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

Independent Auditors' Report

The Public Printer
United States Government Printing Office:

We have audited the accompanying consolidated balance sheets of the United States Government Printing Office (GPO) as of September 30, 2011 and 2010, and the related consolidated statements of revenues, expenses, and changes in retained earnings and cash flows (hereinafter referred to as "consolidated financial statements") for the years then ended. The objective of our audits was to express an opinion on the fair presentation of these consolidated financial statements. In connection with our fiscal year 2011 audit, we also considered GPO's internal control over financial reporting and tested GPO's compliance with certain provisions of applicable laws, regulations, and contracts that could have a direct and material effect on these consolidated financial statements.

Summary

As stated in our opinion on the consolidated financial statements, we concluded that GPO's consolidated financial statements as of and for the years ended September 30, 2011 and 2010, are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles.

Our consideration of internal control over financial reporting resulted in identifying certain deficiencies that we consider to be significant deficiencies, as defined in the Internal Control over Financial Reporting section of this report, as follows:

A. Controls over Processing and Maintenance of Human Resource and Payroll Information
B. Information Technology General and Application Controls

We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses as defined in the Internal Control over Financial Reporting section of this report.

The results of our tests of compliance with certain provisions of laws, regulations, and contracts disclosed no instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards*, issued by the Comptroller General of the United States.

The following sections discuss our opinion on GPO's consolidated financial statements; our consideration of GPO's internal control over financial reporting; our tests of GPO's compliance with certain provisions of applicable laws, regulations, and contracts; and management's and our responsibilities.

Opinion on the Financial Statements

We have audited the accompanying consolidated balance sheets of the United States Government Printing Office as of September 30, 2011 and 2010 and the related consolidated statements of revenues, expenses, and changes in retained earnings and cash flows for the years then ended.

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the United States Government Printing Office as of September 30, 2011 and 2010, and the results of its operations and its cash flows for the years then ended, in conformity with U.S. generally accepted accounting principles.

Our audits were conducted for the purpose of forming an opinion on the consolidated financial statements taken as a whole. The information in the Management's Discussion and Analysis section is presented for purposes of additional analysis and is not required as part of the consolidated financial statements. This information has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

Internal Control over Financial Reporting

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a 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.

Our consideration of internal control over financial reporting was for the limited purpose described in the Responsibilities section of this report and was not designed to identify all deficiencies in internal control over financial reporting that might be deficiencies, significant deficiencies, or material weaknesses. In our fiscal year 2011 audit, we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above. However, we identified certain deficiencies in internal control over financial reporting described in Exhibit I that we consider to be significant deficiencies in internal control over financial reporting. A significant deficiency is a deficiency, or a 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.

Exhibit II presents the status of prior year significant deficiencies.

We noted certain additional matters that we have reported to management of GPO in a separate letter.

Compliance and Other Matters

The results of our tests of compliance as described in the Responsibilities section of this report disclosed no instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards.*

* * * * * * *

Responsibilities

Management's Responsibilities. Management is responsible for the consolidated financial statements; establishing and maintaining effective internal control; and complying with laws, regulations, and contracts applicable to GPO.

Auditors' Responsibilities. Our responsibility is to express an opinion on the fiscal year 2011 and 2010 consolidated financial statements of GPO based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America; and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the consolidated financial statements are free of material misstatement. An audit includes consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of GPO's internal control over financial reporting. Accordingly, we express no such opinion.

An audit also includes:

- Examining, on a test basis, evidence supporting the amounts and disclosures in the consolidated financial statements;
- Assessing the accounting principles used and significant estimates made by management; and
- Evaluating the overall consolidated financial statement presentation.

We believe that our audits provide a reasonable basis for our opinion.

In planning and performing our fiscal year 2011 audit, we considered GPO's internal control over financial reporting by obtaining an understanding of GPO's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of GPO's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of GPO's internal control over financial reporting.

As part of obtaining reasonable assurance about whether GPO's fiscal year 2011 consolidated financial statements are free of material misstatement, we performed tests of GPO's compliance with certain provisions of laws, regulations, and contracts, noncompliance with which could have a direct and material effect on the determination of the consolidated financial statement amounts. We limited our tests of compliance to the provisions described in the preceding sentence, and we did not test compliance with all laws, regulations, and contracts applicable to GPO. However, providing an opinion on compliance with laws, regulations, and contracts was not an objective of our audit and, accordingly, we do not express such an opinion.

GPO's responses to the findings identified in our audit are presented in Exhibit I. We did not audit GPO's responses and, accordingly, we express no opinion on them.

This report is intended solely for the information and use of GPO's management, GPO's Office of Inspector General, the U.S. Government Accountability Office, and the U.S. Congress and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

December 16, 2011

Exhibit I

Fiscal Year 2011 Significant Deficiencies

A. Controls over Processing and Maintenance of Human Resource and Payroll Information

We noted the following areas where the United States Government Printing Office (GPO) needs to improve its internal controls over processing and maintenance of human resource and payroll information:

a. We noted that 35 of 120 employees tested during the year were nominated and approved for a goal sharing payment. Of the 35, we noted 1 employee never received the goal sharing award of $100 even though the employee was approved and included on the list of approved awardees that was sent to the National Finance Center (NFC), GPO's payroll/personnel service provider, for payments.

b. We noted 24 of 120 balances tested where the annual leave balance recorded in Web Time & Attendance (WebTA) did not agree to the annual leave balance recorded by the NFC, which is reflected on the employee's Statement of Earning and Leave. WebTA is GPO's web-based time and attendance program which employees use to enter and keep track of their hours worked and leave used. GPO management detected and corrected the errors during the year for 21 of the 24 exceptions. However, for the remaining 3 employees tested, 2 had balances that were not detected or corrected by management as of September 30, 2011, resulting in an incorrect leave balance recorded at year end, and 1 employee separated from the agency in July 2010 with the incorrect leave balance.

c. We noted for 2 of 72 personnel files reviewed that the GPO payment plan reflected on the Standard Form (SF)-50, *Notification of Personnel Action,* did not agree to the GPO payment plan reflected on the SF-52, *Request/or Personnel Action,* maintained in the employee's personnel file. However, we noted that in each of these instances the employee's rates of pay reflected on the SF-50 and SF-52 were in agreement with the amount being processed by NFC for the pay period tested.

d. Of the 120 WebTA sheets reviewed, we identified 8 instances where the WebTA sheet was certified by a person not listed on the list of approved supervisors. Additionally, no evidence was made available to verify that the individuals who certified the timesheets had been delegated that authority by an approved supervisor or that the supervisor had reviewed the timesheet in the following period for reasonableness.

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* requires the following:

- Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements or budget development and execution. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.

Fiscal Year 2011 Significant Deficiencies

- Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation. Control activities may be applied in a computerized information system environment or through manual processes.

- Transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from the initiation and authorization through its final classification in summary records. In addition, control activities help to ensure that all transactions are completely and accurately recorded.

The causes of the conditions above were deficiencies in the operating effectiveness of internal controls to ensure all information processed is properly reviewed for accuracy and reasonableness.

Recommendations:

We recommend that GPO strengthen its controls over the processing and maintenance of human resource and payroll information as follows:

1. Perform a review of all information uploaded to NFC to verify that the upload was successful and accurate.

2. Develop and implement Standard Operating Procedures detailing how to correctly enter leave adjustments in the WebTA system and the NFC mainframe.

3. Develop and implement policies and procedures for payroll personnel to reconcile annual leave balances per WebTA to NFC to ensure that leave hours are properly accrued and that the annual leave balance is correct at the end of each pay period.

4. Improve communication with NFC to ensure that: a) the GPO payment plan information reflected on the SF·50's maintained in employee personnel files are accurate; and b) employee pay plans provided to NFC agrees with employee actions and their personnel file.

5. Develop and implement policies and procedures over the maintenance of authorized and approved Web Time & Attendance certifiers. Policies and procedures should be established to prevent inappropriate delegations of certifying authority. In addition, all approved delegates should be properly trained and able to determine the reasonableness of hours and/or expenses which they are certifying.

Management Response:

Management concurs with these recommendations and has already worked to implement a corrective action plan.

Fiscal Year 2011 Significant Deficiencies

B. Information Technology General and Application Controls

During fiscal year 2011, deficiencies in the design and/or operations of GPO's information technology (IT) general and application controls were noted in the areas of Security Management, Access Controls, Segregation of Duties, Configuration Management, and Contingency Planning. These conditions were generally due to resource constraints and competing priorities at GPO. The details of these conditions, several of which have been reported to management in prior years' audit reports, are as follows:

1. Security Management

GPO made progress in fiscal year 2011 to formalize its established information security objectives and high level policy. However, we noted that although GPO had previously completed the security assessment and authorization process for both the GPO Business Information System (GBIS) and the GPO General Support System (GSS), GBIS operated without a current security authorization since May 2010 when the Interim Authorization to Operate (IATO) for GBIS expired. Also, the following exceptions were observed during our test work:

i. For both GSS and GBIS, System Security Plans and Risk Assessment Reports did not include IT security controls that were equivalent to the high impact control baseline from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.

ii. For GBIS and the GSS, security assessment testing did not include a population of IT security controls equivalent to the high impact control baseline from NIST SP 800-53.

Operating an application in production without a current security authorization increases the risk that since the previous security assessment and authorization, the current state of the system, its controls or the environment it operates in will have changed to the point that the system security plan no longer describes the system's current controls or plans necessary controls, and the security assessment no longer considers the full range of significant risks to which the system is subject.

Incomplete system security plans may lead to incomplete security assessment testing that does not include all necessary IT security controls and does not document test procedures and results for all necessary IT security controls. Not performing security assessment testing of all necessary IT security controls, increases the risk that control gaps or weaknesses will not be detected and corrected or be mitigated with compensating controls. This may lead to necessary controls not being included in system security plans. The resulting control gaps may subject data and resources to unauthorized use, loss, or disclosure.

Additionally, not documenting system security plans in detail sufficient to plan IT controls that are identical or equivalent to the applicable NIST SP 800-53 baseline controls may lead to gaps in system security planning, and more specifically, may lead to the GPO not planning and implementing IT security controls that are equivalent or identical to those recommended by NIST SP 800-53.

Fiscal Year 2011 Significant Deficiencies

2. Access Controls

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:

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

   i. Of a sample selection of 15 separated GPO personnel, 3 retained access to GPO's Active Directory network.

b. Periodic reviews of user access were not consistently documented:

   i. The GPO Finance Office lacks documented evidence of a monthly GBIS user access review and recertification. On a monthly basis, IT Security sent user access lists to the Finance Office for review. However, the Finance Office did not retain evidence of its reviews.

   ii. There is no process in place to document a periodic review of GPO GSS users.

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

Access controls should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized access, modification, disclosure, loss, or impairment. Not timely removing accounts for separated users increases the risk that unauthorized users will gain access to information systems.

Not consistently documenting periodic reviews of user access increases the risk that users who no longer require access will retain access.

With no audit log reviews done at the application level for GBIS, events within the application that may represent attempts to gain unauthorized access or otherwise circumvent controls may not be detected and responded to.

3. Segregation of Duties

Effective segregation of duties starts with effective entity-wide policies and procedures that are implemented at the system and application levels. Although Finance Office segregation of duties procedures document conflicting activities within GBIS, the procedures are not sufficiently detailed to identify which roles within GBIS are considered to be conflicting. Not identifying conflicting roles within GBIS may lead to GBIS users having conflicting access to this key financial system, which could result in a user having end-to-end control over a transaction such that they could both initiate and approve an erroneous transaction.

4. Configuration Management

GPO does not centrally manage the security patching of Microsoft Windows desktops and laptops. Desktop and laptop computers without current security patches may not be properly

safeguarded from security vulnerabilities. As a result, vulnerabilities may be exploited and data and resources may be subject to unauthorized use, loss, or disclosure.

GPO Information Technology and Systems (IT&S) management has implemented a process for centrally managing patching for Microsoft Windows servers using Microsoft Windows Server Update Services (WSUS). GPO's first priority was to implement the patch management process for these servers. However, GPO has not yet created standard operating procedures for desktop/laptop patch management and has not yet expanded its centralized Microsoft Windows patch management process to include desktops and laptops.

5. Contingency Planning

The contingency plan for GPO's GSS has not been finalized, approved or tested, and is still in draft form. GPO may not be able to successfully recover critical applications and systems to maintain business functions during the event of a service disruption, without an effective contingency plan and testing process in place. Without documented contingency plan test results, management may be unaware of any weaknesses in disaster recovery capabilities that could have been revealed by disaster recovery testing.
Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* requires organizations to authorize the operation of organizational information systems.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, provides more detailed guidance for the security authorization process and directs organizations to:

- Develop security plans for information systems that describe the security controls in place or planned for meeting the control requirements from SP 800-53 including rationale for control tailoring and supplementation decisions, and

- Assess the planned security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome and to document the results of the assessment to provide to the authorizing official.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, provides guidance for managing access controls and directs organizations to:

- Operate procedures for disabling and removing access when users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;

- Periodically review accounts;

- Implement separation of duties through assigned information system access authorizations; and

- Review and analyze information system audit records for indications of inappropriate or unusual activity and report findings to designated organizational officials.

Fiscal Year 2011 Significant Deficiencies

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, states that organizations should remediate vulnerabilities by maintaining a process to install security patches.

In addition, NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, states that organizations should develop contingency plans for their information systems that are reviewed and approved by designated officials, should test to determine the plans' effectiveness, should review the contingency plan test results, and initiate corrective actions.

Recommendations:

We recommend that GPO continue to strengthen its IT general and application controls in each of the five identified domains, as follows:

1. Security Management

We recommend that GPO management ensure that:

a. GPO documents system security plans and risk assessments in detail sufficient to plan system security controls for general support systems and major applications that are equivalent to the NIST SP 800-53 high-impact baseline controls.

b. Security assessment testing used to support decisions to authorize systems for operation covers all planned system security controls at the point of initial authorization and at least once every three years thereafter, and includes descriptions of the test procedures performed and the results obtained.

c. The GBIS application is re-authorized to operate.

2. Access Controls

We recommend that GPO management ensure that:

a. The sign out process for removing system access from separated personnel is evaluated, revised as necessary, and formally documented to help ensure that system access is removed at the time personnel leave GPO.

b. A periodic review of users with access to the GPO GSS is implemented.

c. Procedures for periodically reviewing and recertifying access to GPO systems, including GBIS, are evaluated, revised as necessary, and formally documented to help ensure that access is reviewed on a periodic basis and that the review is documented.

d. GPO designs and implements a risk-based approach to reviewing application audit log events for GBIS.

Fiscal Year 2011 Significant Deficiencies

3. Segregation of Duties

We recommend that GPO management revise procedures for maintaining segregation of duties within GBIS so that the procedures include sufficient detail to identify conflicting roles within GBIS.

4. Configuration Management

We recommend that GPO management ensure that:

a. IT&S completes the development of centrally managed desktop and laptop patch management procedures to help ensure that security patches are deployed to desktop and laptop computers in a timely manner.

b. IT&S documents standard operating procedures for desktop and laptop patch management.

5. Contingency Planning

We recommend that GPO management:

a. Finalize and approve the contingency plan for GPO's GSS.

b. Periodically perform contingency plan testing, document the test plans and results, and take appropriate corrective action based on the results, if necessary, for GPO's GSS.

Management Response:

Management concurs with these recommendations and is in the process of implementing a corrective action plan.

Exhibit II

Status of Prior Year Findings

Prior Year Condition	Prior Year Recommendation	Status as of September 30, 2011
	Significant Deficiencies	
A. Controls over Preparation, Review, and Approval of Special Journal Entries	We recommended that GPO strengthen its internal control over the preparation, review and approval of special journal entries by : 1. Requiring that GPO personnel responsible for preparing an entry (1) gather the necessary facts and supporting documentation to fully understand the entry that they are preparing; and (2) perform a self-review over the entry prior to submitting it for approval to ensure that the proper accounts, cost codes, function codes, and amounts are used for the journal entries. 2. Developing standard operating procedures documenting the requirements and instructions for supervisors reviewing journal entries including: (1) which supervisors are qualified to review certain types of special journal entries that impact certain areas (i.e., for all entries that impact fixed assets, the Chief of Property and Accounting must approve); (2) what information should be verified before the entry can be approved; and (3) the type of documentation that is considered to be sufficient to support/justify the basis for the entry.	**Closed**
B. Controls over Processing and Maintenance of Human Resource Data	We recommended that GPO strengthen its controls over the processing and maintenance of human resource and payroll information as follows: 1. Improve controls within the Human Capital Office and the Finance Department to ensure that only employees who are eligible to participate in GPO's annual goal sharing program pursuant to GPO Directive 665.22 receive annual goal sharing payments. 2. Improve its internal controls to ensure that GPO payment plan information reflected on the SF-50s maintained in employee personnel files are accurate; and employee service dates reflected in WebTA agree with employee service dates reflected in NFC records and the SF-52 maintained in the employee's personnel file. 3. Develop Standard Operating Procedures detailing how to correctly enter leave adjustments in the WebTA system and the NFC mainframe.	**Significant Deficiency** This finding has been partially repeated in FY 2011; see Exhibit I.

.

Exhibit II

Status of Prior Year Findings

Prior Year Condition	Prior Year Recommendation	Status as of September 30, 2011
	4. Develop a report based on information from NFC that can be run bi-weekly that will identify any change made to an employee's record subsequent to the initial interface with NFC. 5. Implement a control where payroll personnel reconcile the annual leave balances per WebTA to NFC ensuring that the proper numbers of hours are being accrued per pay period and that the annual leave balance is correct.	
C. Information Technology General and Application Controls		
1. Security Management	We recommended that GPO management document its system security plans in detail sufficient to plan system security controls for general support systems and major applications that are identical or equivalent to the applicable NIST SP 800-53 baseline controls. In addition, we recommended the following: a. GPO management document its risk assessments and considers a full range of significant risks to be consistent with risk assessment requirements from NIST SP 800-30. Also, we recommended that when creating a security authorization package, GPO document procedures performed and results obtained for security assessment testing of all planned IT security controls. Additionally, we recommended that GPO update the security authorization package for the GSS and, after planning and successfully testing the necessary IT security controls, re-authorizes it for operation. b. GPO management document and implement procedures to identify all personnel with significant information security responsibilities and ensure that they receive periodic role-based IT security training. c. GPO request that Oracle amend the scope of the SAS-70 report for Oracle On-Demand to include the Federal Zone where the servers for GBIS are hosted.	**Significant Deficiency** This finding has been partially repeated in FY 2011; see Exhibit I.
2. Access Controls	We recommended that GPO management: a. Evaluate, revise as necessary, and formally document procedures for approving access to the GSS and GBIS to help ensure that approvals are documented prior to granting users access.	**Significant Deficiency** This finding has been partially repeated in FY 2011; see

.

Status of Prior Year Findings

	b. Ensure that controls for removing system access from separated contractors, including the periodic contractor network access review and setting contractor network user accounts to expire, are consistently operated for all contractors with access to GPO's network. c. Evaluate, revise as necessary and formally document procedures for periodically reviewing and recertifying access to GPO systems to help ensure that access that users do not need is removed timely. d. Restrict access to applications and systems, including the GBIS rate maintenance responsibility, to personnel based on defined roles and responsibilities. Access should be removed from user access accounts that do not require such access. e. Enhance its policies and procedures over password settings. With the exception of system service accounts, management should ensure that password expiration settings are applied to all users' network accounts. f. Design and implement a risk-based approach to reviewing application audit log events for GBIS. g. Consistently perform and document a periodic review and recertification of the data center physical access list. The review and certification should be performed and documented, at a minimum, on a quarterly basis.	Exhibit I.
3. Segregation of Duties	We recommended that GPO management document the permissions used within GBIS, identify which permissions conflict, and ensure that conflicting permissions are not assigned to the same user.	**Significant Deficiency** This finding has been repeated in FY 2011; see Exhibit I.
4. Configuration Management	We recommended that GPO management : **a.** Take steps to ensure that emergency changes to GBIS are approved and are tested as soon as possible after implementation into production. b. Complete the development of centrally managed desktop and laptop patch management procedures to help ensure that security patches are deployed to desktop and laptop computers in a timely manner. We also recommended that GPO document its standard operating procedures for patch	**Significant Deficiency** This finding has been partially repeated in FY 2011; see Exhibit I.

.

Exhibit II

Status of Prior Year Findings

	management.	
5. Contingency Planning	We recommended that management: a. Finalize and approve the contingency plan for GPO General Support System Number 1. b. Periodically perform contingency plan testing and document the test plans and the results for GPO General Support System Number 1.	**Significant Deficiency** This finding has been repeated in FY 2011; see Exhibit I.

.