PUBLIC OVERSIGHT HEARING ON

PROGRESS REPORT ON THE FISCAL YEAR 2012 COMPREHENSIVE ANNUAL FINANCIAL REPORT (CAFR) AUDIT RECOMMENDATIONS

Before the

Committee of the Whole
Council of the District of Columbia

The Honorable Phil Mendelson, Chairman
June 11, 2013 1:00 p.m.
John A. Wilson Building
Room 412

Testimony of
Anthony F. Pompa
Deputy Chief Financial Officer
Office of Financial Operations and Systems

Natwar M. Gandhi
Chief Financial Officer
Government of the District of Columbia

Good afternoon Chairman Mendelson and other members of the Council who are present on the dais today. My name is Anthony F. Pompa and I am the Deputy Chief Financial Officer for Financial Operations and Systems. I am here today to present testimony on the progress made toward resolving deficiencies reported by the independent auditors as a result of their audit of the District's FY 2012 Comprehensive Annual Financial Report (CAFR).

The Office of Financial Operations and Systems (OFOS) is responsible for maintaining effective systems of accountability and fiscal discipline throughout the District's financial operations. In keeping with its mission, on an on-going basis, OFOS routinely assesses the District's accounting and financial reporting practices in an effort to enhance business processes, maximize operational efficiency, and strengthen internal controls. A critical part of this internal assessment involves the review and analysis of deficiencies and recommendations reported by the CAFR auditors each year.

To fully address the findings reported by the auditors, OFOS uses a formal remediation process which was first developed and implemented by OFOS in FY 2007. At that time, the main focus of our remediation efforts centered on the audit findings reported in the FY 2007 Yellow Book Report. Consequently, the process established to address the reported issues became known as the Yellow Book Remediation Process.

OVERVIEW OF THE YELLOW BOOK REMEDIATION PROCESS

The Yellow Book Remediation Process is a District-wide process that involves the collaborative efforts and active participation of financial and program staff at the affected agencies, OIO auditors and other key District stakeholders (e.g., Office of the City Administrator and the Council.) (*See* **Attachment A – Remediation Assignments Matrix**) The approach used to address and resolve audit findings involves a comprehensive analysis of each finding in order to gain a full understanding of the reported issues. In addition, the

process also requires the development of detailed corrective action plans by subject matter experts (SMEs) at the affected agencies. Focused remediation efforts typically start in late March/early April each year and continue throughout the remainder of the fiscal year until September 30th. In remediating the audit findings, our goal is to ensure that the necessary steps are taken to prevent the recurrence of reported deficiencies in the subsequent fiscal year.

Each reported finding is assigned to an OFOS liaison who works closely with the designated agency SME (or Agency Liaison) to analyze the reported findings. Although the OFOS Liaison coordinates and monitors the remediation of assigned findings, the SME is responsible for developing a corrective action plan that is fully responsive to the reported findings and implementing the planned corrective actions.

Agencies use a standardized template to develop a detailed corrective action plan that specifically addresses their respective findings. On a weekly basis, Agency Liaisons submit a corrective action plan status report to their designated OFOS Liaison. These status reports are used to monitor the progress of remediation efforts and to determine whether planned milestones are being achieved. (*See* **Attachment B – Agency Corrective Action Plan Status Reports as of May 28, 2013**) As planned corrective action steps are completed, OFOS notifies the Office of Integrity and Oversight (OIO). OIO internal auditors then perform the necessary procedures to confirm that action steps have been satisfactorily completed. To further enhance the effectiveness of the remediation process, a Yellow Book Oversight Committee, comprised of OFOS Liaisons, agency representatives (program and financial staff) and OIO internal auditors, meets periodically to monitor progress of remediation efforts and enforce the timely implementation of planned corrective actions (*See* **Attachment C – Yellow Book Oversight Committee Members (FY 2012 CAFR)**). Historically, these meetings have been well-attended and have provided a forum for meaningful discussion and strategy development.

OFOS prepares various reports (e.g., Remediation Flash Report) (*See* **Attachment D-Remediation Flash Report No. 1 (Dated May 3, 2013)**) to apprise interested parties of the status of remediation activities. OFOS also issues a "Red Alert Report" on an as-needed basis,

to notify key OCFO managers, Council representatives and the Office of the City Administrator of issues which may threaten the successful remediation of findings. (See **Attachment E – Red Alert Report)**

SUMMARY OF FY 2012 DEFICIENCIES

Audit findings are categorized according to their level of severity and are grouped as follows: ***material weaknesses*** which are the most severe breaches in internal controls, ***significant deficiencies*** which are less severe in nature but nonetheless require immediate resolution to prevent them from becoming material weaknesses, and ***management letter comments*** which represent other reportable conditions which should be corrected in order to enhance internal controls or otherwise improve operational efficiency.

As in the prior year, the independent auditors reported no material weaknesses in the FY 2012 Yellow Book Report. However, significant deficiencies were reported in the following four areas: general information technology controls, procurement and disbursement controls, tax revenue accounting and reporting, and financial reporting for capital assets. The numbers of specific conditions (by area) were as follows:

Area	Number of Specific Conditions
General Information and Technology Controls	13
Procurement and Disbursement Controls	51
Tax Revenue Accounting and Reporting	5
Financial Reporting for Capital Assets	4
TOTAL	**73**

In addition, KPMG (the District's independent auditors) reported 37 management letter comments in the following areas:

Area	Number of Comments
Cash and Investments	4
Contingent Liabilities	1
Disability Compensation	2
Capital Assets	3
Grants Management	9
Revenue	8
Loans Receivable	1
Inadequate Documentation of New Hires and Terminated Employees	1
Inadequate Management Review of Statements on Standards for Attestation Engagement 16 Reports	1
District of Columbia Public Schools	7
TOTAL	**37**

Progress of Remediation To-Date

The Yellow Book remediation process for the FY 2012 findings officially began with a Kick-Off session on March 27, 2013. Representatives from the affected agencies, OIO, OFOS as well as the Office of the City Administrator and the Council were in attendance. The purpose of the Kick-Off session was to explain the required process and to address questions pertaining to the process. Since the March 2013 Kick-Off, significant progress has been made toward developing and implementing the necessary corrective actions. Agencies have formulated 191 corrective action steps to address the 73 specific significant deficiencies reported by KPMG. As of May 28, 2013, 86 or 45.0% of the planned corrective action steps had been implemented

by the agencies. A breakdown of planned vs. completed (implemented) action steps is as follows:

Area of Deficiency	Number of Specific Conditions	Number of Planned Action Steps	Number of Action Steps Completed	Percentage of Action Steps Completed
General Information Technology Controls	13	109	54	49.5%
Procurement and Disbursement Controls	51	30	14	46.7%
Tax Revenue Accounting and Reporting	5	23	10	43.5%
Financial Reporting for Capital Assets	4	29	8	27.6%
TOTALS	**73**	**191**	**86**	**45.0%**

To more comprehensively address the reported issues related to capital assets, OFOS is establishing a centralized capital assets management team comprised of accountants skilled in recording, tracking, monitoring and accounting for capital assets. This team will be responsible for recording capital assets by asset class, tracking the physical location of capital assets, and ensuring the timely and accurate recording of disposals in the financial system. In addition, the capital assets management team will coordinate and manage the physical inventories taken of capital assets and will be instrumental in establishing policies and procedures governing capital asset accounting and management, including the transfer of completed projects from Construction in Progress (CIP) to capital assets.

OFOS also recognizes the importance of addressing the reported management letter comments. However, our ability to address all FY 2012 management letter comments in addition to the Yellow Book findings is limited by time constraints and a lack of available resources. Therefore, we are using a risk-based approach in attacking the management letter comments and focusing on those which may more quickly become Yellow Book findings if not addressed now.

Corrective actions related to the Yellow Book deficiencies are on target for completion consistent with the planned implementation deadlines. No major problems have been reported to OFOS or the Yellow Book Remediation Committee that will threaten resolution of findings as planned.

Mr. Chairman, this concludes my formal testimony. I would be happy to answer any questions you may have at this time. Thank you.

ATTACHMENT A
REMEDIATION ASSIGNMENTS MATRIX

MATRIX
Remediation Assignments
(FY 2012 Comprehensive Annual Financial Report (CAFR)

Area of Deficiency	OFOS Liaison(s)	Agency Liaison(s)		OIO Auditor
		Name	Agency	
General Information Technology Controls				
System:				
ACEDS	Jesse Dolojan	Denise Nedab	DHS	Tony The, Elizabeth Jowi
BANNER	Jesse Dolojan	Albert Casciero	UDC	Tony The, Elizabeth Jowi
BARTS, DOCS, DUTAS	Jesse Dolojan	Thomas Luparello	DOES	Tony The, Elizabeth Jowi
CAMA, TAS	Jesse Dolojan	Johnnie Simmons York	OTR/OCIO	Tony The, Elizabeth Jowi
iNOVAH, SOAR	Jesse Dolojan	Lillian Copelin	OFT/OCIO	Tony The, Elizabeth Jowi
MEDITECH	Jesse Dolojan	Ron Walker	UMC/DHS	Tony The, Elizabeth Jowi
PASS, PEOPLESOFT	Jesse Dolojan	Shirley Kwan-Hui	OCTO	Tony The, Elizabeth Jowi
TACIS	Jesse Dolojan	Loretta Walker	MPD	Tony The, Elizabeth Jowi
Procurement and Disbursement Controls	Cassandra Alexander	Yinka Alao	OCP	John Cashmon, Esther Sawyer
		Joseph Giddis	OCFO	John Cashmon, Esther Sawyer
		J.W. Lanum	DCGS	John Cashmon, Esther Sawyer
		Munetsi Musara	DCPS	John Cashmon, Esther Sawyer
Purchase Card	Michelle McNaughton	Yinka Alao	OCP	John Cashmon, Esther Sawyer
Quick Payment Act	Deena Parker	Martha Hopkins	OFOS	Esther Sawyer, Hassan Shode
		Munetsi Musara	DCPS	Esther Sawyer, Hassan Shode
Tax Revenue Accounting and Reporting	Tong Yu	Beth Spooner	OTR	Tisha Edwards, Prince Washaya
Financial Reporting for Capital Assets	Cassandra Alexander	Dave Pivec	OFOS	Khaled Abdel-ghany, Bernard Baranosky
High Risk Management Letter Comment:				
Cash and Investments	Michelle McNaughton	Tonja Lowe	OFOS	Elizabeth Jowi
		Jeffrey Barnette	OFT	Elizabeth Jowi

ATTACHMENT B
AGENCY CORRECTIVE ACTION PLAN STATUS REPORTS
(As of May 28, 2013)

GENERAL INFORMATION TECHNOLOGY CONTROLS

DEPARTMENT OF HUMAN SERVICES - ACEDS
CORRECTIVE ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The	(202) 442-8294	Tiong.The@dc.gov
	Elizabeth Jowi	(202) 442-8306	Elizabeth.Jowi@dc.gov
Agency Liaisons:	Deborah Carroll	(202) 698-3906	Deborah.Carroll@dc.gov
Financial Liaison:	Morris Thorpe	(202) 671-4466	Morris.Torpe@dc.gov
Program Liaison:			
Responsible ACFO:	Deloras Shepherd	(202) 671-4220	Deloras.Shepherd@dc.gov

On Track?
Completed
Yes
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)

DEFICIENCY #1	**ACEDS: 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.
RECOMMENDATION:	Related to Access to Programs and Data controls, KPMG recommends 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 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.

DEPARTMENT OF HUMAN SERVICES - ACEDS
CORRECTIVE ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1- Deficiency #1 - Recommendation a.	Management policies and procedures for production applications and underlying infrastructure systems have been updated in the 2013 version of the ACEDS Security Manual to address requirements for clearly documenting user access request and supervisory authorizations.	Jeffrey Borkman, ESA Deputy Administrator, Division of Information Systems (DIS)	1-Apr-13	30-Apr-13	Completed	X		X				
2 -Deficiency #1; Recommendation a.	Periodic reviews of the appropriateness of user access by agency business management are currently in place during security reviews, which are conducted at each site that houses ACEDS users. Security reviews are held twice yearly at all DHS, ESA Service Centers and once a year at all other locations. Center Managers must sign off on the Security Review Acknowledgement form when the review is completed. A written report of findings ise submitted to the Deputy Administrator for Division Information Systems (DIS) following each review. The updated security review schedule is listed in the revised ACEDS Security Manual.	Jeffrey Borkman, ESA Deputy Administrator, Division of Information Systems (DIS)	1-Apr-13	30-Sep-13	[redacted]		X		X			
3- Deficiency #1; Recommendation a.	Instructions that Program Managers are to provide timely communication of employee separations/transfers, and disablement/removal of the related user access are also delineated in the revised ACEDS Security Manual and is demonstrated in previous and recent communications as evidenced in the attachments.	Jeffrey Borkman, ESA Deputy Administrator, Division of Information Systems (DIS)	1-Apr-13	30-Apr-13	Completed	X		X				
4- Deficiency #1; Recommendation a.	Management formally communicated the updated policies and procedures to control owners and performers, initially in March 2011, via email.	Boyle Stuckey, DHS, Office of Information Systems	1-Apr-13	30-Apr-13	Completed	X		X				
5- Deficiency #1; Recommendation a.	Management instituted a formalized process to monitor adherence to policies and procedures related to key controls and, as performance deviations are identified, and follow up as appropriate. The 2013 version of the ACEDS Security Manual provides the formalized process to monitor adherence to policies and procedures related to key controls. ACEDS Security Officer reviews each Service Center location twice a year and all other locations once per year. A written report of findings, including identified performance deviations, will be submitted to the Deputy Administrator for Information Systems following each review. The report will include an evaluation of users' access rights with respect to current job responsibilities.	Jeffrey Borkman, ESA Deputy Administrator, Division of Information Systems (DIS)	30-Apr-13	30-Sep-13	[redacted]		X		X			
6- Deficiency #1; Recommendation b.	Controls that establish organizational and logical segregation between user roles among different individuals are already in place given that the Program Developers are assigned to and work out of the Office of Information Systems (OIS); the production administration is orchestrated from the Office of the Chief Technology Officer (OCTO); and the business end user is the Economic Security Administration (ESA), whose staff is separate from OCTO and OIS.	Boyle Stuckey,Interim Chief Information Officer (CIO), DHS, Office of Information Systems	1-Apr-13	30-Apr-13	Completed	X		X				

DEPARTMENT OF HUMAN SERVICES - ACEDS
CORRECTIVE ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

7- Deficiency #1 ; Recommendation c.	No one with generic IDs has update capability, only system inquiry is accessible. Independent monitoring of generic ID use is not necessary.	Jeffrey Borkman, ESA Deputy Administrator, Division of Information Systems (DIS)	1-Apr-13	30-Apr-13	**Completed**	X		X				
8- Deficiency #1 ; Recommendation d. i, ii, iii	The recommendation to document the physical access management policy for all server rooms is not appropriately assessed to DHS. The ACEDS server is The Office of the Chief Technology Officer (OCTO) is responsible for physical access to the ACEDS server which is located at 3919 Benning Rd NE, Washington, DC 20019. Given that OCTO is responsible for developing policies relative to the District's IT systems, DHS will apprise OCTO of this recommendation.	Boyle Stuckey, Interim Chief Information Officer (CIO), DHS, Office of Information Systems	30-Apr-13	31-May-13	[redacted]		X		X			

COMMENTS:
Agency: With respect to ACEDS (DHS) Deficiency 1, it appears that the scope of the findings has been broadened to include findings relative to OCTO Policy, and should not be attributed to DHS,ESA and ACEDS. However, ESA have a policy in place to address this issue. DHS is willing to convey this finding to OCTO for its response. DHS will likely revise some of these plans, given that key staff must provide feedback and approval of content next week.

DEFICIENCY #2	**ACEDS: 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.
RECOMMENDATION:	Related to Program Change controls, KPMG recommends 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. Documentation of these monitoring controls should be maintained and include sign-off of the review as well as notations as to the appropriateness of the actions taken by the developers within the database. Further, any suspicious activity, such as modifications to functionality or data without corresponding change request approvals, should be followed-up upon, as necessary. iii. Additionally, management should continue to document the performance of User Acceptance Testing (UAT). b. Configure settings or implement monitoring tools to log changes made to application functionality, including all configuration changes.

		AGENCY				OFOS				OIG		
			Dates			Ready for OIG Review?		OIG Notified?				
Action Plan Steps	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implemented**	**Not Implemented**

DEPARTMENT OF HUMAN SERVICES - ACEDS
CORRECTIVE ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

1 - Deficiency #2 ; Recommendation #a. i.	DHS was not budgeted funds in FY 2012 or FY 2013 to hire additional staff to fully segregate all program development roles from all production system and database administration roles. Moreover, there are not enough database tasks to maintain a fulltime Database Administrator.	Boyle Stuckey, Interim Chief Information Officer (CIO), DHS, Office of Information Systems	1-Apr-13	30-Sep-13	[redacted]		X		X			
2 - Deficiency #2 ; Recommendation #a. ii.	The recommendation to implement independently operated monitoring controls over the activities of the developers is addressed by OCTO, which utilizes its own tool to monitor and document all suspicious behavior. Once suspicious behavior is identified OCTO communicates it to the appropriate manager, who then follows up on the OCTO notification, takes the appropriate action and provides feedback to OCTO.	Boyle Stuckey, Interim Chief Information Officer (CIO), DHS, Office of Information Systems	4/1/2013	30-Sep-13	[redacted]		X		X			
3 - Deficiency #2 ; Recommendation #a. iii.	Management continues to document the performance of User Acceptance Testing (UAT). It should be noted that this recommendation was successfully addressed in the FY 2011 audit under NFR #IT-2011-01 and the auditor stated that "...we determined this specific aspect of the deficiency pertaining to the lack of maintenance of documentation to support UAT to be remedied."	Jeffrey Borkman, ESA Deputy Administrator, Division of Information Systems (DIS)	1-Apr-13	30-Sep-13	[redacted]		X		X			
4 Deficiency #2 ; Recommendation #b	OCTO maintains monitoring tools to log changes made to application functionality. All table changes are reviewed daily by Assistant Deputy Administrator for the Division of Information Services (DIS). The results of the review are maintained in a log of the daily report.	Jeffrey Borkman, ESA Deputy Administrator, Division of Information Systems (DIS); Catherine King, ESA, Asst. Deputy [redacted]	1-Apr-13	30-Sep-13	[redacted]		X		X			
7	c. The new change request application will require input from test and development stages in order to requests to be closed.											
8												
9												
10												

COMMENTS:

Agency: DHS will likely revise some of these plans, given that key staff must provide feedback and approval of content next week.

OFOS:

OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

UNIVERSITY OF THE DISTRICT OF COLUMBIA - BANNER
ACTION PLAN STATUS REPORT
AS OF:MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaiso	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The Elizabeth Jowi	(202) 442-8294 (202) 442-8306	Tiong.The@dc.gov Elizabeth.Jowi@dc.gov
Agency Liaisons:	UDC Data Center Albert Casciero	(202) 274-5941	
Financial Liaison:			
Program Liaison:			
Responsible ACFO:			

On Track?
Completed
Yes
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
3	2	

DEFICIENCY	**BANNER: 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

RECOMME	Related to Access to Programs and Data controls, KPMG recommends that management:

UNIVERSITY OF THE DISTRICT OF COLUMBIA - BANNER
ACTION PLAN STATUS REPORT
AS OF:MAY 28, 2013

NDATION:	
	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 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	Assess Management Procedures	Maria Byrd	10/01/2011	12/01/2012	Complete	X		X				
2	Controls and Segregation of duties	Maria Byrd	10/11/2013	10/01/2012	Complete	X		X				
3	Use of Genric IDs (Independent Monitoring)	Maria Byrd	06/12/2013	02/13/2013	Complete	X		X				
4												
5												

COMMENTS:
Agency:We have began to perform a periodic review of actions taken under these generic accounts and will continue.
OFOS:

DEFICIENCY	BANNER: 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.

UNIVERSITY OF THE DISTRICT OF COLUMBIA - BANNER
ACTION PLAN STATUS REPORT
AS OF:MAY 28, 2013

RECOMMENDATION:	Related to Program Change controls, KPMG recommends 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. Documentation of these monitoring controls should be maintained and include sign-off of the review as well as notations as to the appropriateness of the actions taken by the developers within the database. Further, any suspicious activity, such as modifications to functionality or data without corresponding change request approvals, should be followed-up upon, as necessary. iii. Additionally, management should continue to document the performance of User Acceptance Testing (UAT). b. Configure settings or implement monitoring tools to log changes made to application functionality, including all configuration changes.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	Change Management Process	Maria Byrd	10/01/2012	01/01/2013	Complete	X		X				
2												

COMMENTS:	
Agency:	
OFOS:	

DEFICIENCY	**BANNER: Program Development**

UNIVERSITY OF THE DISTRICT OF COLUMBIA - BANNER
ACTION PLAN STATUS REPORT
AS OF:MAY 28, 2013

	Conditions: 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. KPMG noted that formal testing and approval documentation was maintained during FY2012 to support the testing and approval for production migration of program changes; however, the prior year finding (FY2011) was determined to be only partially remediated because the following conditions still existed at the time of our audit: - Policies and procedures related to generic account management originally defined by management during FY2012 did not include requirements for logging and monitoring of actions taken under generic accounts. As a result, a series of generic accounts with the ability make changes, including 9 at the database layer, 19 at the operating system layer, and 33 at the application layer, held active access to the environment through FY2012. Of these accounts, a subset were tied to system processes and notprocedurally logged into by end users while others were no longer necessary to existwithin the environment. - While a complete list of patches applied to the application could be provided, changes impacting the functionality of the application made directly through the database during the period could not be produced in order to assess effectiveness of program change controls. 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. As part of our review in FY2012, Management implemented a policy requiring that the individual responsible for developing the change would not be the same individual responsible for migrating the change; however, the two developers with access to production remain able to circumvent this policy without detective controls to identify if such instances were to occur. 3. 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. As part of our assessment for FY2012, KPMG determined that new policies and procedures were implemented to: - Govern the use of generic accounts within the environment only when absolutely necessary to support a business or application function, and - Govern the change management process and the nature and extent of testing and approvals to be documented for program changes made to the application.
RECOMMENDATION:	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

		AGENCY				OFOS				OIG		
			Dates			Ready for OIG Review?		OIG Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Program Development Processes and Controls	Maria Byrd	10/01/2011	12/01/2012	Completed	X		X				
2												

UNIVERSITY OF THE DISTRICT OF COLUMBIA - BANNER
ACTION PLAN STATUS REPORT
AS OF:MAY 28, 2013

COMMENTS:
Agency:
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

DEPARTMENT OF EMPLYMENT SERVICES - BARTS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaiso	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO	Tony The	(202) 442-8294	Tiong.The@dc.gov
Liaison:	Elizabeth Jowi	(202) 442-8306	Elizabeth.Jowi@dc.gov
Agency Liais	Thomas Luparello	(202) 724-5096	Thomas.Luparello@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible	Bright Ahaiwe	(202) 442-6349	Bright.Ahaiwe@dc.gov

On Track?
Completed
[redacted]
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
1	1	

DEFICIENCY

Condition:

We tested management's process for removing access to the District of Columbia Government's computer systems after employee separation by comparing the active user listings from the Budget and Reporting Tracking System (BARTS) and the District Unemployment Tax Administration System (DUTAS) to the population of 92 Department of Employment Services (DOES) separated employees from FY2012, and noted two instances where separated employee's access was not removed after their date of termination. In performing additional evaluation procedures, we noted that these employees did not log into the BARTS and DUTAS applications after their termination dates. Further, in October 2012, we observed the BARTS and DUTAS accounts of the terminated users and noted that the two accounts were deactivated. While the evaluation procedures suggest that these accounts were not used in an unauthorized manner, management's failure to remove or disable them upon termination represents a control deficiency that continued to exist until the accounts were deactiviated.

NFR number: IT-2012-08

RECOMME

Recommendation:

DEPARTMENT OF EMPLYMENT SERVICES - BARTS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

NDATION: **Recommendation:**

We recommend that management re-emphasize the established process for communicating separations and removing separated employees' user access to the BARTS and DUTAS applications with all parties responsible for control performance to increase the consistency with which the process is followed.

Further, management should consider implementing a monitoring process by which weekly reports of terminated employees are received from HR and compared to active users within in-scope applications so that any matches can be further researched and have access removed as necessary.

Lastly, management should periodically monitor control performer adherence to these control activities.

NFR number: IT-2012-08

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	OIT Re-emphasiszes communication from HR	Tom Luparello	1/2/2013	1/7/2013	Completed	X		X				
2												

COMMENTS:

Agency: The two users in questions were not removed from systems in a timely manner due to an unusual miscommunication between Human Resources and the OIT department. It should however be noted that this issue would not have

OFOS:

DEFICIENCY **Condition:**

We reviewed the entire population of accounts with operating system and database administrative privileges supporting the Budget and Reporting Tracking System (BARTS) application and noted the following conditions:

1. Eight system and generic accounts with active access to administer the operating system no longer required these administrative privileges. Per inquiry of management, these accounts have not been procedurally utilized during FY2012 and knowledge of the passwords has been restricted to appropriate individuals. However, the active access for these accounts, which is no longer necessary, represents a weakness in the control environment.

2. Due to the configuration of the Windows SQL Server 2000 environment supporting the BARTS database, access to the "SA" generic account is shared by three individuals in addition to their unique accounts. Additionally, eight individuals with Domain Administrator privileges have access to administer the database supporting the BARTS application through the BUILTIN\Administrators conduit. Per inquiry of management, the individuals with Domain Administrator privileges have not procedurally used their access to administer the database; however, their access to administer the database, which does not commensurate with their job responsibilities, represents a weakness in the control environment.

NFR number: IT-2012-18

DEPARTMENT OF EMPLYMENT SERVICES - BARTS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

RECOMMENDATION:	**Recommendation:** We recommend that management establish and implement formalized operating system anc database security policies that, at a minimum, include consideration for following: • A process to log a ticket each time the "SA" account or other privileged system account is used and monitor the "SA" or other account activity against a change control log. Also ensure that passwords to "SA" or other privileged accounts are periodically changed anc immediately changed upon the separation of an individual with knowledge of the password. • A periodic review of all accounts with access to administer the operating system and database, which verifies the appropriateness of both generic accounts and individuals, including individuals who have privileged access assigned through conduit accounts (e.g. BUILTIN\Administrators). These requirements should be documented in a formalized policy/procedure that is provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis. **NFR number:** IT-2012-18

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	DB privileged access logs Review	Alex Adeduwon	5/1/2013	5/30/2013	Completed	X		X				
2												

COMMENTS:
Agency: The BARTS system/DB admin would be required to extract privileged access logs, on an at least semiannual basis, and submit to IT Security for review
OFOS:

DEFICIENCY	**Condition:** KPMG inspected the User Access Review that was performed for the Budget and Reporting Tracking System (BARTS) on 6/6/2012 and noted that the review was performed by a user who has the logical access rights required to administer security for the BARTS application. This combination of responsibilities within the access review process represents a segregation of duties conflict. **NFR number:** IT-2012-24
RECOMME	**Recommendation:**

DEPARTMENT OF EMPLYMENT SERVICES - BARTS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

NDATION:	**We recommend that management develop and formally document procedures for performing reviews that address and evaluate the appropriateness of the individuals performing the review, verify their ability to determine the appropriateness of access for each user, and ensure that the reviewers do not have additional responsibilities that will result in a lack of segregation of duties.** **Additionally, management should periodically monitor control performer adherence to these control activities.** **NFR number:** IT-2012-24

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	Refine Access Review Requirements (with emphasis on Reviewer)	Tom Luparello	4/30/2013	10/1/2013	Completed	X		X				
2												

COMMENTS:
Agency: The BPC chief (who validates authorized staff) was not available (on-site) during the documentation period and hence was not available to sign the review document. The review however was a collaborative effort between the
OFOS:

DEFICIENCY	**Condition:** **During FY2012, management did not perform official testing to confirm that the backup tapes related to the Budget and Reporting Tracking System (BARTS) can be successfully recovered and restored.** **NFR number:** IT-2012-30

RECOMME	**Recommendation:**

DEPARTMENT OF EMPLYMENT SERVICES - BARTS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

NDATION:	**We recommend that management implement policies and procedures to ensure that backup tapes are officially tested on a semi-annual basis to confirm successful recovery and restoration of data.** **Management should provide training to those responsible for performing these procedures and monitor to ensure adherence to the policy.** **NFR number:** IT-2012-30

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully implemented	Partially implement	Not implemented
1	Semi-Annual Testing of Back-up Tapes	Tom Luparello	6/1/2013	12/31/2013			X		X			
2												

COMMENTS:
Agency: Restoring backups from tape involves coordination between DOES and OCTO (the consolidated datacenter). OIT will review its operations and come up with a streamlined procedure that will afford such testing. It should however
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

CAMA SYSTEM - OTR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The	(202) 442-8294	Tiong.The@dc.gov
	Elizabeth Jowi	(202) 442-8306	Elizabeth.Jowi@dc.gov
Agency Liaisons:	James Hightower	(202) 478-9221	James Hightower@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible ACFO:			

On Track?
Completed
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)

DEFICIENCY #1

Condition:
During FY2012, a reconciliation process for the interface files transferred from the Computer Assisted Mass Appraisal (CAMA) system, "Vision", to the Tax Administration System (TAS) was not officially implemented. KPMG noted that there was no report available within TAS to evidence that the records from CAMA were successfully transferred.

In addition, a reconciliation process that verifies that the total number of records transferred from TAS equals to the total number of records transferred to CAMA was not officially implemented to complement the current error log review.

NFR number: IT-2012-31

RECOMMENDATION:

Recommendation:
We recommend that management design and implement the following:

- TAS file that includes sufficient information to verify the completeness and accuracy of the data transfer from CAMA to TAS in a timely manner;
- CAMA output file that includes sufficient information to verify the completeness and accuracy of the data transfer from TAS to CAMA in a timely manner;
- Formal reconciliation and error resolution process between the CAMA interface file and the designed TAS output file;
- Formal reconciliation and error resolution process between the TAS interface files and the designed detailed CAMA output file.

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

NFR number: IT-2012-31

CAMA SYSTEM - OTR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

		AGENCY				OFOS				OIG		
			Dates			Ready for OIG Review?		OIG Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Implement a report providing sufficient information to verify the completeness and accuracy of the data transfer from **the current version of CAMA (v6.4)** to TAS in a timely manner	Johnnie Simmons York	10/1/2012	12/31/2012	Completed	X		X				
2	Investigate the feasibility of implementing a report with sufficient information to verify the completeness and accuracy of the data transfer from TAS to the **current version of CAMA (v6.4)**. (see comments below)	Johnnie Simmons York	2/1/2013	4/1/2013	Completed	X		X				
3	As part of the project to upgrade CAMA to V7.0 implement a report providing sufficient information to verify the completeness and accuracy of the data transfer from the **upgraded version of CAMA** to TAS in a timely manner	Johnnie Simmons York	6/1/2013	9/30/2013			X		X			
4	As part of the project to upgrade CAMA to V7.0 implement a report providing sufficient information to verify the completeness and accuracy of the data transfer from TAS to the **upgraded version of CAMA** in a timely manner.	Johnnie Simmons York	6/1/2013	9/30/2013			X		X			
5	Implement a formal reconciliation and error resolution process between the CAMA export file and the designed TAS import file.	Robert Farr	6/1/2013	9/30/2013			X		X			
6	Implement a formal reconciliation and error resolution process between the CAMA import file and the designed TAS export file.	Robert Farr	6/1/2013	9/30/2013			X		X			

COMMENTS

Agency: For Action Plan Step 2: The recommended report to verify data transfer from TAS to CAMA must be written by the CAMA application vendor. Due to a heavy load of upgrade commitments to other clients the application vendor can n

DEFICIENCY #1	**Condition:** During our test work over privileged access for the operating system supporting CAMA, "Vision," KPMG noted that there were five Windows server administrative accounts that were shared by four to eleven individuals. These privileged accounts were used by IT personnel to perform maintenance functions for the Windows servers supporting the CAMA application. Per inquiry of management, there is an approval process in place before utilizing these accounts. However, management has not yet implemented a process to log and monitor the activities performed by these accounts.

CAMA SYSTEM - OTR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Additionally, two individuals retained server administration privileges after separation from the organization, after they no longer required access. Furthermore, one account associated with a business end user was not removed timely. While management informed KPMG that the business user was not aware of the account or the password for the account, the existence of the active operating system privileged account was not commensurate with the individual's business end responsibilities. **NFR number:** IT-2012-32
RECOMMENDATION:	**Recommendation:** **We recommend that management design and implement a combination of the following:** • **Re-assess the use and requirement of the shared privileged accounts including the associated access privileges;** • **Establish requirements that administration functions be performed by the appropriate personnel using unique user accounts;** • **Implement a formal pre-approval process and retain the approval documentation;** • **Implement a process, along with supporting mechanisms, by which operating system privileged account activity is logged, monitored, and documentation evidencing the review of this activity by an independent reviewer is maintained.** **Additionally, management should re-emphasize the established process for communicating separations and removing separated employees' access to the O/S supporting the CAMA application. Management should periodically monitor adherence to these control activities.** **NFR number:** IT-2012-32

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Implement a policy covering logical administrative access to application servers and desktops. This policy will require system administrators to login to servers using a non-generic account wherever possible. Where not possible, because of a network outage that prevents them from authenticating using their network ID, administrators will be allowed to login using a generic secadm account. All uses of the Secadm account will be monitored and reported using BlueLance LTAuditor tools, and the NetServ Manager will be required to investigate and document all such usage.	Rick Weil	2/1/2013	6/1/2013			X		X			

CAMA SYSTEM - OTR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

DEFICIENCY #1	**Condition:** KPMG noted that three users for the Computer Assisted Mass Appraisal (CAMA) system "Vision" had systematic access to perform all three functions of entering, reviewing, and approving assessment changes. In addition, monitoring controls over the three individuals' activities were not implemented to verify that the three stages for assessment changes have been performed by separate individuals. While management has deemed the three users' access appropriate to perform this function, the lack of segregation of duties between the entering, reviewing, and approving of assessment changes represents a weakness in the internal control environment for CAMA. NFR number: IT-2012-33
RECOMMENDATION:	**Recommendation:** We recommend that access restrictions over the ability to enter, review, and approve assessment changes within CAMA be refined and assigned to separate individuals based on principles of least privilege and appropriate segregation of duties. However, if system limitations prevent this from being implemented in a feasible manner, we recommend that management implement one or more independently operated monitoring controls over assessment changes within the CAMA application. This review should be: • Performed at a frequency determined by management (e.g. monthly or quarterly); • Performed by someone with knowledge of the changes, who does not individually have access to make the changes within the system; • Based on system-generated reports of assessment changes within the application; • Documented such that the follow up and resolution required for suspicious activity is clear and evidenced; and • Formally documented and signed by the reviewer. NFR number: IT-2012-33

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On-Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Implement in the upgraded version of CAMA (v7.0) restrictions over the ability to enter, review and approve assessment changes within CAMA so that these privileges can be refined and assigned to separate individuals based on least privileges and appropriate segregation of duties.	Johnnie Simmons York	6/1/2013	9/30/2013			X		X			

(OFOS Liaison/FCRD Director/Deputy Controller)

CAMA SYSTEM - OTR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

DEFICIENCY #1	**Condition:** There were 13 Oracle accounts with database administrator privileges shared by four to six individuals that included both IT and business end user personnel. The privileged accounts were used to perform maintenance functions, such as installing security patches and expanding table spaces, on the Oracle databases supporting the Computer Assisted Mass Appraisal (CAMA) system as well as mass uploads of assessment changes through direct on-line database (ODBC) connections. Per inquiry of management, there is an approval process in place before utilizing these accounts. However, management has not yet implemented logging and monitoring capabilities at the database-level to capture the activities performed by these and other database administrator accounts systematically. **NFR number:** IT-2012-34
RECOMMENDATION:	**Recommendation:** We recommend that management take the following actions in remediation of the condition above: • Revoke the logical access rights held by business end users to make mass changes to the CAMA database through ODBC connections, and implement a process by which mass update files are prepared by the appropriate business end users, approved by appropriate management personnel, and then provided to database administrators for implementation into production. • Implement database monitoring capabilities to log direct data changes made by both unique and generic accounts at the database level. The specific changes logged should be determined by management, but may include additions, changes, and deletions made to critical data tables housing information supporting assessment values as well as database schema supporting this application. Additionally, management should perform and document a periodic review of changes made directly at the database level to ensure that that all changes were authorized and appropriate. **NFR number:** IT-2012-34

		AGENCY				OFOS				OIG		
			Dates			Ready for OIG Review?		OIG Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Identify the most appropriate method to control logical access rights currently held by the business end users to make mass changes to the CAMA database	Jim Hightower	4/8/2013	6/1/2013			X		X			
2	Implement the method identified to control logical access rights currently held by the business end users to make mass changes to the CAMA database	Johnnnie Simmons York	6/1/2013	9/30/2013			X		X			

CAMA SYSTEM - OTR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

3	Implement database monitoring capabilities to log direct data changes made by both unique and generic accounts at the database level.	Sandy Pinder	6/1/2013	9/30/2013	[redacted]		X		X			
4	Perform and document a periodic review of changes made directly at the the database level to ensure that all changes were authorized and appropriate	Robert Farr	6/1/2013	9/30/2013	[redacted]		X		X			

DEFICIENCY #1	**Condition:** **At the time of review, the accounts with database administration privileges supporting the Computer Assisted Mass Appraisal (CAMA) System, "Vision", did not have password requirements such as minimum length and complexity configured.** **NFR number:** IT-2012-35

RECOMMENDATION:	**Recommendation:** **We recommend that management implement configuration settings for database passwords for all accounts that adhere to the OCFO/OCIO password policy, where feasible. For system accounts for which password expiration settings cannot be systematically enforced, management should consider implementing a process to protect and periodically change these passwords as well as to track and monitor usage.** **NFR number:** IT-2012-35

		AGENCY				OFOS				OIG		
			Dates			Ready for OIG Review?		OIG Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented

CAMA SYSTEM - OTR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

1	In the upgraded CAMA application implement the OCFO password configuration policies at the application, database and operating system levels.	Sandy Pinder (database), Rick Weil (OS) and Johnnie Simmons York (application)	6/1/2103	9/30/2013	[redacted]		X		X			
2	For operating system accounts for which password expiration settings cannot be systematically enforced, implement a process to protect and periodically change these passwords. In cases where this is not feasible, track and monitor usage of the operating system accounts	Rick Weil (OS)	2/1/2013	6/1/2013	[redacted]		X		X			

DEFICIENCY #1	**Condition:** Three application security administrators possessed conflicting responsibilities as business end users who had access to administer security for the applications within the Computer Assisted Mass Appraisal (CAMA) System, "Vision". While management has deemed their access appropriate to perform this function, the lack of segregation of duties between the application security administration and business end user functions represents a weakness in the internal control environment for CAMA. **NFR number:** IT-2012-36
RECOMMENDATION:	**Recommendation:** We recommend that management continue and complete the process to implement the segregation of duties controls started during FY12 and, at the minimum, develop and implement controls that establish one or more of the following: • Implement access configuration within the CAMA application that will allow the segregation of duties between business end user privileges from security administration privileges; • Document and periodically review policies and procedures that define the job functions authorized by management to have access to the CAMA administrator roles; • Define organizational and logical segregation of duties related to production system support, user security administration, and general business user roles among different individuals; and/or • Implement of one or more independently operated monitoring controls over the activities of individuals with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system. **NFR number:** IT-2012-36

AGENCY			OFOS		OIO		
	Dates		Ready for OIO Review?	OIO Notified?			

CAMA SYSTEM - OTR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implem	Partially Implem	Not Implem
1	Implement segregation of duties between the application security administrator and business end user functions within the **current version of CAMA (v6.4).**	Jim Hightower	12/1/2012	2/1/2013	Completed	X		X				
2	Implement segregation of duties between the application security administrator and business end user functions within the **upgraded version of CAMA (v7.0).**	Johnnie Simmons York	6/1/2013	9/30/2013	[redacted]		X		X			
3	Document and periodically review access privileges granted to CAMA users on a periodic basis within the current version of CAMA (v6.4)	Robert Farr	1/1/2013	On going	Completed	X		X				
4	Document and periodically review access privileges granted to CAMA users on a periodic basis within the upgraded version of CAMA (v7.0).	Robert Farr	6/1/2013	9/30/2013	[redacted]		X		X			
5	Define organization and logical segregation of duties related to CAMA production support, user security administration and general business user roles among different individuals.	Jim Hightower	6/1/2013	9/30/2013	[redacted]		X		X			
6												

DEFICIENCY #1	**Criteria:** **As part of its financial statement audit methodology, KPMG executes tests of General Information Technology (GITC) controls in the areas of access to programs and data, program changes, program development, and computer operations. Our internal framework for identifying and testing 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).** **NFR number:** IT-2012-37

CAMA SYSTEM - OTR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

RECOMMENDATION:	**Recommendation:** **We recommend that management implement policies and procedures to ensure that backup tapes are tested on a semi-annual basis to confirm successful recovery and restoration of data.** **Management should provide training to those responsible for performing these procedures and monitor to ensure adherence to the policy.** **NFR number:** IT-2012-37

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Implement a local Disaster Recovery enclave that will be used to validate on a yearly basis our ability to recover the CAMA application from backup tapes.	Rick Weil	6/1/2013	9/30/2013			X		X			

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

Jim Hightower 04/26/13

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

DEPARTMENT OF EMPLOYMENT SERVICES - DOCS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaiso	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The Elizabeth Jowi	(202) 442-8294 (202) 442-8306	Tiong.The@dc.gov Elizabeth.Jowi@dc.gov
Agency Liais	Thomas Luparello	(202) 724-5096	Thomas.Luparello@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible	Bright Ahaiwe	(202) 442-6349	Bright.Ahaiwe@dc.gov

On Track?
Completed
Yes
At Risk
No

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
3	1	

DEFICIENCY	**Condition:** KPMG observed the entire population of Security Administrators for the District Online Compensation System (DOCS) and the District Unemployment Tax Administration System (DUTAS) applications and noted two of the DUTAS and one of the DOCS users with access to administer security possessed conflicting responsibilities as either developers or business end users who had access to administer security for the applications. Specifically, we noted that two developers had access to administer security for the DUTAS application and one business user had the ability to administer security for the DOCS application. Management has deemed the access of these individuals appropriate to perform this function and has indicated the individuals only possess this level of access in a backup capacity rather than as the primary security administrators for the applications. However, lack of segregation of duties between these functions represents a weakness in the internal control environment for these two applications. **NFR number:** IT-2012-15
RECOMMENDATION:	**Recommendation:** We recommend that management develop and implement controls that establish one or more of the following: - Document and periodically review policies and procedures that define the job functions authorized by management to have access to the DOCS and DUTAS administrator roles; - Define organizational and logical segregation of duties related to production system support, user security administration, and general business user roles among different individuals; and/or - Implement of one or more independently operated monitoring controls over the activities of individuals with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system. Additionally, management should periodically monitor control performer adherence to these control activities. **NFR number:** IT-2012-15

AGENCY	OFOS	OIO

DEPARTMENT OF EMPLOYMENT SERVICES - DOCS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

Action Plan	Description	Lead	Dates		On Track?	Ready for OIO Review?		OIO Notified?		Fully Implemented	Partially Implemented	Not Implemented
			Start	Completion		Yes	No	Yes	No			
1	Segregation of Duties	Tom Luparello	1/7/2011	6/2/2011	Completed	X		X				
2	Priviledged user Activity Monitoring	Gil and OCTO	5/1/2013	5/1/2014			X		X			
3	UI Job Function Definitions documentation	Patrick Holmes	6/1/2013	6/1/2014			X		X			
4												

COMMENTS:

Agency:

1. Access to DUTAS Security administration (ability to assign transaction windows to users) should be viewed within DOES's context. Two of the individuals mentioned (Gil and Zarath) are the only OIT DUTAS system support personnel. The third user (Patrick Holmes) has a compliance role. Segregation of duties is already implemented based on the fact that there are other administrators assigned to other systems who do not have jurisdiction in DUTAS.
2. It should be noted that OCTO monitors unauthorized attempt to browse datasets. Such attempts are flagged and alerts are sent to DOES upon such discovery. DOES then investigates affected user. Ability to fully incorporate additional capabilities for monitoring, logging and reporting of developer/admin activities would require OCTO's input. DUTAS application is sitting on a development platform owned by OCTO. The acquisition of modules and update on such development platform, required to support possible incorporation of advance monitoring capabilities, is outside of DOES's jurisdiction. If OCTO does no purchase required components and give access to DOES developers to build requirments, this action will not be feasible.
3. Job function definition documents as it relates to access to UI systems relies heavily on the office of Unemployment Service at DOES and corresponding resources available to support such objective.

DEFICIENCY

Condition:
KPMG reviewed the entire population of individuals with access to modify data and make application program changes to the District Online Compensation System (DOCS) and the District Unemployment Tax Administration System (DUTAS) applications and determined:

1) One individual with development responsibilities has access to migrate changes to production for DOCS and DUTAS through access to the load library using the employee's own login ID to the system. This user also has access to modify the backend data for the DOCS and DUTAS applications.

2) A series of users were determined to no longer require access to DOCS and DUTAS production datasets, which provides users the ability to modify production data and programs. Those with access include three Department of Employment Services (DOES) personnel and eleven Office of the Chief Technology Officer (OCTO) personnel for the DOCS application and five OCTO systems programmers for DUTAS.

NFR number: IT-2012-16

RECOMMENDATION:

Recommendation:
We recommend that management enhance the current DOES application periodic access review process to review those individuals and accounts with access to make changes to production mainframe supporting DOCS and DUTAS. This review should be consistently performed and documented by data owners with knowledge of the appropriateness of the access rights held to these mainframe datasets and without access to administer security at the Resource Access Control Facility (RACF) mainframe level.

NFR number: IT-2012-16

DEPARTMENT OF EMPLOYMENT SERVICES - DOCS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	Incorporate Datasets access to Review	Alex Adeduwon	10/19/2012	10/31/2012	Completed	X		X				
2												

COMMENTS:

Agency: Users who had access to datasets in question had their roles transitioned to a different group and hence, no longer needed such access. Others served as back administrators. Affected users' accesses were removed as part of our October system access review exercise.

DEFICIENCY

Condition:

KPMG noted that 29 out of 42 users with the ability to add or modify wage information per their system access rights within the District Online Compensation System (DOCS) application did not require this level of access in accordance with their job responsibilities.

NFR number: IT-2012-29

RECOMMENDATION:

Recommendation:

We recommend that access restrictions over the ability to update wage information within DOCS be refined to restrict access based on principles of least privilege including restricting to read-only in production access those IT personnel who are responsible for advanced troubleshooting within the application.

However, if system limitations prevent this from being implemented in a feasible manner, we recommend that management implement an independently-operated monitoring control over changes to wage information within the DOCS application. This review should be:

- Performed at a frequency determined by management (monthly or quarterly);
- Performed by someone with knowledge of the changes, who does individually have access to make the changes within the system;
- Based on system-generated reports of wage changes within the application; and,
- Formally documented and signed by the reviewer.

NFR number: IT-2012-29

DEPARTMENT OF EMPLOYMENT SERVICES - DOCS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

		AGENCY				OFOS				OIG		
			Dates			Ready for OIG Review?		OIG Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	Research incorporating granular wage update capability to DOCS	Alex Adeduwon	6/1/2013	6/1/2014	[redacted]		X		X			
2												

COMMENTS:
Agency: If system or other limitations prevents feasible implementation of above action plan, other proposed reccomendations will be considered, as practically feasible.
OFOS:
OIG:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

DEPARTMENT OF EMPLOYMENT SERVICES - DUTAS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaiso	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The Elizabeth Jowi	(202) 442-8294 (202) 442-8306	Tiong.The@dc.gov Elizabeth.Jowi@dc.gov
Agency Liais	Thomas Luparello	(202) 724-5096	Thomas.Luparello@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible	Bright Ahaiwe	(202) 442-6349	Bright.Ahaiwe@dc.gov

On Track?
Completed
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
1	1	

DEFICIENCY

Condition:
We tested management's process for removing access to the District of Columbia Government's computer systems after employee separation by comparing the active user listings from the Budget and Reporting Tracking System (BARTS) and the District Unemployment Tax Administration System (DUTAS) to the population of 92 Department of Employment Services (DOES) separated employees from FY2012, and noted two instances where separated employee's access was not removed after their date of termination. In performing additional evaluation procedures, we noted that these employees did not log into the BARTS and DUTAS applications after their termination dates. Further, in October 2012, we observed the BARTS and DUTAS accounts of the terminated users and noted that the two accounts were deactivated. While the evaluation procedures suggest that these accounts were not used in an unauthorized manner, management's failure to remove or disable them upon termination represents a control deficiency that continued to exist until the accounts were deactiviated.

NFR number: IT-2012-08

RECOMMENDATION:

Recommendation:
We recommend that management re-emphasize the established process for communicating separations and removing separated employees' user access to the BARTS and DUTAS applications with all parties responsible for control performance to increase the consistency with which the process is followed.

Further, management should consider implementing a monitoring process by which weekly reports of terminated employees are received from HR and compared to active users within in-scope applications so that any matches can be further researched and have access removed as necessary.

Lastly, management should periodically monitor control performer adherence to these control activities.

NFR number: IT-2012-08

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully implemented	Partially implemented	Not implemented
1	OIT Re-emphasiszes communication from HR	Tom Luparello	1/2/2013	1/7/2013	Completed	X		X				
2												

COMMENTS:

DEPARTMENT OF EMPLOYMENT SERVICES - DUTAS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

Agency:
The two users in questions were not removed from systems in a timely manner due to an unusual miscommunication between Human Resources and the OIT department. It should however be noted that this issue would not have gone undiscovered, due to DOES's existing periodic system access review process.

DEFICIENCY

Condition:
KPMG observed the entire population of Security Administrators for the District Online Compensation System (DOCS) and the District Unemployment Tax Administration System (DUTAS) applications and noted two of the DUTAS and one of the DOCS users with access to administer security possessed conflicting responsibilities as either developers or business end users who had access to administer security for the applications. Specifically, we noted that two developers had access to administer security for the DUTAS application and one business user had the ability to administer security for the DOCS application. Management has deemed the access of these individuals appropriate to perform this function and has indicated the individuals only possess this level of access in a backup capacity rather than as the primary security administrators for the applications. However, lack of segregation of duties between these functions represents a weakness in the internal control environment for these two applications.

NFR number: IT-2012-15

RECOMMENDATION:

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

- Document and periodically review policies and procedures that define the job functions authorized by management to have access to the DOCS and DUTAS administrator roles;
- Define organizational and logical segregation of duties related to production system support, user security administration, and general business user roles among different individuals; and/or
- Implement of one or more independently operated monitoring controls over the activities of individuals with administrative access that require the documentation of monitoring activities as well as follow up on any suspicious behavior within the system.

Additionally, management should periodically monitor control performer adherence to these control activities.

NFR number: IT-2012-15

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	Segregation of Duties	Tom Luparello	1/7/2011	6/2/2011	Completed	X		X				
2	Priviledged user Activity Monitoring	Gil and OCTO	5/1/2013	5/1/2014			X		X			
3	UI Job Function Definitions documentation	Patrick Holmes	6/1/2013	6/1/2014			X		X			
4												

COMMENTS:

DEPARTMENT OF EMPLOYMENT SERVICES - DUTAS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

Agency:	**1.** Access to DUTAS Security administration (ability to assign transaction windows to users) should be viewed within DOES's context. Two of the individuals mentioned (Gil and Zarath) are the only OIT DUTAS system support personnel. The third user (Patrick Holmes) has a compliance role. Segregation of duties is already implemented based on the fact that there are other administrators assigned to other systems who do not have jurisdiction in DUTAS. **2.** It should be noted that OCTO monitors unauthorized attempt to browse datasets. Such attempts are flagged and alerts are sent to DOES upon such discovery. DOES then investigates affected user. Ability to fully incorporate additional capabilities for monitoring, logging and reporting of developer/admin activities would require OCTO's input. DUTAS application is sitting on a development platform owned by OCTO. The acquisition of modules and update on such development platform, required to support possible incorporation of advance monitoring capabilities, is outside of DOES's jurisdiction. If OCTO does no purchase required components and give access to DOES developers to build requirments, this action will not be feasible. **3.** Job function definition documents as it relates to access to UI systems relies heavily on the office of Unemployment Service at DOES and corresponding resources available to support such objective.
OFOS:	

DEFICIENCY	**Condition:** KPMG reviewed the entire population of individuals with access to modify data and make application program changes to the District Online Compensation System (DOCS) and the District Unemployment Tax Administration System (DUTAS) applications and determined: 1) One individual with development responsibilities has access to migrate changes to production for DOCS and DUTAS through access to the load library using the employee's own login ID to the system. This user also has access to modify the backend data for the DOCS and DUTAS applications. 2) A series of users were determined to no longer require access to DOCS and DUTAS production datasets, which provides users the ability to modify production data and programs. Those with access include three Department of Employment Services (DOES) personnel and eleven Office of the Chief Technology Officer (OCTO) personnel for the DOCS application and five OCTO systems programmers for DUTAS. **NFR number:** IT-2012-16

RECOMMENDATION:	**Recommendation:** We recommend that management enhance the current DOES application periodic access review process to review those individuals and accounts with access to make changes to production mainframe supporting DOCS and DUTAS. This review should be consistently performed and documented by data owners with knowledge of the appropriateness of the access rights held to these mainframe datasets and without access to administer security at the Resource Access Control Facility (RACF) mainframe level. **NFR number:** IT-2012-16

AGENCY	OFOS	OIO

DEPARTMENT OF EMPLOYMENT SERVICES - DUTAS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Incorporate Datasets access to Review	Alex Adeduwon	10/19/2012	#########	Completed	X		X				
2												

COMMENTS:
Agency: Users who had access to datasets in question had their roles transitioned to a different group and hence, no longer needed such access. Others served as back administrators. Affected users' accesses were removed as part of our October system access review exercise.
OFOS:

DEFICIENCY

Condition:
For one of three new users granted access to the District Unemployment Tax Administration System (DUTAS) application during the fiscal year 2012 and selected by KPMG for testing, there was no notation on the access request form submitted for this user indicating the specific level of access to DUTAS that should be provisioned even though this user was granted access greater than read-only into the application. While KPMG determined the access rights assigned to be appropriate for the user identified above, this lack of documentation represents a weakness in the new user provisioning process.

NFR number: IT-2012-17

RECOMMENDATION:

Recommendation:
We recommend that management re-emphasize the established process for granting new user access to the DUTAS application and formally indicate and approve the specific access that should be granted to new DUTAS users with all parties responsible for control performance to increase the consistency with which the process is followed. Additionally, management should periodically monitor control performer adherence to these control activities.

NFR number: IT-2012-17

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Re-ephasize proper use of Quickbase	Alex Adeduwon	12/7/2012	#########	Completed	X		X				
2												

COMMENTS:

DEPARTMENT OF EMPLOYMENT SERVICES - DUTAS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

Agency: The particular access requests in question did not indicate specifically which transaction windows were being requested. It should however be noted, that the request did indicate the users' job role. The job role, common to both users, is known, as a matter of default, to require read only access to screens required for such a role to perform associated duties. This finding has however been noted and future requests will be required to check off all appropriate options checkboxes in the quickbase application before implementation. No inappropriate access was granted.

OFOS:

DEFICIENCY

Condition:
KPMG reviewed the last program change date for a selection of modules and noted that, for one of three modules changed during FY2012, the change was not reflected in the manual listing that is used for tracking program changes for the District Unemployment Tax Administration System (DUTAS). In addition, documentation that supported the testing and approval of this specific change was not available.

NFR number: IT-2012-23

RECOMMENDATION:

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

- Management should re-emphasize the established process for tracking, testing, and approving program changes to the DUTAS application production environment with all parties responsible for control performance to increase the consistency with which the process is followed. The manual log should be consistently updated for every change applied to the production environment and it should capture the load library modules impacted by the change. Additionally, management should periodically monitor control performer adherence to these control activities.
- Additionally, management should investigate opportunities to migrate to a more automated process to track changes and change control documentation for DUTAS. This may include leveraging software or tools to request, document, and approve program changes.

NFR number: IT-2012-23

		AGENCY				OFOS				OIG		
			Dates			Ready for OIG Review?		OIG Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Re-emphasize change Control Procedure	Alex Adeduwon	12/2/2012	#########	Completed	X		X				
2	Migrate to an Automated CCB	Tom Luparello	6/1/2013	4/1/2014			X		X			
3												

COMMENTS:

DEPARTMENT OF EMPLOYMENT SERVICES - DUTAS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

Agency: **1.** System administrator used his discretion due to the nature of system change. The policy will however be re-enforced to ensure that all program changes go through appropriate testing, documentation and authorization whenever such is required **2.** Automated change control process will be considered
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

OFFICE OF THE CHIEF FINANCIAL OFFICER - INOVAH
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The	(202) 442-8294	Tiong.The@dc.gov
	Elizabeth Jowi	(202) 442-8306	Elizabeth.Jowi@dc.gov
Agency Liaisons:	Clarice Wood	(202) 727-0760	Clarice.Wood@dc.gov
	Donna McKenzie	(202) 727-0805	Donna.McKenzie@dc.gov
	Lillian Copelin	(202) 727-7697	Lillian.Copelin@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible ACFO:			

On Track?
Completed
[redacted]
At Risk
[redacted]

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)

DEFICIENCY #1	**INOVAH: 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.
RECOMMENDATION:	Related to Access to Programs and Data controls, KPMG recommends that management:

OFFICE OF THE CHIEF FINANCIAL OFFICER - INOVAH
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	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 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.

		AGENCY				OFOS				OIO		
			Dates			Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	Review/Revise iNovah Access Policy	Wood/McKenzie	4/22/2013	8/30/2013	YES							
2	Review/Revise iNovah Roles	Wood/McKenzie	4/22/2013	8/30/2013	YES							
3	Review/Revise Policy for Generic ID's	Copelin	4/22/2013	8/30/2013	YES							
4	Review/Revise Server Access Policy	Copelin	4/22/2013	8/30/2013	YES							

COMMENTS:
Agency:
OFOS:
OIO:

DEFICIENCY #2	**INOVAH: 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.

OFFICE OF THE CHIEF FINANCIAL OFFICER - INOVAH
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

RECOMMENDATION:	Related to Program Change controls, KPMG recommends 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. Documentation of these monitoring controls should be maintained and include sign-off of the review as well as notations as to the appropriateness of the actions taken by the developers within the database. Further, any suspicious activity, such as modifications to functionality or data without corresponding change request approvals, should be followed-up upon, as necessary. iii. Additionally, management should continue to document the performance of User Acceptance Testing (UAT). b. Configure settings or implement monitoring tools to log changes made to application functionality, including all configuration changes.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Review/Revise iNovah Change Mgt Policy	Copelin	4/22/2013	8/30/2013	YES							
2	Review/Revise iNovah Config Monitoring	Wood/McKenzie	4/22/2013	8/30/2013	YES							

COMMENTS:
Agency:
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

_____

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

_____

(OFOS Liaison/FCRD Director/Deputy Controller)

NOT-FOR-PROFIT HOSPITAL CORPORATION - MEDITECH
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaiso	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The Elizabeth Jowi	(202) 442-8294 (202) 442-8306	Tiong.The@dc.gov Elizabeth.Jowi@dc.gov
Agency Liais	Ron Walker	(202) 574-6611	rwalker@united-medicalcenter.com
Financial Liaison:			
Program Liaison:			
Responsible	Ron Walker	(202) 574-6611	rwalker@united-medicalcenter.com

On Track?
Completed
Yes
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
4	2	

DEFICIENCY	**Passwords** Conditions: During our review of the password requirements for the Medical Information Technology, Inc. (MEDITECH) Health Care Information System (HCIS), we noted the following areas in which the enforced password settings did not align with the Medical Center Password Policy: a). Password parameters for the network supporting the MEDITECH HCIS have been configured to include complexity or account lockout requirements, and minimum length has been configured to only six characters rather than the eight character minimum outlined in the policy noted above. b). Password parameters for the MEDITECH HCIS have not been configured to include complexity, password history, or account lockout requirements and minimum outlined in the policy noted above.
RECOMMENDATION:	We recommend that management reconfigure existing password configuration settings at application, the operating system, and database level, where applicable, in accordance with the Medical Center Password Management Policy, which includes requirements for enabling password complexity and requiring a password length of eight characters.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	Extend the minimum length required to 8 characters for passwords.	Janice Akintewe	1/17/2013	2/1/2013	Completed	X		X				
2	Passwords changed to alpha-numeric.	Janice Akintewe	1/17/2013	2/1/2013	Completed	X		X				
3	Update policy to reflect change in passwords.	Janice Akintewe	2/1/2013	5/9/2013	Completed	X		X				
4	Obtain approvals and add onto intranet	Janice Akintewe	5/9/2013	6/30/2013	Yes		X		X			
5												

COMMENTS:	
Agency:	

DEFICIENCY	**Periodic Application Access Review**

NOT-FOR-PROFIT HOSPITAL CORPORATION - MEDITECH
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

During our control test work over the periodic access review process for the Medical Information Technology, Inc. (MEDITECH) Health Care Information System (HCIS), we noted that the Director of IT performs an access review by which users and and roles are randomly selected to be evaluated for appropriateness of access. However, the following conditions were noted to be present within this process:

1). The review is performed by an individual with the ability to grant or modify access for the application, rather than by an independent business owner. This combination of conflicting responsibilities represents weakness within the control environment.

2). Since the review captures one user or role at random, it does not comrehensively cover all users possessing greater than read-only application access on a consistent time-period basis.

RECOMMENDATION: We recommend that management refine the current periodic access review process to include the following characteristics, which will strengthen it to consistently capture and remediate, in a comprehensive manner, cases of excessive access privileges stemming from either changes in job functions or unauthorized modifications to access rights:

* The review should be comprehensive of all user IDs with greater than read-only privileges to the application, which is performed quarterly or semi-annually depending on considerations such as the volume of user access and likelihood of changes, the operation and strength of access controls around provisioning, de-provisioning, and management of changes for transfers, and the relative risk of the system with respect to operational and financial importance to the company.

* The review should be conducted by business owners that are knowledgeable and can certify appropriateness of user access within the system and who do not also have access to modify users and privileges.

* The review should be based upon system-generated reports, even if these reports are re-formatted into Excel to facilitate the review process.

* The required changes resulting from the review should be remediated within one week of the required change being identified.

* The results of the review, including the original review access reports reviewed and management's requested changes and sign-off of the review, should be documented for audit trail purposes.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	IT to provide business owners access listing for the roles of staff in their areas; to review and sign off on for appropriateness.	Janice Akintewe	4/10/2013	6/1/2013	Yes		X		X			
2	Business owners will review and either approve c	Janice Akintewe	4/10/2013	6/1/2013	Yes		X		X			
3	Identified changes made to access within one week of the review as recommended when possible.	Janice Akintewe	4/10/2013	6/1/2013	Yes		X		X			
4	IT to work with key stakeholders to review, modi	Janice Akintewe	4/10/2013	6/1/2013	Yes		X		X			
5	IT to work with business owners with defining the	Janice Akintewe	4/10/2013	6/1/2013	Yes		X		X			
6												

COMMENTS:

Agency:

NOT-FOR-PROFIT HOSPITAL CORPORATION - MEDITECH
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

DEFICIENCY	**MEDITECH Vendor Access Review** During our fiscal year 2011 audit, we were informed by Medical Center management and representatives of the Medical Center's primary health care information system (HCIS) vendor, Medical Information Technology, Inc. (MEDITECH), that as many as over 3,000 MEDITECH employees may have write-level or greater remote access to UMC's instance of MEDITECH. The current support model from MEDITECH allows the vendor to have full access to the MEDITECH production system on an ongoing basis to support UMC's request for technical support, enhancements, changes, and to apply software updates as needed. Although MEDITECH remote user access to the HCIS was tracked in audit logs available on MEDITECH's customer portal, UMC management was not proactively reviewing the logs on a periodic basis to determine whether the vendor's remote access wa authorized by the Medical Center's Information Technology department. A review process was implemented by management during fiscal year 2012 and was documented beginning July 20, 2012 in remediation of the issue noted above. However, a deficiency int he control environment existed for the period during the year under audit of October 1, 2011 through July 19, 2012.
RECOMMENDATION:	While we consider this condition to be remediated, we recommend that UMC IT enable the configuration within their Help Desk workflow to log the specific individual on the Help Desk staff who has completed the review of MEDITECH remote access for the date in question.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement.**	**Not Implemented**
1	Modify daily help desk log so that it is checked-off when a review has been performed.	Shahzad Ahmed	1/1/2013	1/1/2013	**Completed**	X		X				
2												

COMMENTS:
Agency:
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

OFFICE OF THE CHIEF TECHNOLOGY OFFICER - PASS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The	(202) 442-8294	Tiong.The@dc.gov
	Elizabeth Jowi	(202) 442-8306	Elizabeth.Jowi@dc.gov
Agency Liaisons:	Shirley Kwan-Hui (Main)	(202) 727-5625	Shirley.Kwan-Hui@dc.gov
	Melanie Nathan	(202) 724-2017	Melanie.nathan@dc.gov
	David Jennings	(202) 727-5316	David.Jennings@dc.gov
	Felix Liderman	(202) 724-5130	Felix.Liderman@dc.gov
	Bill Machen	(202) 727-8793	Bill.Machen@dc.gov
Financial Liaison:			
	Dervel Reed	(202) 741-8836	Dervel.Reed@dc.gov
Program Liaison:	Tegene Baharu	(202) 727-7349	Tegene.Baharu@dc.gov
Responsible ACFO:	Phil Peng	(202)-727-8472	Phil.Peng@dc.gov

On Track?
Completed
Yes
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)

DEFICIENCY #1	**PASS: 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.
RECOMMENDATION:	Related to Access to Programs and Data controls, KPMG recommends 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.

OFFICE OF THE CHIEF TECHNOLOGY OFFICER - PASS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	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 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
For Condition #2 (NFR IT-2012-12): 2.1	As part of the datacenter upgrade effort, OCTO is implementing and maintaining a stricter control of access requirements to the datacenter floor.	David Jennings	7/1/2012	8/30/2013	Yes							
2.2	Removal of Access from other agencies except DGS, MPD and EOM	David Jennings	10/1/2012	12/31/2012	Completed	X						
2.3	Development of access policies and procedures and maintain relevancy of documentation	David Jennings	10/1/2012	12/31/2012	Completed	X						
2.5	Additional physical access and security monitoring controls will be implemented as part of the datacenter upgrade project.	David Jennings	10/1/2012	9/30/2013	Yes							
2.6	Maintain on-going process of monthly review of access requests	David Jennings	1/2/2013	9/30/2013	Yes							
2.7	Complete follow-up process for users requesting temporary access and disabling access of terminated users.	David Jennings	10/1/2012	9/30/2013	Yes							
2.8	Complete Training appropriate personnel in the access process request to ensure compliance and commitment to established policies and processes. (Additional Training will be done as needed throughout the fiscal year.)	David Jennings	10/1/2012	1/31/2013	Completed	X						
For Condition #3 (NFR IT-2012-05): 3.1	Create a "Default_DBA" profile for the DBAs to remediate the password requirement condition to administer Oracle database for both PeopleSoft and PASS.	Felix Liderman Other: Ajay Damireddy	10/9/2012	10/9/2012	Completed	X						
3.2	Testing, procurement and installation of the Database Activity Monitoring (DAM) tool.	Bill Machen Other: Felix Liderman	5/15/2012	3/4/2013	Completed	X						

OFFICE OF THE CHIEF TECHNOLOGY OFFICER - PASS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

3.3	Provide audit monitoring of PASS/PeopleSoft databases. Detect and Maintain On-going Operational procedures during fiscal year.	Bill Machen	3/4/2013	9/30/2013	[redacted]							
COMMENTS:												
Agency: Condition# 1 does not apply to PASS, only to PeopleSoft (see NFR# IT-2012-07); Condition# 4 has been remediated on August 31st, 2012 as noted in NFR# IT-2012-4 and Yellow Book Report on Pg. A-1 and A-2.												
OFOS:												
OIO:												

DEFICIENCY #2	**PASS: 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.
RECOMMENDATION:	Related to Program Change controls, KPMG recommends 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. Documentation of these monitoring controls should be maintained and include sign-off of the review as well as notations as to the appropriateness of the actions taken by the developers within the database. Further, any suspicious activity, such as modifications to functionality or data without corresponding change request approvals, should be followed-up upon, as necessary. iii. Additionally, management should continue to document the performance of User Acceptance Testing (UAT). b. Configure settings or implement monitoring tools to log changes made to application functionality, including all configuration changes.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implemented**	**Not Implemented**
For Condition #3 (NFR IT-2012-05): 3.1	Create a "Default_DBA" profile for the DBAs to to remediate the password requirement condition to administer Oracle database for both PeopleSoft and PASS.	Felix Liderman Other: Ajay Damireddy	10/9/2012	10/9/2012	**Completed**	X						
3.2	Testing, procurement and installation of the Database Activity Monitoring (DAM) tool.	Bill Machen Other: Felix Liderman	5/15/2012	3/4/2013	**Completed**	X						

OFFICE OF THE CHIEF TECHNOLOGY OFFICER - PASS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

3.3	Provide audit monitoring of PASS/PeopleSoft databases. Detect and Maintain On-going Operational procedures during fiscal year.	Bill Machen	3/4/2013	9/30/2013	[redacted]							

COMMENTS:
Agency: Condition# 2 and #3 do not apply to PASS.
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

OFFICE OF THE CHIEF TECHNOLOGY OFFICER - PEOPLESOFT
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The	(202) 442-8294	Tiong.The@dc.gov
	Elizabeth Jowi	(202) 442-8306	Elizabeth.Jowi@dc.gov
Agency Liaisons:	Shirley Kwan-Hui (Main)	(202) 727-5625	Shirley.Kwan-Hui@dc.gov
	Melanie Nathan	(202) 724-2017	Melanie.nathan@dc.gov
	David Jennings	(202) 727-5316	David.Jennings@dc.gov
	Felix Liderman	(202) 724-5130	Felix.Liderman@dc.gov
	Bill Machen	(202) 727-8793	Bill.Machen@dc.gov
Financial Liaison:			
Program Liaison:	Dervel Reed	(202) 741-8836	Dervel.Reed@dc.gov
	Tegene Baharu	(202) 727-7349	Tegene.Baharu@dc.gov
Responsible ACFO:	Phil Peng	(202)-727-8472	Phil.Peng@dc.gov

On Track?
Completed
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)

DEFICIENCY #1

PEOPLESOFT: 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.

RECOMMENDATION:

Related to Access to Programs and Data controls, KPMG recommends 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 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.

OFFICE OF THE CHIEF TECHNOLOGY OFFICER - PEOPLESOFT
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

		AGENCY				OFOS				OIG		
			Dates			Ready for OIG Review?		OIG Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
For Condition #1 (NFR IT-2012-07): 1.1	Develop ERP policy to govern PeopleSoft Security Adminstration	CWITS	10/1/2012	3/19/2013	Completed	X						
1.2	Develop technical process for remediation of PeopleSoft User Security administration	Felix Liderman	10/1/2012	4/17/2013	Completed	X						
1.3	Development of PeopleSoft Security Administration Unit in CWITS	Bill Machen	10/1/2012	6/30/2013	[redacted]							
1.4	Provide quarterly review of PeopleSoft Application Access	Bill Machen Others: DCHR, OPRS and other District Agencies	7/1/2013	9/30/2013	[redacted]							
For Condition #2 (NFR IT-2012-12): 2.1	As part of the datacenter upgrade effort, OCTO is implementing and maintaining a stricter control of access requirements to the datacenter floor.	David Jennings	7/1/2012	8/30/2013	[redacted]							
2.2	Removal of Access from other agencies except DGS, MPD and EOM	David Jennings	10/1/2012	12/31/2012	Completed	X						
2.3	Development of access policies and procedures and maintain relevancy of documentation	David Jennings	10/1/2012	12/31/2012	Completed	X						
2.5	Additional physical access and security monitoring controls will be implemented as part of the datacenter upgrade project.	David Jennings	10/1/2012	9/30/2013	[redacted]							
2.6	Maintain on-going process of monthly review of access requests	David Jennings	1/2/2013	9/30/2013	[redacted]							
2.7	Complete follow-up process for users requesting temporary access and disabling access of terminated users.	David Jennings	10/1/2012	9/30/2013	[redacted]							
2.8	Complete Training appropriate personnel in the access process request to ensure compliance and commitment to established policies and processes. (Additional Training will be done as needed throughout the fiscal year.)	David Jennings	10/1/2012	1/31/2013	Completed	X						
For Condition #3 (NFR IT-2012-05): 3.1	Create a "Default_DBA" profile for the DBAs to to remediate the password requirement condition to administer Oracle database for both PeopleSoft and PASS.	Felix Liderman Other: Ajay Damireddy	10/9/2012	10/9/2012	Completed	X						
3.2	Testing, procurement and installation of the Database Activity Monitoring (DAM) tool.	Bill Machen Other: Felix Liderman	5/15/2012	8/4/2013	Completed	X						

OFFICE OF THE CHIEF TECHNOLOGY OFFICER - PEOPLESOFT
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

3.3	Provide audit monitoring of PASS/PeopleSoft databases. Detect and Maintain On-going Operational procedures during fiscal year.	Bill Machen	3/4/2013	9/30/2013	[redacted]								

COMMENTS:
Agency: Condition# 4 has been remediated on August 31st, 2012 as noted in NFR# IT-2012-4 and Yellow Book Report on Pg. A-1 and A-2.
OFOS:
OIO:

DEFICIENCY #2	**PEOPLESOFT: 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.
RECOMMENDATION:	Related to Program Change controls, KPMG recommends 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. Documentation of these monitoring controls should be maintained and include sign-off of the review as well as notations as to the appropriateness of the actions taken by the developers within the database. Further, any suspicious activity, such as modifications to functionality or data without corresponding change request approvals, should be followed-up upon, as necessary. iii. Additionally, management should continue to document the performance of User Acceptance Testing (UAT).

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
2012-05):	Create a "Default_DBA" profile for the DBAs to	Felix Liderman	10/9/2012	10/9/2012	Completed	X						
3.2	Testing, procurement and installation of the Database Activity Monitoring (DAM) tool.	Bill Machen Other: Felix Liderman	5/15/2012	3/4/2013	Completed	X						
3.3	Provide audit monitoring of PASS/PeopleSoft databases. Detect and Maintain On-going Operational procedures during fiscal year.	Bill Machen	3/4/2013	9/30/2013	[redacted]							

COMMENTS:
Agency: Condition# 2 and #3 do not apply to PASS.
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

OFFICE OF THE CHIEF TECHNOLOGY OFFICER - PEOPLESOFT
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

(OFOS Liaison/FCRD Director/Deputy Controller)

OFFICE OF THE CHIEF FINANCIAL OFFICER - SOAR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaiso	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The	(202) 442-8294	Tiong.The@dc.gov
	Elizabeth Jowi	(202) 442-8306	Elizabeth.Jowi@dc.gov
Agency Liaisons:	David Pivec Lillian	(202) 478-1424	David.Pivec@dc.gov
	Copelin	(202) 727-7697	Lillian.Copelin@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible ACFO:			

On Track?
Completed
Yes
At Risk
No

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
1		

DEFICIENCY	**SOAR: 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.

RECOMMENDATION:	Related to Program Change controls, KPMG recommends 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. Documentation of these monitoring controls should be maintained and include sign-off of the review as well as notations as to the appropriateness of the actions taken by the developers within the database. Further, any suspicious activity, such as modifications to functionality or data without corresponding change request approvals, should be followed-up upon, as necessary. iii. Additionally, management should continue to document the performance of User Acceptance Testing (UAT). b. Configure settings or implement monitoring tools to log changes made to application functionality, including all configuration changes.

OFFICE OF THE CHIEF FINANCIAL OFFICER - SOAR
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Design and Implement Monitoring Controls over Developer activities	Lillian Copelin	May 1 2013	Sep 30 2013	Yes		X		X			
2												

COMMENTS:
Agency:
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

TACIS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The	(202) 442-8294	Tiong.The@dc.gov
	Elizabeth Jowi	(202) 442-8306	Elizabeth.Jowi@dc.gov
Agency Liaisons:	Loretta Walker	(202) 727-4317	Loretta.Walker@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible ACFO:	Angelique Hayes	(202) 673-3341	Angelique.Hayes@dc.gov

On Track?
Completed
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
100%		

DEFICIENCY #1	**TACIS: 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.
RECOMMENDATION:	Related to Access to Programs and Data controls, KPMG recommends 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.

TACIS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	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 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Segregation of duties involving the contract developer from mitigrating changes to programs/data into production was implemented.	Keely Williams	Nov-11	Nov-11	Completed							
2	New procedures were implemented for approving all systems/user access changes.	Keely Williams	Feb-11	Feb-11	Completed							
3	Created month reports of all systems/user access changes.	Keely Williams	Nov-11	Nov-11	Completed							
4	Reconciles all change requests forms to the monthly report.	Keely Williams	Nov-11	Nov-11	Completed							

COMMENTS:
Agency: Action plan steps 2-4 are on-going since program/user access changes occur frequently.
OFOS:
OIO:

DEFICIENCY #2	**TACIS: 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.

TACIS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

RECOMMENDATION:	Related to Program Change controls, KPMG recommends 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. Documentation of these monitoring controls should be maintained and include sign-off of the review as well as notations as to the appropriateness of the actions taken by the developers within the database. Further, any suspicious activity, such as modifications to functionality or data without corresponding change request approvals, should be followed-up upon, as necessary. iii. Additionally, management should continue to document the performance of User Acceptance Testing (UAT). b. Configure settings or implement monitoring tools to log changes made to application functionality, including all configuration changes.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Segregaton of contract developer duties from mitigrating changes in production have been implemented.	Keely Williams	Nov-11	Nov-11	Completed							
2	Monthly reports are generated and reconciled for all system/access change requests	Keely Williams	Feb-11	Feb-11	Completed							

COMMENTS:
Agency: Action plan step number two (2) will be an on-going process to reconcile system/access changes to the related monthly reports.
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

_____Angelique R. Hayes_____
(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

_____
(OFOS Liaison/FCRD Director/Deputy Controller)

OFFICE OF THE CHIEF FINANCIAL OFFICER - TAS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Jesse Dolojan	(202) 442-8331	Jesse.Dolojan@dc.gov
OIO Liaison:	Tony The	(202) 442-8294	Tiong.The@dc.gov
	Elizabeth Jowi	(202) 442-8306	Elizabeth.Jowi@dc.gov
Agency Liaisons:	James Hightower	(202) 478-9221	James Hightower@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible ACFO:			

On Track?
Completed
[redacted]
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)

DEFICIENCY #1

Condition:

We tested management's process for removing access to the District of Columbia Government's computer systems after employee separation by comparing the active user listings from the Tax Administration System (TAS) to a list of separated employees, and noted two instances where separated employee's access was not removed from after their date of termination date. In addition, we noted that two of these three individuals were not captured and removed through the quarterly periodic access review control designed to capture these employees with terminated access.

In performing additional evaluation procedures, we noted that these employees did not log into the TAS application after their termination date. Further, in October 2012, we observed the TAS accounts of the terminated users and noted that the three accounts were deactivated. While the evaluation procedures suggest that these accounts were not used in an unauthorized manner, management's failure to remove or disable them upon termination represented a control deficiency that continued to exist until the accounts were deactivated.

NFR number: IT-2012-10

RECOMMENDATION:

Recommendation:

We recommend that management consistently follow the formally documented process for communicating and removing separated employees' access to TAS. Further, management should re-emphasize and train managers on the specific requirements to be addressed in completing the quarterly periodic reviews of access for the TAS application. Lastly, management should periodically monitor control performer adherence to these control activities.

OFFICE OF THE CHIEF FINANCIAL OFFICER - TAS
ACTION PLAN STATUS REPORT
AS OF: MAY 28, 2013

NFR number: IT-2012-10

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Re-emphasize and train managers on specific requirements to be addresses in completing the quarterly periodic reviews of access for the TAS application	Jim Hightower	1/2/2013	3/1/2013	Completed	X		X				
2	Implement an additional quarterly separated-employee review procedure to compare a list of separated employees provided from the OCFO PeopleSoft Human Capital Management System against the list of active users in TAS.	Jim Hightower	3/3/2013	On going	Completed	X		X				
3												
4												
5												
6												

COMMENTS

Agency:

OFOS:

OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

Jim Hightower 04/26/2013

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

PROCUREMENT AND DISBURSEMENT CONTROLS

OFFICE OF CONTRACTING AND PROCUREMENT
ACTION PLAN STATUS REPORT
As of: 05-24-2013

	Name	Phone Number	Email Address
OFOS Liaison:	Cassandra Alexander	(202) 442-8314	cassandra.alexander@dc.gov
OIO Liaison:	Esther Sawyer	(202) 442-8276	esther.sawyer@dc.gov
	John Cashmon	(202) 442-8297	john.cashmon@dc.gov
Agency Liaisons:	N/A		
Financial Liaison:	Shilonda Wiggins	(202) 727-6535	shilonda.wiggins@dc.gov
Program Liaison:	Yinka Alao	(202) 724-4089	yinka.alao@dc.gov
Responsible ACFO:	Mohamed Mohamed	(202) 727-8178	mohamed.mohamed@dc.gov

On Track?
Completed
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
4		

DEFICIENCY #1	Sole Source Procurements - (a) For 10 of 38 sole source procurements, there was not sufficient documentation to validate that the sole source method was justified; (b) For 1 of 38 sole source procurements tested, Council approval was not available for review; (c) For 1 of 38 sole source procurements, the Determination and Findings was not available for review; (d) for 1 of 38 sole source procurements, the purchase order amount was greater than the contract amount by $150,000; and (e) For 1 of 38 sole source procurements, the contract did not cover the period of the purchase order.
RECOMMENDATION:	The District should continue to strengthen its internal controls over procurement through the implementation of 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Continue with the execution of pre-award Notice of Intent to Award Sole Source (NIAS) reviews and post-award Sole Source contract audits	OCP Office of Procurement Integrity and Compliance	10/1/2011	9/30/2013								
2	Continue with the periodic issuance of Bellwether Reports and Summary Statistics to EOM and OCFO representatives	OCP Office of Procurement Integrity and Compliance	10/1/2011	9/30/2013								
3	Schedule mandatory 'All Hands' CAFR Briefing with procurement staff and OCP delegation holders	OCP Office of Procurement Integrity and Compliance	3/11/2013	3/11/2013								
4	Issue CAFR Remediation notices detailing audit findings to affected Commodity Managers	OCP Office of Procurement Integrity and Compliance	3/11/2013	3/11/2013								
5	Schedule follow-up meetings with affected Commodity Managers	OCP Office of Procurement Integrity and Compliance	5/3/2013	7/30/2013								
6	Automate notification and tracking process for policy and procedural updates	OCP Office of Procurement Integrity and Compliance in collaboration with OCP's IT Division	2/19/2013	5/3/2013								

7	Draft and issue series of critical operational directives to clarify procurement practice and strengthen internal controls.	OCP Office of Procurement Integrity and Compliance in collaboration with OCP's Legal Counsel and Senior Management	10/1/2012	5/3/2013									
8	Execute enhancements to records room and file tracking procedures (active and legacy paper files) to include: (a) complete and accessible contract file inventory; (b)upgrades to physical security; (c) check-in/check-out procedures; (d) updated records retention policy; and (e) automated file tracking and reconcillation capabilities	OCP Office of Procurement Integrity and Compliance	2/8/2013	5/31/2013									

COMMENTS:	
Agency: Items (1) and (2) were implemented at the beginning of FY2012 as a direct response to the results of the FY2010 CAFR in accordance with OCP's multi-year remediation plan. These audit programs will continue throughout FY2013. Item 6 addresses an NFR in the FY2011 CAFR pertaining to the lack of a systematic approach to updating and maintaining policy and directives. The series of critical operational directives cited in item 7 above are as follows: (a) Procurement Review Committee; (b) Contract File Maintenance (e-records); (c) File Transfer Protocol; (d) Disciplinary Action (Escalation Policy for Non-Compliance); (e) Check-in/Checkout Procedures (paper records); (f) OCP Acquisition Planning. Together, these action steps address all the deficiencies in the FY12 CAFR.	
OFOS:	
OIO:	
DEFICIENCY #2	**Sole Source Procurements** (Department of General Services) - For 1 of 2 DGS sole source procurements, the procurement file was not available for review; and (b) for 1 of 2 DGS sole source procurements, the contractor's delegation of authority was not available for review.

RECOMMENDATION:	The District should continue to strengthen its internal controls over procurement through the implementation of 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implemented**	**Not Implemented**
1	Grant independent agency access to online Control Self Assessment (CSA), and follow-up as needed.	OCP Office of Procurement Integrity and Compliance	4/30/2013	9/30/2013								

COMMENTS:	
Agency: Consistent with OCP's management response to the FY12 CAFR, and a notable departure from our approach in the previous audit cycle, we will share best practices and lessons learned through this medium. The results of the CSA may trigger follow-up discussions. Please note that this is not mandatory and follow-up is dependent on whether the independent agency participates and/or if the responses highlight significant gaps in the interpretation and application of procurement rules. Also, please note that the cited DGS procurement was included in the OCP sample due to misclassification in the General Ledger (per Independent Auditor). This issue needs to be addressed.	
OFOS:	
OIO:	
DEFICIENCY #3	**Emergency Procurements** - (a) For 5 of 13 emergency procurements, there was not sufficient documentation to validate that the emergency procurement method was justified; (b) For 1 of 13 emergency procurements, the

	determination and finding (D & F) was not made available for review; and (c) For 3 of 13 emergency procurements, the period of performance exceeded the 120 day maximum duration requirement for an emergency procurement.

RECOMMENDATION:	The District should continue to strengthen its internal controls over procurement through the implementation of 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Please reference action steps detailed for Deficiency #1.	OCP Office of Procurement Integrity and Compliance	10/1/2011	9/30/2013								

COMMENTS:
Agency: Items (1) and (2) were implemented at the beginning of FY2012 as a direct response to the results of the FY2010 CAFR in accordance with OCP's multi-year remediation plan. Item 6 addresses an NFR in the FY2011 CAFR pertaining to the lack of a systematic approach to updating and maintaining policy and directives. The series of critical operational directives cited in item 7 above are as follows: (a) Procurement Review Committee; (b) Contract File Maintenance (e-records); (c) File Transfer Protocol; (d) Disciplinary Action (Escalation Policy for Non-Compliance); (e) Check-in/Checkout Procedures (paper records); (f) OCP Acquisition Planning. Together, these action steps address all the deficiencies in the FY12 CAFR.
OFOS:
OIO:

DEFICIENCY #4	**Emergency Procurements** (Department of General Services) - (a) For one DGS emergency procurement, the contracting officer's delegation of authority was not available for review.

RECOMMENDATION:	The District should continue to strengthen its internal controls over procurement through the implementation of 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Grant independent agency access to online Control Self Assessment (CSA), and follow-up as needed.	OCP Office of Procurement Integrity and Compliance	4/30/2013	9/30/2013								

COMMENTS:
Agency: Consistent with OCP's management response to the FY12 CAFR, and a notable departure from our approach in the previous audit cycle, we will share best practices and lessons learned through this medium. The results of the CSA may trigger follow-up discussions. Please note that this is not mandatory and follow-up is dependent on whether the independent agency participates and/or if the responses highlight significant gaps in the interpretation and application of procurement rules. Also, please note that the cited DGS procurement was included in the OCP sample due to misclassification in the General Ledger (per Independent Auditor). This issue needs to be addressed.
OFOS:
OIO:

OFFICE OF CONTRACTING AND PROCUREMENT
ACTION PLAN STATUS REPORT
As of: 05-24-2013

DEFICIENCY #5	**Competitive Procurements** - (a) For 30 of 131 competitive procurements, there was no evidence that the procurement went through the competitive process; (b) For 2 of 131 competitive procurements, evidence of Council approval was not available for review; (c) For 15 of 131 competitive procurements, evidence of the excluded party list review was not available; (d) For 1 of 131 competitive procurements, evidence of review of the contractor's compliance with District tax code was not available for review; (e) For 1 of 131 competitive procurements, there were insufficient quotes available for review for small purchases; (f) For 1 of 131 competitive procurements, the contract was missing the authorizing signature; (g) For 2 of 131 competitive procurements, the contract was not available for review; and (h) For 1 of 131 competitive procurements, the contract was not available for review.

RECOMMENDATION:	The District should continue to strengthen its internal controls over procurement through the implementation of 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implemented**	**Not Implemented**
1	Please reference action steps detailed for Deficiency #1.	OCP Office of Procurement Integrity and Compliance	10/1/2011	9/30/2013								

COMMENTS:
Agency:
OFOS:
OIO:

DEFICIENCY #6	**Competitive Procurements** (Department of Health) - (a) For 7 of 9 agreements, the determination and finding was not available for review; (b) For 3 of 9 agreements, the period of performance noted in the agreement did not cover the period being audited; (c) For 1 of 9 agreements, the agreement was not available for review; (d) For 1 of 9 agreements, the Attorney General's legal review/approval was not available for review; (e) For 2 of 9 agreements, evidence of the excluded party list was not available for review; and (f) For 4 of 9 agreements, evidence of contractor compliance with District tax code was not available for review.

RECOMMENDATION:	The District should continue to strengthen its internal controls over procurement through the implementation of 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implemented**	**Not Implemented**
1	Grant independent agency access to online Control Self Assessment (CSA), and follow-up as needed.	OCP Office of Procurement Integrity and Compliance	4/30/2013	9/30/2013								

COMMENTS:
Agency: Consistent with OCP's management response to the FY12 CAFR, and a notable departure from our approach in the previous audit cycle, we will share best practices and lessons learned through this medium. The results of the CSA may trigger follow-up discussions. Please note that this is not mandatory and follow-up is dependent on whether the independent agency participates and/or if the responses highlight significant gaps in the interpretation and application of procurement rules. Also, please note that the cited DOH procurement was included in the OCP sample due to misclassification in the General Ledger (per Independent Auditor). This issue needs to be addressed.
OFOS:
OIO:

OFFICE OF CONTRACTING AND PROCUREMENT
ACTION PLAN STATUS REPORT
As of: 05-24-2013

DEFICIENCY #7	**Competitive Procurements** (Department of General Services) - (a) For 2 of 2 DGS competitive procurements, there were insufficient quotes available for review for the small purchases.

RECOMMENDATION:	The District should continue to strengthen its internal controls over procurement through the implementation of 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.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implemented**	**Not Implemented**
1	Grant independent agency access to online Control Self Assessment (CSA), and follow-up as needed.	OCP Office of Procurement Integrity and Compliance	4/30/2013	9/30/2013								

COMMENTS:

Agency: Consistent with OCP's management response to the FY12 CAFR, and a notable departure from our approach in the previous audit cycle, we will share best practices and lessons learned through this medium. The results of the CSA may trigger follow-up discussions. Please note that this is not mandatory and follow-up is dependent on whether the independent agency participates and/or if the responses highlight significant gaps in the interpretation and application of procurement rules. Also, please note that the cited DGS procurement was included in the OCP sample due to misclassification in the General Ledger (per Independent Auditor). This issue needs to be addressed.

OFOS: Action Step 1 implemented but will continue throughout the fiscal year.

OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

	Name	Phone Number	Email Address
OFOS Liaison:	Cassandra Alexander	(202) 442-8314	cassandra.alexander@dc.gov
OIO Liaison:	Esther Sawyer	(202) 442-8276	esther.sawyer@dc.gov
	John Cashmon	(202) 442-8297	john.cashmon@dc.gov
Agency Liaisons:	Joe Giddis		
Financial Liaison:			
Program Liaison:			
	Joe Giddis	(202) 442-6428	joseph.giddis@dc.gov
Responsible ACFO:			

On Track?
Completed
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
X		

DEFICIENCY #1	**Sole Source Procurements** - (a) For 2 of 25 sole source procurements, the use of the sole source procurement method was not justified.

RECOMMENDATION:	The District should continue to strengthen its internal controls over procurement through the implementation of 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.

OFFICE OF CONTRACTING AND PROCUREMENT
ACTION PLAN STATUS REPORT
As of: 05-24-2013

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Establish Policy covering SSP/CE	Drakus Wiggins	Feb-13	Apr-13	Completed	X		X				
2												
3												
4												
5												
6												

COMMENTS:
Agency: Office of Contracts, Policy establishes the internal process for sole source and contract extensions. Review of contract files are reviewed in preparation for auditreview by Contracting Officers and Contract Specialists
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the Independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

DC PUBLIC SCHOOLS
ACTION PLAN STATUS REPORT
AS OF: MAY 24, 2013

	Name	Phone Number	Email Address	On Track?
OFOS Liaison:	Cassandra Alexander	202) 442-831	cassandra.alexander@	Completed
OIO Liaison:	Esther Sawyer	202) 442-827	esther.sawyer@dc.gov	Yes
	John Cashmon	202) 442-829	john.cashmon@dc.gov	
Agency Liaisons:				At Risk
Financial Liaison:	Munetsi Musara	202) 442-528	munetsi.musara@dc.g	
Program Liaison:	Glorious Bazemore	202) 442-511	glorious.bazemore@dcps.gov	
	Anthony DeGuzman	202) 442-511	anthony.deguzman@dc.gov	
Responsible ACFO:	Deloras Shepherd	202) 442-513	deloras.shepherd@dc.gov	

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)

DEFICIENCY #1	For 3 of 180 purchase order files, the files did not originally include a search for federal debarment. For 1 of 64 contract files for payment, the file did not include the required Determination and Findings. For 1 purchase order and contract file for payment, the purchase order file and contract file were not provided by DCPS.

RECOMMENDATION:	No specific recommendation provided in the Yellow Book Report by KPMG.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Conduct refresher training regarding required supporting documentation for each file, inclusive of Determination and Findings and Debarment.	Glorious Baz	6/1/2013	6/30/2013	Yes							
2	Review OCA filing and retention policies and revise as necessary	Glorious Baz	6/1/2013	6/30/2013	Yes							
3	Distribute filing and document retention policies to staff with formal communication	Glorious Baz	6/1/2013	6/30/2013	Yes							
4												
5												
6												
7												
8												
9												
10												

COMMENTS:
Agency:
OFOS:
OIO:

DC PUBLIC SCHOOLS
ACTION PLAN STATUS REPORT
AS OF: MAY 24, 2013

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

OFFICE OF CONTRACTING AND PROCUREMENT
ACTION PLAN STATUS REPORT
AS OF: MAY 24, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Michelle McNaughton	202-442-8286	michelle.mcnaughton@dc.gov
OIO Liaison:	Esther Sawyer	202-442-8276	esther.sawyer@dc.gov
Agency Liaisons:	Shilonda Wiggins	202-727-6535	shilonda.wiggins@dc.gov
	Yinka Alao	202-724-4089	yinka.alao@dc.gov
Responsible ACFO:	Mohamed Mohamed	202-727-8178	mohamed.mohamed@dc.gov

On Track?
Completed
Yes
At Risk

# Completed (Per Agency)	# Ready for Review	# Verified as Completed (Per

DEFICIENCY #1	For 22 of the monthly reconciliations totaling $3,304,205 of the 36 monthly reconciliations tested totaling $4,349,614, we noted that the reconciliations were not reviewed and approved by the approving official in a timely manner in accordance with OCP Policy No.2009-01. Of the 22 exceptions we noted the following Agencies did not comply with the policy: - Fire and Emergency Medical Services (7) - Metropolitan Police Department (3) - Office of Tenant Advocate (3) - Office of the Mayor (4) - Office of the Secretary (1) - DC Public Library 1) - Office of Contracting & Procurement (3) b. For 5 individual transactions totaling $15,090 out of 40 transactions tested totaling $252,456, there was not sufficient documentation to support the purchase or validate that it was for an approved transaction. All 5 exceptions were from the Office of Tenant Advocate. c. For 2 individual transactions totaling $11,850 out of 40 transactions tested totaling $252,456, we noted that the authorizer approved purchases exceeding the $2,500 single and $10,000 cycle transaction limit, these exceptions related to the Office of the Mayor and the Metropolitan Police Department. d. For 3 monthly statements totaling $134,343 of 36 monthly statements totaling $4,349,614, we noted that 2 cardholders exceeded their approved cycle limit for the months reviewed. These exceptions related to Fire and Emergency Services and the Office of Tenant Advocate. e. For 1 transaction totaling $100,411 out of 40 transactions tested totaling $252,456, the cardholder exceeded the small purchase limit of $100,000 per PPRA Sec. 407 small
RECOMMENDATION:	**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.

OFFICE OF CONTRACTING AND PROCUREMENT
ACTION PLAN STATUS REPORT
AS OF: MAY 24, 2013

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified ?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Issuance (and reissuance for agencies with new leadership) of Responsibility Acknowledgement Letters certified by Agency Directors.	OCP PCard PMO and the OCP Office of Procurement Integrity and Compliance.	10/1/2012	9/30/2013								
2	Continue with the execution of desk and field audits.	OCP Office of Procurement Integrity and Compliance.	10/1/2012	9/30/2013								

COMMENTS:
Agency: As communicated in the FY10 and FY11 audit cycles, the majority of these findings are attributable to the quality of program oversight and surveillance reporting performed by each Agency Review Teams (ART). As part of the
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

OFFICE OF FINANCIAL OPERATIONS AND SYSTEMS
ACTION PLAN STATUS REPORT
AS OF: MAY 24, 2013

	Name	Phone Number	Email Address	On Track?
OFOS Liaison:	Deena Parker	202-442-8291	deena.parker@dc.gov	Completed
	Esther Sawyer	202-442-8276	esther.sawyer@dc.gov	
OIO Liaison:	Hassan Shode	202-442-8275	hassan.shode@dc.gov	
Agency Liaisons:				At Risk
Financial Liaison:	Martha Hopkins		martha.hopkins@dc.gov	
Program Liaison:	Tim Musara	202-442-5280	munetsi.musara@dc.gov	
Responsible ACFO:	Deloras Shepherd	202-442-5135	deloras.shepherd@dc.gov	

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)
2	2	

DEFICIENCY #1	**(a.)** 1 of 67 District payments (i.e. non-DCPS) selected for testing were not paid timely in accordance with the Quick Payment Act and **(b.)** 100 of 426 DCPS payments selected for testing were not paid timely in accordance with the Quick Payment Act.
RECOMMENDATION:	There was no specific recommendation regarding the QPA in the Yellow Book report. However, per the Findings & Recommendations, KPMG recommended that: the Agency ACFO strenghten their controls surrounding the payment of expenditures to ensure that they are being compliant with the requirements of the Quick Payment Act.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	CFOSolve Query for QPA Compliance Rate needs to be tweaked: Set up meeting with HSSC and OFOS to discuss report revision needed.	MARTHA HOPKINS	4/10/2013	5/10/2013								
2	Prepare and distribute a memorandum to DCPS requesting: (1) explanations/reasons for DCPS late payments and, (2) what actions will be taken to ensure future prompt payment.	MARTHA HOPKINS	4/10/2013	4/11/2013	C[redacted]D	X		X				
3	Request Organization Development and Learning (OD&L) assistance for training development.	MARTHA HOPKINS	4/10/2013	4/24/2013	C[redacted]D	X		X				
4	Invite OD&L, DCPS, OCFO Legal and OFOS for a "QPA Training Brain-Storming" meeting.	MARTHA HOPKINS	5/1/2013	5/30/2013								
5	OD&L develops an OCFO QPA Training Class and Schedule.	MARTHA HOPKINS	6/1/2013	8/31/2013								

COMMENTS:

STEP 1: Agency does not have the skill set to fix the identified problems with the CFOSolve query. OFOS has to identify a resource to fix the problem.
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any circumstances that will impede progress or prevent completion of any corrective action plan steps.

RESPONSIBLE AGENCY REPRESENTATIVE (AGY DIRECTOR, PROGRAM MGR, FISCAL STAFF)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

OFOS LIAISON/FCRD DIRECTOR/DEPUTY CONTROLLER

TAX REVENUE ACCOUNTING AND REPORTING

OFFICE OF TAX AND REVENUE
ACTION PLAN STATUS REPORT
AS OF: MAY 24, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Tong Yu	202 442 8301	tong.yu@dc.gov
OIO Liaison:	Tisha Edwards	202 442 6446	tisha.edwards@dc.gov
	Prince Washaya	202 442 8274	prince.washaya@dc.gov
Agency Liaisons:	Beth Spooner	202 442 6486	beth.spooner@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible ACFO:			

On Track?
Completed
Yes
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)

DEFICIENCY # a	Individual settlements associated with Superior Court Appeals are usually less than the $200,000 threshold used. As a result, most outstanding Superior Court Appeals related to property tax assessments are not being assessed for inclusion in the District's fiscal year end claims and judgment accrual. This resulted in an understatement of the accrual due to property tax assessments of approximately $58 million as of September 30, 2012. District management subsequently recorded an adjustment to correct for this understatement in its 2012 government-wide financial statements.
RECOMMENDATION:	We recommend that OTR strengthen its policies, procedures and controls to ensure that the above noted deficiencies are addressed.

		AGENCY				OFOS				OIO		
			Dates			Ready for OIO Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implemented	Not Implemented
1	Settled Court Cases-RPTA created a Settlement/Court Order Tracking file (excel) of all settled court cases and relate court orders.	Doug Collica	9/30/2011	9/30/2011	Completed	Yes						
2	RPTA will develop a file (excel) of court orders for confirmation of refund status (paid or unpaid).	Doug Collica	9/30/2013	9/30/2013	Yes							
3	RPTA will develop a file (excel) for RAA.	Doug Collica	9/30/2013	9/30/2013	Yes							
4	Pending Court Cases- RPTA will create from the 3rd Level Appeals Tracking System a file (excel) of pending court orders.	Doug Collica	9/30/2013	9/30/2013	Yes							
5	RPTA will develop a reconciliation process between ITS and 3rd Level Appeals Tracking System data.	Doug Collica	9/30/2013	9/30/2013	Yes							
6	RPTA will develop a file (excel) for RAA.	Doug Collica	9/30/2013	9/30/2013	Yes							
7	RPTA will establish policies and procedures to address the District's fiscal year end claims and judgment accrual.	Stephen Cappello	4/12/2013	6/28/2013	Yes							

COMMENTS:	
Agency:	
OFOS:	
OIO:	
DEFICIENCY # b	OTR records accounts receivables for Sales & Use and Personal Income taxes at the fully realizable amount instead of applying the one-year availability criteria to the balances. This resulted in an understatement

OFFICE OF TAX AND REVENUE
ACTION PLAN STATUS REPORT
AS OF: MAY 24, 2013

	of deferred revenue of approximately $5.5 million and $17.4 million for Sales & Use and Personal Income taxes, respectively.

RECOMMENDATION:	We recommend that OTR strengthen its policies, procedures and controls to ensure that the above noted deficiencies are addressed.

		AGENCY				OFOS				OIO		
			Dates			Review?		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement**	**Not Implemented**
1	Update policy and procedure #35302003, "Preparing the Revenue Lead Sheet"	Bert Molina	27-Mar-13	24-Apr-13	**Completed**	Yes						
2	Format "Expected AR Collections in FY 2014" work papers for all the applicable tax types for use at fiscal year-end.	Bert Molina	22-Apr-13	30-Apr-13	**Completed**	Yes						

COMMENTS:	
Agency:	
OFOS:	
OIO:	

DEFICIENCY # c	We noted that there is no formal review process in place to check the completeness and accuracy of the information uploaded into ITS from FoxPro.

RECOMMENDATION:	We recommend that OTR strengthen its policies, procedures and controls to ensure that the above noted deficiencies are addressed.

		AGENCY				OFOS				OIO		
			Dates			Review?		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement**	**Not Implemented**
1	Systematic Interface (Roll Corrections) TSG created a nightly import log that specifically identifies all value and/or use code changes.	TSG	10/1/2012	10/1/2012	**Completed**	Yes						
2	RPTA will compare the TSG report to roll correction data.	Robert Worthington	10/1/2012	10/1/2012	**Completed**	Yes						
3	Systematic Interface (Roll Corrections-(Supplemental)) TSG created a nightly import log that specifically identifies all value and/or use code changes.	TSG	10/1/2012	10/1/2012	**Completed**	Yes						
4	RPTA will compare the TSG report to roll correction data.	Robert Worthington	5/15/2013	6/7/2013	[redacted]							
5	RPTA will examine the report for accuracy if the parcel count is 50 or below, all items will be reviewed, otherwise a 10% sampling will be applied.	Robert Worthington	5/15/2013	6/7/2013	[redacted]							
6	Manual Interface (All Others) TSG created a nightly import log that specifically identifies all value and/or use code changes.	TSG	10/1/2012	10/1/2012	**Completed**	Yes						

OFFICE OF TAX AND REVENUE
ACTION PLAN STATUS REPORT
AS OF: MAY 24, 2013

7	RPTA will compare the TSG report to System file.	Bill Nelson	5/15/2013	6/7/2013	Yes							
8	RPTA will examine the report for accuracy if the parcel count is 50 or below, all items will be reviewed, otherwise a 10% sampling will be applied. RPTA will also verify total parcel count.	Robert Worthington	5/15/2013	6/7/2013	Yes							
9	RPTA will establish policies and procedures to check the completeness and accuracy of the information uploaded into ITS from FoxPro for both Systematic and Manual Interface.	Stephen Cappello	5/15/2013	6/28/2013	Yes							
Agency:												
OFOS:												
OIO:												

DEFICIENCY # d	During our internal control test work over real property assessment appeals, 2 adjustments out of 40 adjustments tested were not approved by the Chief Assessor as required by the Appeals Divisions policies and procedures.

RECOMMENDATION:	We recommend that OTR strengthen its policies, procedures and controls to ensure that the above noted deficiencies are addressed.

		AGENCY				OFOS				OIO		
			Dates			Review?		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement**	**Not Implemented**
2	RPTA will closely monitor compliance of the automated tiered sign-off.	Stephen Cappello	10/1/2012	12/31/2012	**Completed**	Yes						
3	IT Specialist will create a report to verify appropriate signature(s).	Robert Farr	10/1/2012	12/31/2012	**Completed**	Yes						
9	RPTA will establish policies and procedures to validate appropriate sign-off approvals.	Stephen Cappello	5/15/2013	5/30/2013	Yes							

COMMENTS:	
Agency:	
OFOS:	
OIO:	

DEFICIENCY # e	Monthly reconciliations between certain tax revenue subsidiary records and the general ledger contained un-reconciled differences that were not identified during the supervisory review of the reconciliation. Of 15 reconciliations tested, we noted 2 reconciliations with combined unreconciled differences of $10,865. In addition, we noted that for 1 of the reconciliations, the supervisory review was not performed timely.

RECOMMENDATION:	We recommend that OTR strengthen its policies, procedures and controls to ensure that the above noted deficiencies are addressed.

		AGENCY				OFOS				OIO		
			Dates			Review?		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement**	**Not Implemented**

OFFICE OF TAX AND REVENUE
ACTION PLAN STATUS REPORT
AS OF: MAY 24, 2013

1	Create monthly reconciliation tracking Log for all reconciliations to monitor completion status and verify supervisory review and approvals on a monthly and quarterly basis.	Eric Bime	3/28/2013	4/15/2013	**Completed**	Yes						
2	Revenue accounting manager to monitor all tracking logs to ascertain timely reconciliation of accounts on a monthly basis and verify that outstanding items are resolved in a " timely" manner.	Eric Bime	4/30/2013	5/20/2013	[redacted]							

COMMENTS:
Agency:
OFOS:
OIO:

I certify that the information presented above accurately reflects the status of the Yellow Book corrective actions as of the indicated date. I further certify that the Office of Financial Operations and Systems will be timely notified of any

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff)

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

FINANCIAL REPORTING FOR CAPITAL ASSETS

Capital Assets
OFFICE OF FINANCIAL OPERATIONS AND SYSTEMS
ACTION PLAN STATUS REPORT
As of: MAY 24, 2013

	Name	Phone Number	Email Address
OFOS Liaison:	Cassandra Alexander	(202) 442-8314	cassandra.alexander@dc.gov
OIO Liaison:	Khaled Abdel-ghany;	(202) 442-8277	Khaled.Abdelghany@dc.gov
	Bernie Baranosky	(202) 442-6561	Bernie.Baranovsky@dc.gov
Agency Liaisons:	David Pivec	(202) 478-1424	david.pivec@dc.gov
Financial Liaison:			
Program Liaison:			
Responsible ACFO:	Not Applicable		

On Track?
Completed
At Risk

# Completed (Per Agency)	# Ready for Review (Per OFOS)	# Verified as Completed (Per OIO)

DEFICIENCY 1:	Lack of uniform, District-wide policies and procedures for the identification of completed capital projects to ensure that projects are transferred from CIP to capital assets in the period in which the assets are placed in operation consistently across District agencies

RECOMMENDATION #1:	Develop District-wide policies and procedures for identifying completed capital projects to ensure that projects are transferred from CIP to capital assets in the period in which the assets are placed into operation.

		AGENCY				OFOS				OIO		
			Dates			Review?		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement**	**Not Implemented**
1	Establish CIP team (agencies, OBP, DGS, GSC, OFOS, OCTO) to strategize and develop draft Capital Projects/CIP Accounting Policies and Procedures	Dave Pivec	04/09/13	04/10/13	Completed							
2	Demonstrate (to the CIP Committee) CIP database currently used by DGS to assess the need for making such database accessible to all agencies and including its used in the District's official policies and procedures	Valerie Brown (DGS)	04/23/13	04/29/13	Completed							
3	Prepare draft District-wide Capital Projects/CIP Accounting Policies and Procedures that include specific guidance on transferring completed projects from CIP to capital assets	Dave Pivec/Wilma Matthias	04/16/13	04/22/13	Completed							
4	Discuss draft policies and procedures with other interested parties or stakeholders (OFOS, other agencies) for feedback before finalization; consider discussing with KPMG	Dave Pivec/Wilma Matthias	04/29/13	05/29/13								
5	Finalize draft policies and procedures and issue to all agencies	Dave Pivec/Wilma Matthias	06/18/13	06/24/13								
6	Conduct training sessions by cluster to explain the required process for accounting for and reporting for closed capital projects	Dave Pivec	6/25/2013	09/30/13								
7												
8												

Capital Assets
OFFICE OF FINANCIAL OPERATIONS AND SYSTEMS
ACTION PLAN STATUS REPORT
As of: MAY 24, 2013

9												
10												

COMMENTS:
Agency:
OFOS:
OIO:

DEFICIENCY 2:	Methods used by agencies to account for CIP vary widely throughout the District , which results in a highly decentralized and inconsistently applied capital assets financial reporting process

RECOMMENDATION #1:	Develop District-wide policies and procedures for identifying completed capital projects to ensure that projects are transferred from CIP to capital assets in the period in which the assets are placed into operation.

RECOMMENDATION #2:	Reconcile agency fixed asset activity to the general ledger on a periodic basis rather than only at year-end

RECOMMENDATION #3:	

		AGENCY				OFOS				OIO		
			Dates			Review?		OIO Notified?				
Action Plan Steps:	Description	Lead	Start	Completion	On Track?	Yes	No	Yes	No	Fully Implemented	Partially Implement	Not Implemented
1	Establish CIP team (agencies, OBP, DGS, GSC, OFOS, OCTO) to strategize and develop draft Capital Projects/CIP Accounting Policies and Procedures	Dave Pivec	04/09/13	04/10/13	Completed							
2	Demonstrate (to the CIP Committee) CIP database currently used by DGS to assess the need for making such database accessible to all agencies and including its used in the District's official policies and procedures	Valerie Brown (DGS)	04/23/13	04/29/13	Completed							
3	Prepare draft District-wide Capital Projects/CIP Accounting Policies and Procedures that include specific guidance on transferring completed projects from CIP to capital assets	Dave Pivec/Wilma Matthias	04/16/13	04/22/13	Completed							
4	Discuss draft policies and procedures with other interested parties or stakeholders (OFOS, other agencies) for feedback before finalization	Dave Pivec/Wilma Matthias	04/29/13	05/29/13								
5	Finalize draft policies and procedures and issue to all agencies	Dave Pivec/Wilma Matthias	06/18/13	06/24/13								
6	Conduct training sessions by cluster to explain the required process for accounting for and reporting for closed capital projects	Dave Pivec	6/25/2013	09/30/13								

Capital Assets
OFFICE OF FINANCIAL OPERATIONS AND SYSTEMS
ACTION PLAN STATUS REPORT
As of: MAY 24, 2013

7	Meet at least quarterly with each Cluster of agencies (program and financial staff) to review capital projects, assess completion, and determine whether any portion of CIP is to be transferred to assets and whether there have been any disposals, or significant changes in capital assets	Dave Pivec	6/1/2013	9/30/2013	[redacted]							
8	Hire team of Capital Assets Accountants to centralize certain capital assets accounting and reporting functions (i.e., reconciling FAS to SOAR at least quarterly, closely monitor progress of capital projects and manage CIP transfers; coordinate physical inventory of assets, etc.)	Bill Slack/Diji Omisore	6/1/2013	7/15/2013	[redacted]							

COMMENTS:	
Agency:	
OFOS:	
OIO:	

[redacted]	District does not have a formal procedure in place to monitor CIP balances to ensure the timely transfer of costs to capital assets upon project completion

RECOMMENDATION #1:	Develop District-wide policies and procedures for identifying completed capital projects to ensure that projects are transferred from CIP to capital assets in the period in which the assets are placed into operation.

RECOMMENDATION #2:	Implement a centralized project accounting system that is fully integrated with the general ledger that allows capital asset transactions to be tracked at an invoice and project level.

		AGENCY			OFOS				OIO		
			Dates			Review?		OIO Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement**	**Not Implemented**
1	Demonstrate (to the CIP Committee) CIP database currently used by DGS to assess the need for making such database accessible to all agencies and including its used in the District's official policies and procedures	Valerie Brown, DGS	04/23/13	04/29/13	Completed							
2	Prepare draft District-wide Capital Projects/CIP Accounting Policies and Procedures that include specific guidance on identifying completed capital projects to ensure that such projects are transferred from CIP to capital assets in the period in which the assets are placed into operation.	Dave Pivec/Wilma Matthias	04/16/13	04/22/13	Completed							

Capital Assets
OFFICE OF FINANCIAL OPERATIONS AND SYSTEMS
ACTION PLAN STATUS REPORT
As of: MAY 24, 2013

3	Discuss draft policies and procedures with other interested parties or stakeholders (OFOS, other agencies) for feedback before finalization	Dave Pivec/Wilma Matthias	04/29/13	05/29/13								
4	Finalize draft policies and procedures and issue to all agencies	Dave Pivec/Wilma Matthias	06/18/13	06/24/13								
5	Conduct training sessions by cluster to explain the required process for accounting for and reporting closed capital projects	Dave Pivec/Wilma Matthias	6/25/2013	09/30/13								
6	Meet at least quarterly with each Cluster of agencies (program and financial staff) to review capital projects, assess completion, and determine whether any portion of CIP is to be transferred to assets and whether there have been any disposals, or significant changes in capital assets	Dave Pivec	6/1/2013	9/30/2013								
7	Hire team of Capital Assets Accountants to centralize certain capital assets accounting and reporting functions (i.e., reconciling FAS to SOAR at least quarterly, closely monitor progress of capital projects and manage CIP transfers; coordinate physical inventory of assets, etc.)	Bill Slack/Diji Omisore	6/1/2013	7/15/2013								
8	Engage the EOM (DMPED, OCA) to open the channels of communication to develop a process whereby the OCFO is formally notified when projects (economic development "deals") are initiated	Bill Slack/Dave Pivec	7/15/2013	7/31/2013								
9	Formulate a Capital Projects Oversight Committee comprised of reps from the DMPED, OBP, DGS, OFOS, OCTO, OAG, OCFO-OGC etc. to discuss planned projects, new projects, completed projects, etc.; committee to be convened at least monthly	Dave Pivec	7/15/2013	9/30/2013								

COMMENTS:	
Agency:	
OFOS:	
OIO:	

DEFICIENCY 4:	Detail of current capital expenditures and costs associated with completed projects transferred to capital assets by project is not available at OFOS, although agencies transfer CIP based on the completion of a project
RECOMMENDATION #1:	Implement a centralized project accounting system that is fully integrated with the general ledger that allows capital asset transactions to be tracked at an invoice and project level.
RECOMMENDATION #2:	Develop District-wide policies and procedures for identifying capital project expenditures that are non-capital in nature and ensure such expenditures are expensed in the period incurred

Capital Assets
OFFICE OF FINANCIAL OPERATIONS AND SYSTEMS
ACTION PLAN STATUS REPORT
As of: MAY 24, 2013

RECOMMENDATION #3:	Provide training to District agencies regarding policies and procedures for determining proper classification of capital expenditures and timely transfer of completed projects to fixed assets to reinforce that such procedures are uniformly applied across the District

		AGENCY				OFOS				OIO		
			Dates			Review?		OIG Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement**	**Not Implemented**
1	Make CIP database available to agencies to be used by them to capture and track all costs/activities associated with capital projects	Dave Pivec	7/15/2013	8/15/2013								
2	Hire team of Capital Assets Accountants to centralize certain capital assets accounting and reporting functions (i.e., reconciling FAS to SOAR at least quarterly, closely monitor progress of capital projects and manage CIP transfers; coordinate physical inventory of assets, retain detailed information on expenditures and costs associated with completed capital projects, etc.)	Bill Slack/Diji Omisore	6/1/2013	7/15/2013	[redacted]							

COMMENTS:
Agency:
OFOS:
OIO:

DEFICIENCY 5:	Internal controls in place over the review of agency-submitted closing packages (at OFOS) are not operating effectively to ensure timely and accurate reporting of District capital assets additions (For 4 of 8 closing packages, review checklist was not signed by the OFOS reviewer; for 2 of 7 closing packages, the closing package was prepared and reviewed by the same individual in OFOS)

RECOMMENDATION #1:	Adhere 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 and that the reported capital asset data is complete and accurate.

		AGENCY				OFOS				OIO		
			Dates			Review?		OIG Notified?				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement**	**Not Implemented**
1	Implement quality control measures that require secondary review of closing packages by "back-up" FCRD reviewers or the reviewer's immediate supervisor (secondary review would be to ensure proper sign-offs on packages/review checklists, completion of required checklists, etc.)	Diji Omisore	10/1/2013	1/31/2014	[redacted]							

Capital Assets
OFFICE OF FINANCIAL OPERATIONS AND SYSTEMS
ACTION PLAN STATUS REPORT
As of: MAY 24, 2013

2	implement process that requires segregation of duties with respect to closing package preparation (in the event that OFOS FCRD personnel completes a closing package (Master Lease) the individual will sign package as preparer and his/her immediate supervisor will sign as the reviewer/approver	Diji Omisore	10/1/2013	1/31/2014								

COMMENTS:	
Agency:	
OFOS:	
OIO:	

DEFICIENCY 5:	Supporting documentation for 2 of the 42 capital expenditure transactions tested was not provided to the auditors for review

RECOMMENDATION #1:	*(No specific recommendation made by KPMG; may be inferred that policies and procedures should include controls requiring the retention of adequate supporting documentation)*

		AGENCY				**OFOS**				**OIO**		
			Dates			**Review?**		**OIO Notified?**				
Action Plan Steps:	**Description**	**Lead**	**Start**	**Completion**	**On Track?**	**Yes**	**No**	**Yes**	**No**	**Fully Implemented**	**Partially Implement**	**Not Implemented**
1	Issue memorandum to agencies stressing the importance of retaining documentation for expenditure transactions in a manner that allows quick retrieval of information, when needed	Dave Pivec	7/1/2013	7/31/2013								
2	Include specific guidance in capital assets policies and procedures that discusses the types of supporting documentation to be retained for capital expenditures, how it is to be retained, and how long it is to be retained	Dave Pivec/Wilma Matthias	4/23/2013	6/24/2013								

COMMENTS:	
Agency:	
OFOS:	
OIO:	

that will impede progress or prevent completion of any planned corrective action steps.

(Responsible Agency Representative (Agency Director, Program Manager, Fiscal Staff))

OFOS has reviewed the above corrective action plan and has determined that the planned measures are reasonable and appear to fully respond to the deficiencies noted by the independent auditors.

(OFOS Liaison/FCRD Director/Deputy Controller)

ATTACHMENT C
YELLOW BOOK OVERSIGHT COMMITTEE MEMBERS
(FY 2012 Comprehensive Annual Financial Report)

YELLOW BOOK OVERSIGHT COMMITTEE
AUDIT OF THE FY 2012 COMPREHENSIVE ANNUAL FINANCIAL REPORT

Name	Agency/Office
Anthony Pompa	Office of Financial Operations and Systems
Bill Slack	Office of Financial Operations and Systems
Cassandra Alexander	Office of Financial Operations and Systems
Jesse Dolojan	Office of Financial Operations and Systems
Martha Hopkins	Office of Financial Operations and Systems
Tonja Lowe	Office of Financial Operations and Systems
Michelle McNaughton	Office of Financial Operations and Systems
Wilma Matthias	Office of Financial Operations and Systems
Diji Omisore	Office of Financial Operations and Systems
Deena Parker	Office of Financial Operations and Systems
Norma Payton	Office of Financial Operations and Systems
David Pivec	Office of Financial Operations and Systems
Tong Yu	Office of Financial Operations and Systems
Mohamad Yusuff	Office of Integrity and Oversight
Khaled Abdel-ghany	Office of Integrity and Oversight
Bernard Baranosky	Office of Integrity and Oversight
John Cashmon	Office of Integrity and Oversight
Tisha Edwards	Office of Integrity and Oversight
Elizabeth Jowi	Office of Integrity and Oversight
Esther Sawyer	Office of Integrity and Oversight
Hassan Shode	Office of Integrity and Oversight
Tony The	Office of Integrity and Oversight
Prince Washaya	Office of Integrity and Oversight
Yinka Alao	Office of Contracting and Procurement
Jeffrey Barnette	Office of Finance and Treasury
Jennifer Budoff	Council of the District of Columbia
Albert Casciero	University of the District of Columbia
Lillian Copelin	Office of the Chief Information Officer
Michelle Dee	Council of the District of Columbia
Eric Bime	Office of Tax and Revenue
Tehsin Faruk	Office of the Chief Technology Officer
Joseph Giddis	OCFO Office of Contracts
Warren Graves	Office of the City Administrator
Shirley Kwan-Hui	Office of the Chief Technology Officer
J.W. Lanum	Department of General Services
Thomas Luparello	Department of Employment Services
Munetsi Musara	DC Public Schools
Denise Nedab	Department of Human Services
Phil Peng	Office of the Chief Technology Officer
Beth Spooner	Office of Tax and Revenue

YELLOW BOOK OVERSIGHT COMMITTEE
AUDIT OF THE FY 2012 COMPREHENSIVE ANNUAL FINANCIAL REPORT

Name	Agency/Office
Loretta Walker	Public Safety and Justice Cluster
Ron Walker	Not-for-Profit Hospital Corporation
Sam Yeung	Office of the City Administrator
Johnnie Simmons York	Office of the Chief Information Officer
Abdi Yusuf	Office of the Chief Technology Officer
Mohamed Mohamed	Government Operations Cluster
Delicia Moore	Human Support Services Cluster
Angelique Hayes	Public Safety and Justice Cluster
Deloras Shepherd	Education Cluster

ATTACHMENT D
REMEDIATION FLASH REPORT
(Dated May 3, 2013)

Office of the Chief Financial Officer

Yellow Book Remediation Flash Report

Office of Financial Operations and Systems
Yellow Book Remediation Oversight Committee

May 3, 2013
Report No. 01

PURPOSE

The purpose of this report is to update the Executive Office of the Mayor, the Council, and OCFO management regarding the progress being made toward resolving the FY 2012 Yellow Book findings reported by the District's independent auditors, KPMG, LLP. This **Flash Report** presents "snapshots" of the current status of the District's remediation efforts, with a goal of providing information that is concise and understandable.

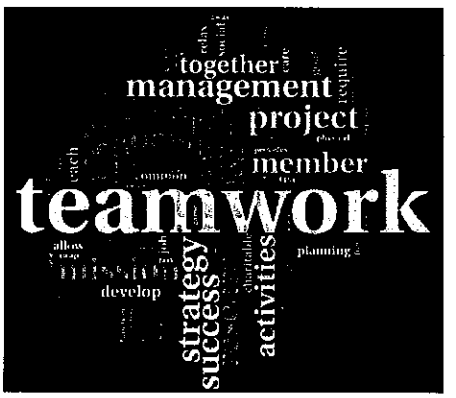
INTRODUCTION

Each year, after completing the audit of the District's Comprehensive Annual Financial Report (CAFR), the independent auditors issue an opinion on the District's financial statements. In addition to the opinion, the independent auditors also issue two other important reports: a report, required for audits conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States (commonly referred to as the Yellow Book Report); and a Management Letter. The Yellow Book Report, which presents the auditor's findings with respect to internal controls and compliance with applicable laws and regulations, is so termed because the *Government Auditing Standards* are published in a book that has a yellow cover.

Audit findings presented in the Yellow Book report are categorized as either material weaknesses (the most severe) or significant deficiencies. Material weaknesses in internal controls threaten the government's ability to produce timely and reliable financial data and thus, depending upon the number and nature of the material weaknesses, may adversely affect the type of audit opinion received. Although significant deficiencies are not as severe as material weaknesses, they should be addressed and resolved without delay to prevent them from escalating and becoming material weaknesses.

As in the prior fiscal year, for FY 2012, the Yellow Book report issued by KPMG contained no material weaknesses. However, the report presented significant deficiencies in four areas: *General Information Technology Controls*, *Procurement and Disbursement Controls*, *Tax Revenue Accounting and Reporting*, and *Financial Reporting for Capital Assets*.

The independent auditors also issued a management letter to communicate other conditions that present opportunities for the District to improve operational efficiency and strengthen internal controls. Such comments are not severe in nature but should also be corrected to minimize the risk of them becoming Yellow Book findings. The Yellow Book Remediation Oversight Committee, comprised of OFOS liaisons, agency subject matter experts, and OIO auditors, decided to address the FY 2012 management letter comments related to Cash and Investments as part of the Yellow Book Remediation Process. This approach has been adopted because Cash and Investments is a high-risk area and if not swiftly addressed, the reported control deficiencies in this area may become Yellow Book deficiencies.



PROGRESS/CURRENT STATUS

The FY 2012 Yellow Book remediation process officially began with a Kick-Off session on March 27, 2013. Representatives from the affected agencies, the Office of Integrity and Oversight (OIO), the Office of Financial Operations and Systems (OFOS) as well as the Office of the City Administrator and the Council were in attendance. The purpose of the Kick-Off session was to explain the required process and to address questions pertaining to the remediation process.

Since the March 2013 Kick-Off, notable progress has been made toward developing and implementing the necessary corrective actions. Agencies have developed corrective action plans and have begun implementing planned action steps. To assist OFOS in tracking progress, agencies submit weekly status reports to OFOS and communicate regularly with their designated OFOS liaisons.

Of the 161 action steps identified to resolve the 73 specific deficiencies reported by KPMG, 58, or 36% were implemented ***as of April 29, 2013***. The vast majority of the remaining planned action steps appear to be on track for timely implementation, consistent with the agencies' established targeted completion dates.

The numbers of planned and completed action steps for each finding are presented in the following table.

Table 1 – Progress of Remediation Efforts
As of April 29, 2013

Finding No.	Area of Deficiency	Number of Specific Conditions	Number of Action Steps	Findings Resolved	Action Steps Completed	Percentage of Action Steps Completed
2012-01	General Information Technology Controls	13	110	0	43	39.1%
2012-02	Procurement and Disbursement Controls	51	22	0	5	22.7%
2012-03	Tax Revenue Accounting and Reporting	5	23	0	7	30.4%
2012-04	Financial Reporting for Capital Assets	4	6	0	3	50.0%
	TOTALS	**73**	**161**	**0**	**58**	**36.0%**

The deficiencies reported in the areas of *General Information Technology Controls* and *Procurement and Disbursement Controls* represent approximately 88% of the total number of specific conditions/deficiencies reported by the independent auditors for FY 2012. **Chart 1** presents a graphic depiction of the percentage breakdown of deficiencies reported in each area of finding, as shown in **Table 1** above.

Chart 1
Percentage of Total Reported Conditions in Each Area of Deficiency

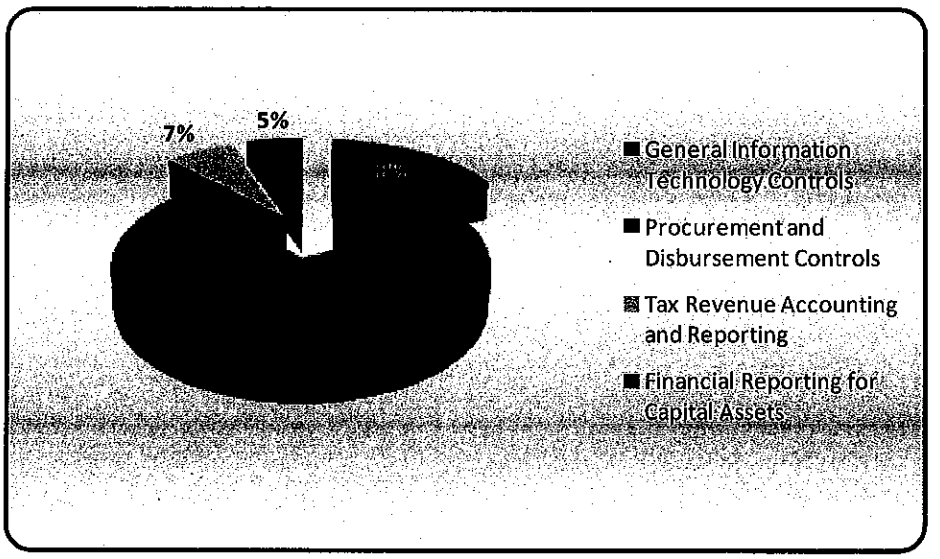
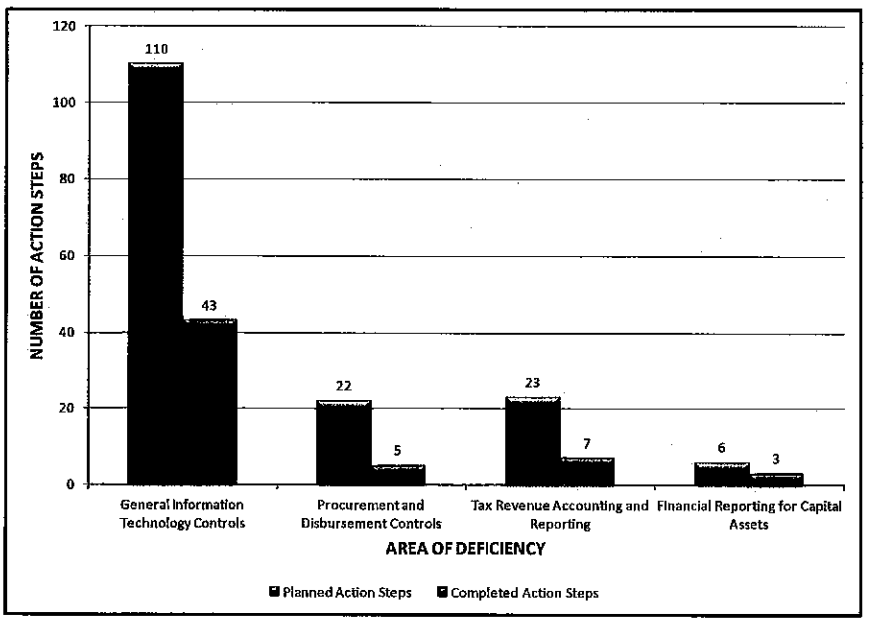


Chart 2 presents a comparative "snapshot" of the number of action steps (planned and completed) for each area of finding.

Chart 2
Comparative Snapshot: Planned vs. Completed Corrective Actions as of April 29, 2013



PROBLEMS/RED ALERT ISSUES TO-DATE

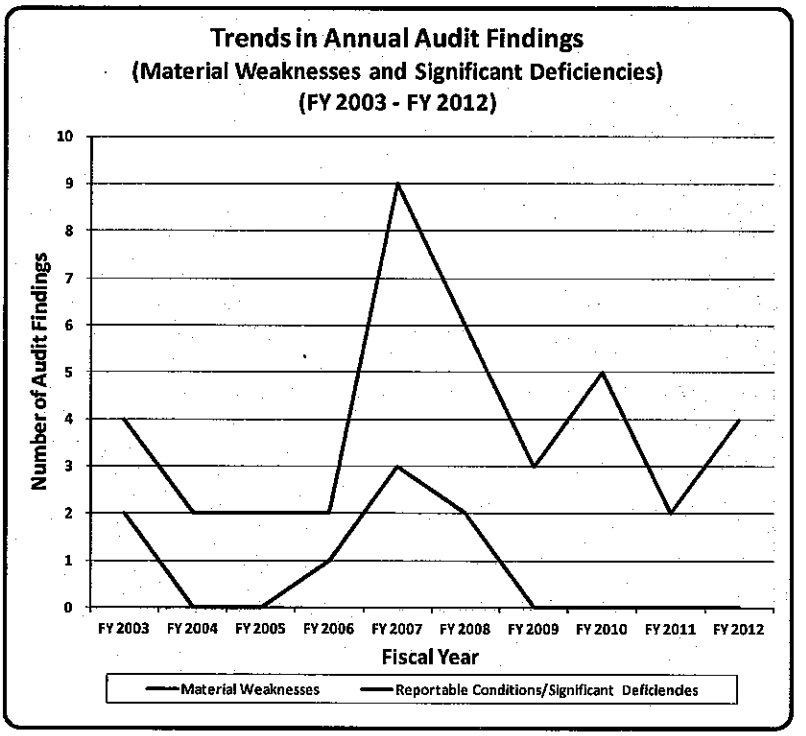
As the remediation process progresses, the Office of the City Administrator, the Council, and OCFO management will be timely informed of any circumstances that arise which may negatively impact the District's ability to resolve reported Yellow Book deficiencies and high-risk management letter comments.

GOING FORWARD

OFOS will continue to monitor the progress being made toward resolving FY 2012 audit findings and will ensure that OIO is timely informed as action steps are completed. OFOS will coordinate with its partners in OIO to track the number of completed action steps which have been verified by OIO. As the remediation process progresses, future **Flash Reports** will present information on the progress of OIO's verification process.

CONTACT INFORMATION

Questions or requests for further information regarding remediation efforts should be directed to: Bill Slack, Deputy Controller or Diji Omisore, Director for Financial Control and Reporting, Office of Financial Operations and Systems, 1100 4th Street, S.W., 8th Floor, Washington, D. C. 20024. Telephone: (202) 442-8200.



Yellow Book Remediation Flash Report

Office of Financial Operations and Systems **May 3, 2013**
Yellow Book Remediation Oversight Committee **Report No. 01**

STATISTICS
Last Five Fiscal Years

Fiscal Year Ending September 30	Area of Finding/Deficiency	Material Weaknesses	Significant Deficiencies
2008	Treasury Functions	X	
	Management of the Medicaid Program	X	
	Compensation		X
	Office of Tax and Revenue		X
	D.C. Public Schools		X
	Management of the Postretirement Health and Life Insurance Trust		X
	Note: OFOS created the Yellow Book Remediation Oversight Committee		
	FY 2008 Totals	**2**	**4**
2009	D.C. Public Schools		X
	Management of the Medicaid Program		X
	Office of Tax and Revenue		X
	FY 2009 Totals	**0**	**3**
2010	General Information Technology Controls		X
	Procurement and Disbursement Controls		X
	Monitoring Stand-Alone Reports		X
	Financial Reporting Process at the Office of Tax and Revenue		X
	Personnel Management and Employee Compensation Process		X
	Note: Change in independent auditors under new 5-year contract. Change in audit approach added two noncompliance findings as Yellow Book significant deficiencies.		
	FY 2010 Totals	**0**	**5**
2011	General Information Technology Controls		X
	Procurement and Disbursement Controls		X
	FY 2011 Totals	**0**	**2**
2012	General Information Technology Controls		X
	Procurement and Disbursement Controls		X
	Tax Revenue Accounting and Reporting		X
	Financial Reporting for Capital Assets		X
	FY 2012 Totals		**4**

ATTACHMENT E
RED ALERT REPORT

FY 2008 Yellow Book Deficiencies
Remediation Process

"Red Alert" Report

Containing Front Burner Issues or "At-Risk" Items
Reported at the September 1, 2009 Joint OFOS/OIO Meeting

All Areas of Deficiency	***Liaison(s): All Designated OFOS, OIO and Agency Liaisons***
	Issue: Attendance at the joint OFOS-OIO sessions is mandatory until such time that the sessions are discontinued. Each OFOS liaison, OIO liaison, and Agency liaison must be present at all joint meetings to discuss the current status of remediation efforts. In the event that a liaison has a scheduling conflict, the liaison should arrange for a knowledgeable representative to be in attendance. Representatives from the following entities/agencies were not in attendance at the September 1st meeting: • Human Support Services Cluster (DOH, DMH, CFSA, DHCF); • Office of Finance and Treasury; and • Office of Tax and Revenue. **Effect:** As a result, all perspectives regarding the status of remediation efforts and potential issues/concerns could not be fully discussed at the September 1st meeting . **Action Needed:** Management should strongly remind all involved parties of the importance of the remediation process. The team cannot lose momentum as the year-end approaches.

FY 2008 Yellow Book Deficiencies
Remediation Process

"Red Alert" Report

Containing Front Burner Issues or "At-Risk" Items
Reported at the September 1, 2009 Joint OFOS/OIO Meeting

Cash and Investments	***Liaison(s): Martha Hopkins (OFOS); Elizabeth Jowi (OIO); Jeffrey Barnette (OFT)***
Unresolved (Issue Has Been On-Going)	**Issue:** OFT's change in planned actions to remediate deficiencies related to the opening and closing of bank accounts has resulted in a revised timeframe for completing remediation activities. OFT had planned to issue a memo to agencies and work with agencies to resolve this issue. However OFT has begun a review of documents at the banks to determine how accounts were opened. The anticipated date of completion for this review was August 15, 2009. Remediation of the corresponding deficiencies by year-end (September 30, 2009) is considered to be "at risk." **Effect:** As a result, the remediation of 1 material weakness (Maintenance of the Accounts Database) by September 30, 2009 is considered to be at risk. (This also may delay the remediation of two management letter comments (Opening Bank Accounts and Closing Bank Accounts). **Action Needed: This is a "Need to Know" item only.** No action is needed by management at this time other than to encourage OFT to complete the review of bank account documentation by the stated deadline of August 15, 2009.

OTR	***Liaison(s): Tong Yu (OFOS); Tisha Edwards (OIO); Beth Spooner (OTR); Edward Anthony (OTR)***
Unresolved (Issue Has Been On-Going)	**Issue:** OTR has not allowed the OIO liaison to test within the Homestead unit due to a backlog of transactions (refunds) which had to be processed. Staff resources have been dedicated to preparing for the upcoming tax sale. **Effect:** As a result, the remediation of at least 3 significant deficiencies by September 30, 2009 is at risk. **Action Needed: This is a "Need to Know" item only.** There are currently at least two critically important competing priorities at OTR—the Tax Sale (important to revenue generation) and YB Remediation (important to a clean audit opinion).

FY 2008 Yellow Book Deficiencies
Remediation Process

"Red Alert" Report

Containing Front Burner Issues or "At-Risk" Items
Reported at the September 1, 2009 Joint OFOS/OIO Meeting

OPEB	***Liaison(s): Andy Urcia (OFOS); Elizabeth Jowi (OIO; Jeffrey Barnette (OFT)***
Unresolved (Issue Has Been On-Going)	**Issue:** BDO Seidman found that "the Postemployment Health and Life Insurance Trust (the Plan) needs to improve its recordkeeping over retirees and active personnel." To address this deficiency, DCHR is working with OCTO to determine whether OPEB participants may be included in PeopleSoft. It has been reported that this planned action may not be possible and if possible, it may not be implemented before year-end. **Effect:** As a result, the remediation of 1 significant deficiency by September 30, 2009 is at risk. **Action Needed:** Management needs to notify the Director of DCHR, stressing the importance of implementing all planned actions by September 30, and encourage a prompt determination as to whether the action described above is doable. In the event that it is found not to be doable, DCHR should be strongly encouraged to develop and implement other measures that address the reported recordkeeping issues.