documentation from the scheduling and processing utility to evidence the completion status of system jobs scheduled through the applications' utilities.

The table below summarizes the key financial applications that were impacted by the findings noted above.

Table 1: Summary of Applications Impacted by the Findings

Application	Access to Program and Data	Program Changes	Program Development	Computer Operations
PeopleSoft		N	N/A	
TACIS			N/A	
PASS			N/A	
ACEDS			N/A	
DOCS	N			N
DUTAS	N		N/A	N
BARTS			N/A	
MEDITECH Health Care Information System (HCIS)	N		N/A	
TAS	N	N	N/A	
SOAR	N	N	N/A	
iNovah	N	N	N/A	
Banner	T	T	T	

Legend

-  No prior year findings remediated in FY 2011.
-  Prior year findings partially remediated in FY 2011.
-  Prior year findings fully remediated in FY 2011.
-  Prior year findings not tested in FY 2011 due to other control objective failures.
- N New findings noted in FY 2011.
- T Findings noted in FY 2011; system not tested in prior year.
- N/A Not applicable; no systems development work was done within FY 2011.

Criteria:

1. 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 National Institute of Standards and Technology (NIST). The following NIST criteria were considered:
 - a. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995;
 - b. NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009;
 - c. NIST SP 800-64, Security Considerations in the System Development Life Cycle, October 2008; and
 - d. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology, September 1996.
2. The Information Systems Audit Control Association (ISACA) Control Objectives for Information and related Technology (COBIT®) 4.1, 2007.

Cause/Effect:

The findings highlighted above include weaknesses in both the design and operating effectiveness of controls considered relevant to the access to programs and data, program changes, program development, and computer operations areas. Although management has made progress remediating previous findings, additional improvements in formalizing key GITC processes and creating an effective monitoring function are needed. The existence of these findings increases the risk that unauthorized changes applied to key financial applications and the data they process adversely affect application processing and data integrity and, as a result, may materially impact the financial statements. Additionally, the existence of these findings impacts the reliability of key application reports and the ability to rely upon automated, configurable controls embedded within key financial applications.

Recommendations:

We noted that management did remediate several control deficiencies from the prior year across both access to programs and data and program changes. We recommend that management continue to perform the remediated control activities put in place. Further, we recommend that management monitor the effectiveness of these controls on a regular and periodic basis going forward.

To the extent the following findings are not remediated, we recommend the following:

1. Related to Access to Programs and Data controls, we recommend that management:
 - a. Assess and update or, as applicable, develop and document access management policies and procedures for production applications and underlying infrastructure systems. These policies and procedures should address requirements for clearly documenting user access requests and supervisory authorizations, periodic reviews of the appropriateness of user access by agency business management, timely

communication of employee separations/transfers, and disablement/removal of the related user access. Management should formally communicate policies and procedures to control owners and performers. Further, management should institute a formalized process to monitor adherence to policies and procedures related to key controls and, as performance deviations are identified, follow up as appropriate.

- b. Develop and implement controls that establish organizational and logical segregation between program development roles, production administration roles, and business end user roles among different individuals or, independently performed monitoring of the activities of users provided with conflicting system access over the activities of the developers (and other individuals) with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.
- c. Restrict the use of generic IDs or, if such access is required, implement independent monitoring of the activities performed using generic IDs.
- d. Develop and implement a process to review, update, and communicate a District-wide password management policy to responsible individuals on a periodic basis to help ensure it remains current and does not conflict in scope or content with other similar policies enacted across the District. We further recommend that this policy include, at a minimum, requirements for the following password configuration settings:
 - i. Minimum password length;
 - ii. Password aging and update requirements;
 - iii. Password complexity (e.g., at least one number, letter, and special character);
 - iv. User account lockout after a predefined number invalid logon attempts; and
 - v. Password history/reset restrictions.

In support of the recommended remediation, management should reconfigure existing password configuration settings at the application, operating system and database level, where applicable, in accordance with the District-wide password management policy. Finally, we recommend that management monitor adherence to the policy.

- e. Develop and formally document the physical access management policy and procedures for all server rooms. We recommend that these include, at a minimum, procedural and documentary requirements for:
 - i. Requesting and approving physical access;
 - ii. Timely disablement/removal of physical access rights during instances of employee separations; and
 - iii. Performing periodic reviews of access in consideration of users' ongoing need to retain physical access, and the modification of any updates required as a result of inappropriate access identified during the review process.

2. Related to Program Change controls, we recommend that management:
 - a. Develop and implement change management processes and controls that establish one or more of the following:
 - i. Organizational and logical segregation of program development roles from production system and database administration roles among different individuals; and
 - ii. Implementation of one or more independently operated monitoring controls over the activities of the developers (and other individuals) with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.
 - iii. Additionally, management should continue to document the performance of User Acceptance Testing (UAT).

3. Related to Program Development Controls, we recommend that management:

- a. Develop and implement program development processes and controls that establish one or more of the following:
 - i. An evaluation of the generic accounts that exist and documentation of the purpose of each generic account required to remain active, if any. Furthermore, for generic accounts that are required to remain active, we recommend management implement a formal process to approve and document each access request to generic accounts and perform a documented periodic review of generic account activity.
 - ii. The implementation of procedural and documentary requirements for:
 - Recording the nature of each change being applied;
 - Evaluating the impact and risk of each change relative to objective rating criteria;
 - Approving (and documenting such approvals of) changes; and
 - Validating the functionality/system impact of each change via pre-production testing in a model environment.

These policies/procedures should be provided to and discussed with control performers. Further, management should monitor control performer adherence to policies/procedures periodically.

4. Related to Computer Operations controls, we recommend that management:

- a. Implement any required changes to support an extended retention of job processing logs in support of audit requirements. Additionally, we recommend that management continue to save daily Excel reports produced by systems to limit the impact of any future archival issues.
- b. Document the completion of the new process put in place to monitor open application incidents reported to the OCFO Help Desk that are forwarded to the TSG, and also to

ensure that they are remediated within a defined time period that is acceptable to application owners.

These procedures should be provided to and discussed with the personnel responsible for enforcing the control activity. Further, management should monitor the personnel responsible for enforcing the control activity periodically.

Management Response:

The District agrees that there are weaknesses in its general information technology controls and has taken measures to address many of the issues raised by the auditors. For some of the issues, however, there simply are no “quick fixes.” Consequently, full remediation of the problems identified will require a longer period of time to develop and implement the appropriate actions.

Some of the measures implemented between 2010 and 2011 include the following:

Tax Administration System (TAS)

To address issues pertaining to access to programs and data, the District has completed the following with respect to the referenced systems:

- Implemented a new security report and signoff workflow application;
- Documented the policies and procedures related to the specific time requirements for completing user access reviews, modifying application privileges to remove any inappropriate access levels identified during reviews, and assigning accountability for the performance of these reviews;
- Incorporated the new policies and procedures into the workflow application;
- Modified the current policy and process to add a supervisory authorization requirement for user access request;
- Implemented a formalized, periodic review process to ensure individuals are not provided the ability to both approve quality assurance (QA) testing and approve migration to production for TAS application changes;
- Updated existing change management policies and procedures to require that documentation of testing results is completed prior to migrating TAS application changes into production;
- Implemented a formalized, periodic review process to determine whether users who have the ability to migrate TAS application changes into production require this access to perform their job responsibilities; and
- OCIO management instituted a formalized reporting mechanism to bring critical help desk ticket open issues to the bi-weekly prioritization meeting for discussion and prioritization and address the non-critical issues through the help desk incident management process.

BARTS/DOCS/DUTAS

- Developed an electronic routing system for access approval flow;

- Reviewed and updated the access control framework and documentation;
- Began performing regular reviews and created reports documenting user and generic access by level and system;
- Established an Access Control Board, consisting of DOES management, to semi-annually review existing access grants (including generic grants) and evaluate their appropriateness (the Board also reviews the access reports for suspect behavior and takes the actions as deemed to be appropriate and necessary);
- Reviewed, updated, finalized and published all OIT policy documents to the OIT policy document library and required all pertinent personnel to review them;
- Held training seminars on the OIT document library; and
- Consolidated the existing ticketing systems into a single OIT issue tracking system.

PASS

- Copies of OCFO Security Policy and Procedures were distributed to each Agency Security Officer (ASO);
- ASOs are required to maintain a working copy and an updated copy of security access reports to show before and after processing;
- Deletion of financial system logon IDs was included as a separate item on the Separation Clearance Form to be signed off by the ASO upon an employee's separation from an agency; and
- Created a standardized worksheet that is to be used as a reporting tool for modifications and deletions needed as a result of the security review.

PeopleSoft

- Identified the applicable IT governance policies to manage the network security;
- Began development of a PeopleSoft System Security Plan which details the functional and technical procedures and mechanisms for PeopleSoft security;
- Communicated with the PeopleSoft Governance Committee to obtain approval for the Security Plan;
- Updated/reviewed current configuration management changes with technical staff; and
- Eliminated/reduced the usage of the "aribasystem" generic user account.

Meditech

- UMC IT staff perform routine reviews of user access to assess compliance with established policies; and
- On a quarterly basis, UMC IT staff selects at least two users groups from the functional areas such as: Radiology, Emergency Room, Patient Billing, for access review.

To address issues pertaining to program changes, the District has completed the following with respect to the referenced systems:

PeopleSoft

- Began work to create a Technical Operations Runbook and Configuration Management Guide for PeopleSoft;
- Implemented the Agile software development methodology; and
- Discussed the development of the Runbook and Configuration Management Guide and implementation of the Agile methodology with the PeopleSoft Governance Committee.

Banner

Deficiencies were also noted with respect to Banner, a system recently implemented by the University of the District of Columbia (the University). The University concurs with the findings as presented by the auditors and has taken measures to address many of the issues noted. For example, the University has:

- Established a Banner Users Group to start reviewing user access in accordance with the established security classes and roles;
- Made plans to continue working with individual business units and departments to assign university functions to specific Banner roles;
- Implemented policies and procedures to minimize the number of generic accounts;
- Begun working with the University's Human Resources Department to develop and implement a communication process to notify Banner Project Management of personnel changes that affect the roles of individuals using Banner;
- Removed Banner Project consultants' access to generic accounts; one consultant can make data changes in production using a "personal" account and this consultant's system use is closely monitored;
- Initiated a review of Banner ERP Security Access;
- Developed and implemented a new Change Control Policy that requires a Change Control Form in order to request, track, and approve system and application changes;
- Began the process for procuring Change Management Software; and
- Instituted a policy requiring all Banner System users to sign a confidentiality agreement prior to being provided database access to the Banner System.

The actions delineated above represent only a portion of the steps taken to address issues in the area of General Information Technology Controls. The District fully recognizes that although much has been accomplished in improving IT controls, there is much yet to be done. The District will continue to be diligent in its efforts to strengthen IT controls and maximize overall operational efficiency.

Finding 2011-02 – Weaknesses in the District’s Procurement and Disbursement Controls

Background:

The District expends over \$8 billion per year in non-personnel related expenditures. In order to be as efficient and effective as possible, the District has established policies and procedures at the Office of Contracts and Procurement (OCP), as well as at those agencies that have independent procurement authority, to procure goods and services and to make payments for those goods and services. Further, these policies and procedures serve to ensure the District’s compliance with various laws and regulations governing procurement and payment, such as the Procurement Practices Act and the Quick Payment Act.

OCP has implemented a comprehensive, multi-year remediation plan to address previously identified deficiencies and has completed the steps scheduled for FY 2011 implementation. A key aspect of the remediation plan is addressing the governance framework and the risk assessment capabilities of OCP. Some of the key aspects of the remediation plan implemented in FY 2011 are as follows:

- **May 14, 2011** – For the first time, delivered an agency-wide CAFR debrief (FY 2010) to all staff and shared lessons learned and remediation action steps with both OCP-dependent and independent agencies with stand-alone procurement operations;
- **June 9, 2011** – Distributed an official memo to contracting officers reiterating their responsibilities for maintaining complete and accurate contract files, and the consequences (penalties) for any failures to comply, identified through audits and other means, which includes loss of delegated authority, suspension and/or termination;
- **June 14, 2011** – Delivered presentation to the Audit Division of the Office of the Inspector General as part of the FY 2012 Audit Symposium and Planning Conference. Provided an overview of the plans for OCP and OPIC, all of which have been or are in the process of being implemented. Also, highlighted opportunities for collaboration.
- **August 22 - August 26, 2011** – Peer review of OCP’s Office of Procurement Integrity and Compliance (OPIC) conducted by the Association of Local Government Auditors (ALGA). OPIC (internal audit group) deemed to be satisfactorily complying with Yellow Book standards.
- **September 1 - September 30, 2011** – OCP realignment plan implemented/executed. OPIC reorganized to include expansion of scope and frequency of audit and compliance activities. Risk Controls Framework developed containing over 200 risk statements for 5 procurement-specific lines of business and 3 support lines of business. FY 2012 goal is to mainstream the use/understanding of this tool throughout the organization.

Subsequent to the 2011 fiscal year end, the District also implemented the following:

- **November 8, 2011** - Directive issued to all contracting officers mandating the upload of all newly awarded and active contracts (as of October 1, 2011) into OCP's Contracts Compliance Module by December 31, 2011.
- **November 14, 2011; December 21, 2011 (Follow-Up)** – Directive issued to all agency directors (including those independent of CPO authority), contract administrators and contracting officers alerting them of the need to complete refresher training; beginning December 5th, the commencement of 'penalty free' contract administration audits performed by OPIC; changes to vendor evaluation procedures; and the commencement of official contract administration audits beginning February 27, 2012. For the first time, the official audit reports will be submitted to the City Administrator as well as affected agency directors and responsible staff.

However, as these remediation efforts did not take place until FY 2011 was well under way, the deficiency conditions continued to exist during part of the fiscal year and have been repeated.

Conditions:

1. We selected a sample of ninety-five (95) sole-source procurements executed by the District in FY 2011 and noted the following:

Lack of supporting documentation:

- a. For two (2) of ninety-five (95) sole-source procurements, adequate substantiating evidence was not maintained in the file documenting why, in the case of that respective procurement, a Determination and Findings (D&F) form was not required.
- b. For three (3) of ninety-five (95) sole-source procurements, the D&F form was not available for review.
- c. For five (5) of ninety-five (95) sole-source procurements, evidence showing that a search was performed to determine whether the vendor was debarred or suspended from doing business with the District was not available for review.
- d. For three (3) of ninety-five (95) sole-source procurements, the use of the sole-source method of procurement was not appropriate or adequately justified.
- e. For two (2) of ninety-five (95) sole-source procurements, the contract was not contained in the contract file.
- f. One (1) of ninety-five (95) files requested could not be located and made available for our inspection.

Inadequate approvals:

- g. For five (5) of ninety-five (95) sole-source procurements, the D&F was not approved by the respective Agency Director or Department Head.
- h. For five (5) of ninety-five (95) sole-source procurements, the D&F was not approved by the Contracting Officer.

- i. For one (1) of fifty-five (55) contracts, the Contracting Officer's maximum approval authority was less than the amount of the procurement on the purchase requisition.
 - j. For three (3) of ninety-five (95) contracts, evidence of the Contracting Officer's approval authority was not available for review.
 - k. For one (1) of ninety-five (95) sole-source procurements, there was no evidence as to whether the contractor was in compliance with the District tax filings requirement.
2. We also selected a sample of seventy (70) emergency procurements executed during FY 2011 and noted the following:

Lack of supporting documentation:

- a. For four (4) of thirty-seven (37) 'small' (\geq \$5,000 but $<$ \$100,000) emergency procurements tested, the applicable quotes were not made available for review.
- b. For one (1) of thirty-seven (37) 'small' emergency procurements, there was insufficient documentation substantiating that the appropriate number of quotations were received.
- c. For six (6) of twenty-four (24) 'large' (\geq \$100,000) emergency procurements, evidence showing that a search was performed to determine whether the vendor was debarred or suspended from doing business with the District was not available for review.
- d. For eight (8) of twenty-four (24) 'large' procurements tested, there was no evidence as to whether the contractor was in compliance with the District tax filings requirement.
- e. One (1) of twenty-four (24) 'large' procurements, the contract requested could not be located and made available for our inspection.
- f. For one (1) emergency procurement in excess of \$1 million, evidence of City Council approval and evidence of legal review by the Office of the Attorney General was not contained in the contract file.
- g. For eight (8) emergency procurements, the length of the procurement was not documented in the contract file.
- h. For three (3) emergency procurements, the D&F was not made available for review.
- i. For eleven (11) procurements, there was no evidence that the procurement was on a sole source basis or that there was competition.

Inadequate approvals:

- j. For one (1) emergency procurement, the D&F was not approved by the respective Agency Director or Department Head.
- k. For three (3) emergency procurements, the D&F was not approved by the Contracting Officer.
- l. For one (1) contract, the Contracting Officer's maximum approval authority was less than the amount of the procurement on the purchase requisition.
- m. For twenty-three (23) contracts, evidence of the Contracting Officer's approval authority was not available for review.

Non-compliance with emergency criteria requirement:

- n. For six (6) contracts inspected, the period of performance exceeded the 120 day maximum duration requirement for an emergency procurement.

3. We selected ninety-five (95) competitive procurements executed during FY 2011 for review and noted the following:

Lack of Supporting Documentation:

- a. For nine (9) of forty-six (46) 'small' (\geq \$5,000 but $<$ \$100,000) competitive procurements tested, the applicable quotes were not made available for review.
- b. For four (4) of forty-six (46) 'small' competitive procurements, there was insufficient documentation substantiating that the appropriate number of quotations were received.
- c. For fourteen (14) of forty-five (45) 'large' (\geq \$100,000) competitive procurements over \$100,000, there was insufficient documentation substantiating that the appropriate number of quotations were received.
- d. For fifteen (15) of forty-five (45) 'large' procurements tested, evidence showing that a search was performed to determine whether the vendor was debarred or suspended from doing business with the District was not available for review.
- e. For ten (10) of forty-five (45) 'large' procurements tested, there was no evidence as to whether the contractor was in compliance with the District tax filings requirement.
- f. For two (2) of forty-five (45) 'large' procurements tested, the contract was not contained in the contract file.
- g. For one (1) of eight (8) procurements in excess of \$1 million, evidence of City Council approval was not contained in the contract file.

Inadequate approvals:

- g. For one (1) of forty-nine (49) competitive procurements, the contract was not signed by the Contracting Officer.
 - h. For two (2) of forty-nine (49) competitive procurements, the Contracting Officer's maximum approval authority was less than the amount of the procurement on the purchase requisition.
 - i. For one (1) of forty-nine (49) competitive procurements, the contract amount was less than the PO amount and the legal sufficiency review from the OAG expired. When the contract was executed in August 2009, the contract was for \$3,628,719; however, the amount has since increased to \$11,371,705 with no additional modification to the contract, legal review, or Council approval able to be provided.
 - j. For five (5) of forty-nine (49) competitive procurements, evidence of the Contracting Officer's approval authority was not available for review.
4. We also selected ninety-five (95) direct vouchers for testing and noted eight (8) transactions were missing the required approval from the District's Office of Financial Operations and Systems (OFOS).
 5. During testing over purchase card (P-Card) transactions and monthly P-Card statement reconciliations, we noted the following deficiencies:

- a. For two (2) of twenty-five (25) P-Card transactions for amounts over \$2,500, amounting to \$7,640 of \$171,793 tested, documentation to support the purchases was not available for review.
 - b. For three (3) of twenty (20) foreign transactions taking place outside of the U.S. (i.e. foreign transactions), documentation supporting the purchases was not made available for review.
 - c. For six (6) of twenty-five (25) monthly P-Card statement reconciliations selected, the monthly reconciliation was not performed timely.
 - d. For three (3) of twenty-five (25) monthly P-Card statement reconciliations selected, there was no evidence that the reconciliation was performed as the supporting documents were not made available for review.
6. In our testing of procurement and disbursement transactions at the District of Columbia Public Schools (DCPS), we observed the following:
- a. For three (3) contract files supporting payments totaling \$19,588, there was insufficient substantiating evidence for a subsequent modification of the respective purchase order; further, DCPS was not able to provide such support after it was not found in the contract files.
 - b. For seven (7) purchase order files for payments totaling \$988,206, the files did not include a completed Determination of Reasonable Price and Award when the file was first provided by DCPS, specifically:
 - o For three (3) purchase order files for payment totaling \$2,068, the Contract Specialist had not indicated how the price for the procurement was deemed reasonable.
 - o For four (4) purchase order files for payments totaling \$986,138, the Determination of Reasonable Price Award was not signed by the Contracting Officer.
 - c. For one (1) contract file for payment totaling \$51,422, the file did not include the appropriate D&F form.
 - d. For two (2) contract files for payments totaling \$259,905, the file did not contain evidence of appropriate competitive vendor selection.
 - e. For thirteen (13) transactions totaling \$704,708, the respective purchase order and/or contract file was not provided by DCPS.
 - f. Three (3) disbursements totaling \$2,327 were incurred in the prior year, but were charged to current year expenditures and not properly accrued at the end of the prior year.
 - g. For one (1) purchase order in the amount of \$7,485, the Contracting Officer did not timely perform the 'Determination of Reasonable Price and Award' and 'Determination for Sole Source Procurement.' Both determinations were signed on 1/23/2012, the day the file was provided as support.
7. With regard to our testing of compliance with the District of Columbia Quick Payment Act, we determined that:
- a. Eighty-one (81) of seven hundred thirty-two (732) District payments (i.e. non-DCPS) selected for testing were not paid timely in accordance with the Quick Payment Act.

- b. One hundred twenty-five (125) of four hundred twenty-five (425) DCPS payments selected for testing were not paid timely in accordance with the Quick Payment Act. All transactions were paid more than 30 days after the Office of the CFO received the invoice.

Criteria:

The Procurement Practices Act indicates the following:

27 DCMR chapter 17, states that: *“In each instance where the sole source procurement procedures are used, the contracting officer shall prepare a written determination and findings (“D&F”) justifying the procurement which specifically demonstrates that procurement by competitive sealed bids or competitive sealed proposals is not required.”*

27 DCMR chapter 17, states that: *“Each sole source D&F for a procurement in an amount greater than twenty-five thousand dollars (\$25,000) shall be reviewed by the Director before solicitation and shall be approved by the Director before contract execution.”*

DC Code 1-204.51, states that: *“prior to the award of a multiyear contract or a contract in excess of \$1,000,000 during a 12-month period, the Mayor or executive independent agency or instrumentality shall submit the proposed contract to the Council for review and approval.”*

DCMR chapter 17 states that *“An “emergency condition” is a situation (such as a flood, epidemic, riot, equipment failure, or other reason set forth in a proclamation issued by the Mayor) which creates an immediate threat to the public health, welfare, or safety. The emergency procurement of services shall be limited to a period of not more than one hundred twenty (120) days. If a long-term requirement for the supplies, services, or construction is anticipated, the contracting officer shall initiate a separate non-emergency procurement action at the same time that the emergency procurement is made. The contracting officer shall attempt to solicit offers or proposals from as many potential contractors as possible under the emergency condition. An emergency procurement shall not be made on a sole source basis unless the emergency D&F includes justification for the sole source procurement. When an emergency procurement is proposed, the contracting officer shall prepare a written determination and findings (D&F) that sets forth the justification for the emergency procurement.”*

Financial Management and Control Order 07-004A states that *“Direct Voucher payment requests that are not explicitly identified in Financial Management and Control Order 07-004A, shall be submitted to the Deputy Chief Financial Officer for the Office of Financial Operations and Systems (OFOS) for consideration and approval in accordance with policy and procedures set forth for direct voucher payment review and consideration by OFOS.”*

According to the District Purchase Card program policies and procedures:

- **Purchase limit:** An individual who is issued a P-Card under the DC Purchase Card Program shall use the purchase card to buy commercially available goods and services, for *Official Government Business only*, with a value that does not exceed \$2,500 per single transaction and a total amount of \$2,500 per card per day and \$10,000 per card account per monthly

cycle, unless otherwise specified by the Chief Procurement Officer in the delegation of contracting authority.

- **Reconciliation:** Each approving official will have a queue of all P-card statements waiting for them in the PaymentNet system. By the 27th of each month, the Approving Official should obtain original receipts from cardholders under their jurisdiction and ensures that the cardholders have reviewed all transactions in PaymentNet. The Approving Official should review each transaction to verify that the good or service were received, that the nature of the purchase was within programmatic guidelines, and that the receipts match the amount listed in PaymentNet. The Approving Official should mark each transaction as Approved in PaymentNet by the 3rd day of the subsequent month.

According to DC Code 1-204.51, “prior to the award of a multiyear contract or a contract in excess of \$1,000,000 during a 12-month period, the Mayor or executive independent agency or instrumentality shall submit the proposed contract to the Council for review and approval”

Also, DC Code 2-301.05(G) states that “All contracts over a million dollars must go to the Office of the Attorney General (OAG) for a legal sufficiency review.”

27 DCMR chapter 15

1511.3 Prospective bidders that have been debarred or suspended from District contracts or otherwise determined to be ineligible to receive awards shall be removed from solicitation mailing lists to the extent required by the debarment, suspension, or other determination of ineligibility

The requirements for allowable costs/cost principles are contained in the A-102 Common Rule (§__.22), OMB Circular A-110 (2 CFR section 215.27), OMB Circular A-87, “Cost Principles for State, Local, and Indian Tribal Governments” (2 CFR part 225), program legislation, Federal awarding agency regulations, and the terms and conditions of the grant award. Management is required to maintain adequate internal controls to prevent and detect instances of noncompliance.

The District’s Quick Payment Act indicates the following: *If a contract specifies the date on which payment is due, the required payment date is the date specified in the contract. If a contract does not specify a payment date, the required payment date will be one of the following:*

- (a) Meat and meat food products - the seventh (7th) day after the date of delivery of the meat or meat product;*
- (b) Perishable agricultural commodities - the tenth (10th) day after the date of delivery of the perishable agricultural commodity; or*
- (c) All other goods and services - the thirtieth (30th) day after the receipt of a proper invoice by the designated payment officer.*

Cause/Effect:

District agencies are not adhering to the established policies and procedures governing creation and maintenance of procurement documentation and the payment of vendor obligations, which

may cause noncompliance with the Procurement Practices Act and the Quick Payment Act. Further, comprehensive monitoring controls were not established by OCP until FY 2011.

Recommendation:

We recommend that the District continue to implement its deficiency remediation plan. These implementation efforts should continue to be led by the OCP Procurement Integrity and Compliance Office (PICO), and sufficient resources should be provided to this office to ensure it can successfully implement the remediation plan. The performance measurement statistics monitored by PICO should be provided to both the Mayor and the Chief Financial Officer at least semi-annually so that senior District management is apprised of progress on the remediation plan.

Management Response:

Office of Contracting and Procurement (OCP)

Unlike past years, results from the FY 2011 CAFR show deficiencies widely distributed across the District's decentralized procurement operations. In FY 2010, OCP operations, presently servicing 52 District agencies, accounted for sixty-eight percent (68%) of the approximately one hundred twenty four (124) deficiencies cited, with the balance attributed to procurement offices independent of the Chief Procurement Officer's (CPO's) authority. This year, OCP accounted for forty-one percent (41%) of the approximately 177 deficiencies cited, while independent agencies accounted for the balance, an increase from the preceding year. Given these results, the District acknowledges the need to closely coordinate oversight, monitoring and remediation activities to uniformly and systematically reduce instances of non-compliance.

In response to the FY 2010 CAFR findings, the Office of Contracting and Procurement (OCP) noted in part that, "...*While tangible results might not be immediate, we expect that periodic training/refreshers and regular compliance reviews will strengthen the control environment and ultimately improve compliance outcomes in subsequent fiscal years.*"

Consistent with this representation, OCP crafted and implemented a comprehensive multi-year remediation action plan, which, among other risk areas, addressed concerns relative to the award of sole source, emergency, small and large competitive procurements. As of September 30, 2011, ninety-seven percent (97%) of planned actions had been ratified as fully implemented by the District's responsible oversight body.

Further, OCP's Office of Procurement Integrity and Compliance (OPIC) has increased the coverage and frequency of its audits and compliance reviews. Results are now reported in a 'Bellwether' Report to management detailing:

- The phases in the procurement lifecycle where audit concerns or violations have been identified;
- The total number of such concerns/violations by each phase;
- The prevailing themes;
- The accountable procurement staff; and

- Pertinent transaction details and actionable recommendations.

For the first time, quantifiable performance information is readily available to management, providing a near real-time snapshot of OCP issues. OCP will be using this data to correct unsatisfactory actions.

Also noteworthy is that close coordination between the External Auditor and OCP-OPIC is underway, to the extent practicable; to eliminate duplication of effort and to gain 'real-time' visibility into the conditions in the control environment before, during and after an audit engagement.

The District agrees that Purchase Card (P-Card) policies and procedures are not being followed consistently by all District agencies. However, and as communicated in the FY 2010 audit cycle, these findings refer to program oversight and surveillance reporting under the purview of each Agency Review Team (ART). The Office of Contracting and Procurement (OCP) has followed through on its prior year commitment to increase oversight activities. In FY 2012, following an agency-wide realignment, OCP's Office of Procurement Integrity and Compliance (OPIC) began random audits of select District agencies to augment training, administration and guidance provided by the District's P-Card Program Management Office (PMO).

District of Columbia Public Schools (DCPS)

Management concurs with the finding as noted by the auditors. To strengthen controls with respect to contracting and procurement, DCPS-Office of Contracts and Acquisitions (OCA) will provide training on Procurement Regulations, applicable D.C. Code, and other guidance pertaining to the retention of contract files.

To improve controls with respect to direct voucher payments, DCPS has amended its year-end accrual process instructions to include a checklist of items to review when requesting the accrual or processing of direct voucher payments at year-end. In addition, for direct voucher payments, a summary of key items requiring review will be disseminated to DCPS program and accounts payable staff.

To minimize the use of incorrect comptroller object codes, DCPS will re-emphasize the importance of approvers reviewing such codes for accuracy during the requisition and purchase order approval process. This will be communicated to staff in the form of a memorandum as well as through face-to-face discussion during staff meetings.

Office of Financial Operations and Systems

Management concurs with the finding as written regarding noncompliance with the Quick Payment Act. In August 2011, a joint memorandum issued by the Office of the Chief Financial Officer (OCFO) and the City Administrator was distributed to all agencies in order to communicate the prevalent causes for late vendor payments and to create a partnership between the District's program staff and the OCFO. The Office of Financial Operations and Systems (OFOS) will continue to bring awareness to the Quick Payment Act in FY 2012 by developing training material on the requirements of the "Act." OFOS will also meet with each cluster Controller and their respective Accounts Payable teams, to discuss this finding, to provide an understanding of the specific requirements of the Quick Payment Act, and to assist with identifying solutions to cluster issues that may prevent prompt payment.

Appendix B – Status of Prior Year Significant Deficiencies in Internal Control Over Financial Reporting

Prior Year Finding #	Prior Year Finding Title	Prior Year Finding Classification	Current Status
2010-01	Weaknesses in the District’s General Information Technology Controls	Significant Deficiency	Repeated as a significant deficiency in fiscal year 2011
2010-02	Weaknesses in the District’s Procurement and Disbursement Controls	Significant Deficiency	Repeated as a significant deficiency in fiscal year 2011
2010-03	Weaknesses in Monitoring Financial Reporting and Non-Routine Transactions in Stand-Alone Reports	Significant Deficiency	Remediated, comment not repeated
2010-04	Weaknesses in the Financial Reporting Process at the Office of Tax and Revenue	Significant Deficiency	Remediated, comments to be included in fiscal year 2011 management letter
2010-05	Weaknesses in the Personnel Management and Employee Compensation Process	Significant Deficiency	Remediated, comments to be included in fiscal year 2011 management letter