U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

December 21, 2010

To

Public Printer

From

Inspector General

Subject

Report on the Consolidated Financial Statement Audit of the Government Printing Office for Fiscal Years Ended September 30, 2010 and 2009
Report Number 11-04

This report contains the audit of the annual consolidated financial statements of the Government Printing Office (GPO) as of the fiscal years (FY) ended September 30, 2010 and 2009. We contracted with the independent public accounting firm of KPMG LLP (KPMG) to audit the consolidated balance sheet, statement of revenue and expenses, and statement of cash flows for the years then ended. The audits were conducted in accordance with auditing standards generally accepted in the United States, and the standards applicable to financial audits contained in *Government Auditing Standards* (GAS) issued by the Comptroller General of the United States.

Results of Independent Audit

KPMG expressed an unqualified opinion on the GPO consolidated financial statements as of the FYs ended September 30, 2010, and 2009, by concluding that the GPO financial statements were fairly presented, in all material respects, in conformity with generally accepted accounting principles (GAAP). KPMG's consideration of internal control over financial reporting resulted in three significant deficiencies,[1] which KPMG did not

---

[1] A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

consider to be material weaknesses. Details on these three deficiencies, which were in the areas of controls over special journal entries, controls over human resource data, and information technology are as follows:

1. Controls over Preparation, Review and Approval of Special Journal Entries

KPMG identified that internal controls over the preparation, review and approval of special journal entries need to be strengthened. Specifically, it was noted that 27 of 85 (32%) special journal entries tested had been recorded in the wrong general ledger account and/or recorded in the wrong amount. Of the 27 erroneous entries, 23 were subsequently detected and corrected by GPO. Of the four entries not detected by GPO's internal controls, two were subsequently corrected by management to adjust for net overstatements of assets and operating income of approximately $250 thousand. The remaining two were not corrected as the errors were considered to be immaterial to the financial statements.

2. Controls over Processing and Maintenance of Human Resource Data

During 2010, KPMG noted the following areas where GPO needs to improve its internal controls over processing and maintenance of human resource data in the areas of goal sharing, annual leave balances and discrepancies on personnel actions. The details of these deficiencies are as follows:

- **Controls over GPO Goal Sharing Payments.** The lack of adequate controls over the calculation and distribution of goal sharing incentive resulted in goal sharing payments to ineligible employees. GPO annual goal sharing incentivizes employees to pay attention to specific areas of GPO operations in order to lower expenses and reduce accidents. During payroll test work, it was noted that the methodology used to determine eligible employees resulted in goal sharing payments to ineligible employees for amounts inconsequential to the financial statements.

- **Discrepancies with Employee Annual Leave Balances.** KPMG noted that for 22 of 86 balances tested, the annual leave balance reflected in WebTA (GPO's web-based time and attendance program which employees use to enter and keep track of their hours worked and leave used) did not agree with the annual leave balance reflected by the National Finance Center (NFC), GPO's payroll/personnel service provider.

- **Discrepancies on Personnel Actions.** During payroll test work, KPMG noted that for six of 86 employee personnel files reviewed, the GPO payment plan reflected on the Standard Form 50, *Notification of Personnel Action*, did not agree to the GPO payment plan reflected on the SF-52, *Request for Personnel Action*, maintained in the employees' file. However, it was noted that in each of these instances, the amount of the employee's rate of pay reflected on the SF-50 and SF-52 was in agreement with the amount being processed by NFC for the pay period tested. In addition, 2 of 86 instances were noted where an employee's service date in WebTA did not agree with the employee's service date reflected in NFC's records (Statement of Earnings and Leave) or to the SF-52 in the employee's personnel file.

3. Information Technology General and Application Controls. During fiscal year 2010, deficiencies in the design and/or operations of GPO's information technology (IT) general and application controls were noted in Security Management, Access Controls, Segregation of Duties, Configuration Management and Contingency Planning. Details of these conditions are as follows:

- **Security Management.** GPO made progress in fiscal year 2010 to formalize GPO's established information security objectives and high level policy. However, KPMG noted the following conditions:

    - GPO performs the security authorization process only for major applications and high risk and new systems. GPO's minor applications, such as PROBE, are generally not included in the security authorization process. Although GPO had previously completed the security authorization process for both the GPO Business Information System (GBIS) and the General Support System (GSS), the GSS has operated without a current security authorization since February 2010 when the Interim Authorization to Operate (IATO) for the GSS expired.

    - GPO has not implemented a process to ensure that employees and contractors with significant information security responsibilities (SISR) receive role-based IT security training.

    - The Oracle On-Demand Statement on Auditing Standards No. 70, *Service Organizations* (SAS-70) report provided by Oracle to GPO only partially covered GBIS. Oracle hosts GBIS within the Federal Zone of its Austin, Texas data center. The SAS-70 report for Oracle's Austin Data Center (ADC) only partially applied to GBIS and did not include logical access or configuration management controls applicable to the Federal Zone. The SAS-70 report's applicability to GBIS was limited to such data-center-wide controls as physical access and environmental controls. However, management did not realize that the SAS-70 did not cover the Federal Zone and inadvertently relied on the report.

- **Access Controls.** KPMG noted that overall, access controls at GPO continue to require strengthening in order to provide a more secure financial processing and computing environment. GPO management made progress in addressing the access control deficiencies noted in prior years. However, we noted the following access controls deficiencies that need improvement:

    - GPO does not consistently follow required policies and procedures for granting access and reviewing access to the financial systems or GPO network. Users were granted access to systems without documented approval.

    - User access was not consistently removed after users left GPO or changed job duties.

    - GPO does not have effective policies and procedures to revoke the physical and logical access of contractors after they leave GPO.

    - Periodic reviews of user access were not consistently documented.

    - Access to the GBIS rate maintenance responsibility that controls the ability to modify the All Inclusive Hourly Rate (AIHR) is not properly restricted to only those users responsible for modifying rate information.

    - Audit logs at the application level for GBIS are not reviewed.

    - Of 3,903 network user access accounts, 315 enabled accounts had passwords that were set to never expire.

    - Information Technology and Systems was unable to provide evidence of the quarterly data center access review for one of two quarters selected for testing.

- **Segregation of Duties.** KPMG noted that the lack of adequate controls to prevent the assignment of incompatible functions within GBIS exposes GPO to the risk that certain users may be assigned the ability to perform multiple critical system transactions. As a result, users may be able to initiate and approve an erroneous transaction.

- **Configuration Management.** KPMG noted that implementation of configuration changes for GBIS did not adhere to strict configuration management practices. Specifically, they identified that one of fifteen changes to the GBIS application closed in fiscal year 2010 that was tested did not have the documented approval or evidence of testing for the change. The change where testing and approval was undocumented was an emergency change. Due to the urgency of the change, approval appears to have been communicated informally.

- **Contingency Planning.** KPMG noted that a continuity of operations plan for GPO's general support system has not been finalized and is still in draft form. Furthermore, GPO did not provide evidence of periodic testing of the continuity of operations plan.

KPMG disclosed no instances of noncompliance with certain provisions of laws, regulations and contracts or other matters that are required to be reported under GAS.

Evaluation and Monitoring of Audit Performance

We reviewed the KPMG audit of the GPO consolidated financial statements by:

- Evaluating the independence, objectivity, and qualifications of the auditors and specialists;
- Reviewing the approach of and planning for the audit;
- Attending key meetings with auditors and GPO officials;
- Monitoring the audit progress;
- Examining audit documentation;
- Reviewing the auditors' reports; and
- Reviewing the financial statements and associated footnotes.

KPMG is responsible for the attached reports dated December 20, 2010, and the conclusions expressed in the reports. Our review, as differentiated from an audit in accordance with GAS, was not intended to enable us to express, and accordingly we do not express, an opinion on GPO's financial statements, the effectiveness of internal controls, or compliance with laws and regulations. However, our monitoring review, as limited to the procedures listed above, disclosed no instances in which KPMG did not comply, in all material respects, with GAS.

If you have any questions or comments about this report, please do not hesitate to contact me, or Mr. Kevin Carson, Assistant Inspector General for Audits and Inspections, at (202) 512-2009 or through email at kcarson@gpo.gov.

J. Anthony Ogden
Inspector General

Attachment

cc:
Deputy Public Printer
Acting Chief Management Officer
Acting General Counsel
Chief Financial Officer
Chief Technology Officer