



U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

**AUDIT REPORT
14-09**

**U.S. Government Printing Office FY 2013
Independent Auditor's Report**

February 14, 2014

**Date**

February 14, 2014

To

Public Printer

From

Inspector General

SubjectFY 2013 Independent Auditor's Report
Report Number 14-09

Attached is the Independent Auditor's Report on the U.S. Government Printing Office's (GPO's) FY 2013 financial statements. We contracted with the independent certified public accounting firm of KPMG LLP (KPMG) to audit the financial statements of GPO as of and for the years ending September 30, 2013, and 2012. The contract required that the audit be conducted in accordance with generally accepted government auditing standards (GAGAS).

KPMG's opinion on GPO's financial statements was unqualified. KPMG's consideration of internal control over financial reporting resulted in a material weakness. 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 in a timely basis. In addition, KPMG identified one significant deficiency related to Information Technology General and Application Controls. 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. KPMG made recommendations that GPO address each of the deficiencies.

OIG further recommends that management develop a comprehensive corrective action plan (CAP) that addresses the material weakness identified during the audit. Specifically, reconciliations or comparisons of material data should be addressed separately as part of the CAP.

Appendix A, "Internal Control over Financial Reporting," of the Chief Financial Officer's Council's Implementation Guide for OMB Circular No. A-123, "Management's Responsibility for Internal Control," explains that a comprehensive CAP lists the detailed actions that

agency personnel must perform to resolve a material weakness. The Guide also describes the basic elements of a comprehensive CAP as including:

- A summary description of the deficiency.
- The year the deficiency was first identified.
- The targeted corrective action date (the date of management follow-up).
- The agency official responsible for monitoring progress.
- The indicators, statistics, or metrics used to gauge resolution progress (in advance of audit follow-up) to validate the resolution of the deficiency.
- The quantifiable target or otherwise qualitative characteristic (for example, milestone) that reports how resolution activities are progressing.

While GPO is not required to follow OMB Circular No. A-123, the Circular is considered to contain policy related to internal controls that we consider best practices for the Federal Government. CAPs are the mechanism whereby management presents the procedures the agency will follow to resolve deficiencies.

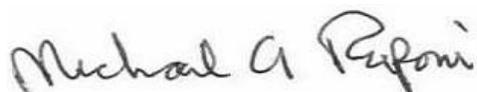
Recommendation

We recommend the Chief Financial Officer prepare a comprehensive CAP that addresses the material weakness identified in the consolidated financial statement audit. Specifically, reconciliations or comparisons of material data should be addressed separately as part of CAP. The CAP should include measurable indicators of compliance and resolution to assess and validate progress throughout the resolution cycle. Management should closely monitor and update the CAP periodically.

KPMG is responsible for the attached auditor's report and the conclusions expressed in the report. However, in connection with the contract, we reviewed KPMG's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with GAGAS, was not intended to enable us to express, and we do not express, an opinion on GPO's financial statements; or conclusions about the effectiveness of

any internal control; or on GPO's compliance with laws and regulations. Our review did not disclose any instances where KPMG did not comply, in all material respects, with GAGAS requirements.

We appreciate the courtesies extended to KPMG and to our audit staff. If you have any questions or comments about this report, please do not hesitate to contact me at (202) 512-0039.



MICHAEL A. RAPONI
Inspector General

Attachment

cc:

Deputy Public Printer
General Counsel
Chief Financial Officer
Chief of Staff



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

Independent Auditors' Report

The Public Printer
United States Government Printing Office

Office of the Inspector General
United States Government Printing Office:

Report on the Financial Statements

We have audited the accompanying consolidated financial statements of the United States Government Printing Office (GPO), which comprise the consolidated balance sheets as of September 30, 2013 and 2012, and the related consolidated statements of revenues, expenses, and changes in retained earnings, and cash flows for the years then ended, and the related notes to the consolidated financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with U.S. generally accepted accounting principles; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these consolidated financial statements 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 audit to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements.

KPMG LLP is a Delaware limited liability partnership,
the U.S. member firm of KPMG International Cooperative
("KPMG International"), a Swiss entity.



We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion on the Financial Statements

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, 2013 and 2012, and the results of its operations and its cash flows for the years then ended in accordance with U.S. generally accepted accounting principles.

Other Matters

Other Information

Our audits were conducted for the purpose of forming an opinion on the basic consolidated financial statements as a whole. The information in the Management's Discussion and Analysis section is presented for purposes of additional analysis and is not a required part of the basic consolidated financial statements. Such information has not been subjected to the auditing procedures applied in the audits of the basic consolidated financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Other Reporting Required by Government Auditing Standards

Internal Control over Financial Reporting

In planning and performing our audit of the consolidated financial statements, we considered the GPO's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances 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 the GPO's internal control. Accordingly, we do not express an opinion on the effectiveness of the GPO's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying Schedule of Findings, we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

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. We consider the deficiencies in controls over financial reporting described in the accompanying Schedule of Findings as item 2013-01 to be a material weakness.

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. We consider the deficiencies in controls over information technology described in the accompanying Schedule of Findings as item 2013-02 to be a significant deficiency.



Compliance and Other Matters

As part of obtaining reasonable assurance about whether GPO's consolidated financial statements are free from 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. However, providing an opinion on compliance with these provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests of compliance as described above disclosed no instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards*.

GPO's Responses to Findings

GPO's responses to the findings identified in our audit are described in the accompanying Schedule of Findings. GPO's responses were not subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the responses.

Purpose of the Other Reporting Required by Government Auditing Standards

The purpose of the communication described in the Other Reporting Required by *Government Auditing Standards* section is solely to describe the scope of our testing of internal control and compliance and the result of that testing, and not to provide an opinion on the effectiveness of GPO's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

February 7, 2014

Fiscal Year 2013 Schedule of Findings

Material Weakness

2013-01 Controls over Financial Reporting

During fiscal year (FY) 2013, we noted several matters that highlighted the need for improved internal controls over financial reporting in several key process areas relating to the preparation, review and posting of journal entries and the review and approval of account reconciliations. We also noted several instances where supervisory reviews were not performed timely or at a precision level that would detect and correct a material misstatement. Collectively, these matters are considered to be a material weakness in internal controls over financial reporting. Specifically, we identified the following:

- The billings to revenue reconciliations for two of three months tested were not properly reviewed by management, which resulted in multiple errors in the reconciliations. For example, amounts in the reconciliations did not agree to the balances recorded in the general ledger; mathematical errors occurred in calculating sum totals; and some of the amounts identified as reconciling items were not true reconciling items. (13-NFR-03)
- We noted that GPO used a report titled "Accounts Receivable and Cash Management Report" to monitor its government-related accounts receivables. However, periodic reconciliations of this report to the general ledger were not performed. As a result of our requests for such reconciliations, we were provided multiple versions of the reconciliations containing material errors. (13-NFR-03) For example:
 - The September 2013 reconciliation reviewed by management listed a reconciling item of approximately \$16.8 million. However, when we tested the reconciliation, we determined it was not a reconciling item but rather an item related to FY 2014 invoices.
 - The second version of the September 2013 reconciliation reviewed by management listed a reconciling item of approximately \$2.5 million. However, when we tested the reconciliation, we determined it was not a reconciling item due to a clerical error. In addition, all reconciling items on the amended version of the September 2013 reconciliation were incorrectly identified as negative numbers when they should have been positive numbers, increasing the balance.
- Our testing of deposit account reconciliations identified mathematical errors and items incorrectly identified as reconciling items, and the monthly journal entry to accrue for unapplied receipts was not posted to the general ledger. (13-NFR-03)
- For the "Annual Allowance for Doubtful Accounts Calculation" as of September 30, 2013, we identified a difference between the FY 2013 "4 Bucket Report" and the general ledger where the general ledger was approximately \$1 million less than the "4 Bucket Report." We also noted that the balance of the accounts over 18 months old from the FY 2012 "4 Bucket Report" used in the FY 2013 allowance calculation was less than the amount from FY 2012 "4 Bucket Report" and resulted in an understatement of the Allowance for Doubtful Accounts and the Bad Debt Expense as of and for the year ended September 30, 2013. As this was considered immaterial by GPO, management did not correct the error. (13-NFR-03)
- Commercial and government accounts payable reconciliations as of September 30, 2013 were reviewed subsequently to GPO closing the month of September 2013 financial records. We also found that the March 2013 accounts payable reconciliations were not performed because the process owner was on leave and GPO had not assigned this responsibility to another individual in the owner's absence. (13-NFR-03)

- We identified journal entries that did not agree to the supporting documentation and an amount was recorded to an incorrect account. (13-NFR-03)
- We found that the lag factor accrual schedule did not take into account the last 3 months of the fiscal year, which resulted in an understatement of revenue and expense by approximately \$1.4 million. We also found that the lag factor accrual schedule contained mathematical errors, which understated the accrual by approximately \$37 thousand. As this was considered immaterial by GPO, management did not correct the error. (13-NFR-03)
- We identified a commercial printing job for which GPO had paid the expense during the year but had not invoiced the customer as of September 30, 2013 resulting in \$13,271 of revenue not being billed as of September 30, 2013. GPO subsequently billed for this amount. (13-NFR-07)
- During our testwork over a sample of unbilled accounts receivable items totaling approximately \$2.7 million, we identified the following:
 - Because of an error in coding one sample item in the amount of approximately \$97 thousand, the item was erroneously not billed to the customer although the contractor had fulfilled the requirements of the contract as of September 30, 2013. As this was considered immaterial by GPO, management did not correct the error. (13-NFR-07)
 - Two sample items related to projects completed in the prior year and no further billings were anticipated. Therefore, the billing variance related to these projects should have been recorded in a previous fiscal year and not in FY 2013. Because of the errors we identified, management performed an analysis over the unbilled accounts receivable account and determined the errors were isolated to (1) monthly jackets (a production and billing mechanism for print jobs) and (2) jackets prior to FY 2009 that had not been closed out even though no further billings were anticipated. As a result of this analysis, management determined that 585 jackets totaling \$2.1 million should have been closed out prior to FY 2013 as no further billings were anticipated. Management corrected this error. (13-NFR-10)
- We performed test work on the advanced billings detail and identified projects that were still recorded in advance billings for which GPO had not properly recognized the revenue. The total balance related to these advanced billings was approximately \$935 thousand as of September 30, 2013. GPO subsequently recorded an adjustment to remove these balances from advanced billings as of September 30, 2013. (13-NFR-09)
- We performed a statistical sample of commercial printing revenue and found that GPO had inadvertently invoiced a commercial printing project, resulting in an overstatement of advanced billings. The projected revenue overstatement as a result of this error is approximately \$1.6 million, which includes the known overstatement of approximately \$167 thousand. As this was considered immaterial by GPO, management did not correct the error. (13-NFR-09)

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.
- 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.

Management reviews are considered a key aspect of control monitoring. Examples of control activities include reviews by management at the functional or activity level. Specifically, the *Standards for Internal Control in the Federal Government* state:

Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.

Recommendations:

We recommend that GPO strengthen its controls over the timely and accurate preparation and review of reconciliations, journal entries, and other adjustments as follows:

1. Establish a level of precision and timeframe for completion of account reconciliations in monthly financial information packages and year-end financial statements. We also recommend GPO management establish a policy for completion of timely reviews of account reconciliations to include evaluation of supporting schedules and reports for completeness and accuracy.
2. Strengthen policies and procedures over the preparation and review of customer bills prior to sending them to customers to ensure completeness and accuracy of each bill and its components.
3. Develop and implement policies and procedures to ensure all commercial bills from the contractors are reviewed and ensure that the customer invoices are generated once the final bill from the contractor is received.
4. Develop and implement policies and procedures to ensure that advanced billing related transactions and balances are properly recorded and evaluated throughout the year.
5. Develop and implement policies and procedures to ensure that balances recorded in unbilled accounts receivable are proper throughout the year and all final billed jackets are properly recorded.
6. Ensure that supervisors are properly reviewing reconciliations, journal entries and any supporting schedules used by GPO to determine final account balances, which includes tracing inputs to underlying data and testing the mathematical accuracy any schedules or calculations used.

Management Response:

Management concurs with the finding. GPO will revise and implement the revised SOPs for reconciliation review and journal entry reviews by June 30, 2014. The revisions will include a realistic timeline for completing reconciliations before the monthly performance information packages are published and completing the year-end reconciliations before the fiscal year is closed and provide guidance for cross footing supporting spreadsheets to eliminate the identified footing errors. The journal entry review SOP will provide guidance and review documentation procedures to establish the appropriate level of review and proofing based on the potential misstatement that could arise from an error in the entry.

Unbilled items will be reviewed on a weekly basis using the Partial Payment Report. Accounts Payable will check weekly all code 8 items when they reach 60 days old to determine if they should be moved to Code 9 (ready to bill).

Significant Deficiency

2013-02 Internal Controls over Information Technology General and Application Controls

During FY 2013, we identified deficiencies in the design and/or operations of GPO's information technology (IT) general controls in the areas of Security Management, Access Controls, Segregation of Duties, 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:

Security Management

We found that GPO major applications did not have finalized Certification and Accreditation (C&A) packages, including Authority to Operate Letters and System Security Plans.

GPO management stated that IT Security did not have the resources to perform a security certification review of two of its major applications due to the workload of other, higher priority application C&A activities and IT Security operational activities.

The lack of completed C&A packages increases the likelihood of unidentified threats compromising the integrity and confidentiality of GPO financial information because system security risks and requirements have not been documented and assessed. GPO Directive 825.33B *Information Technology (IT) Security Program Statement of Policy*, dated May 24, 2011, states systems will undergo C&A before they process any data. Additionally, systems will be re-accredited at least every 3 years. (NFR-IT-2013-06)

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.

The National Institute of Standards and Technology (NIST) Special Publication (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 NIST 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.
- Ensure the final, agreed-upon set of security controls is documented with appropriate rationale in the security plan for the information system. The authorizing official or designated representative, by accepting the security plan, agrees to the set of security controls proposed to meet the security requirements for the information system.

Recommendation:

We recommend that the Chief Information Officer (CIO) allocate the appropriate resources to complete the C&A package documents and process for both application systems and obtain an Authority to Operate.

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:

- User access was granted without the appropriate documented authorization (NFR-IT-2013-05):
 - One of 15 new GPO IT General Support System (GSS) users selected was granted access to the system before the user's access was authorized by the supervisor.
 - GPO was unable to provide documented evidence that three of four new GSS operating system administrators were appropriately authorized prior to obtaining system administrator access.

GPO did not consistently ensure that proper access authorization was documented and accounted for prior to granting new users access to the GPO GSS. Although general policies for restricting unauthorized access were documented, clear and defined procedures for authorizing and granting access to new users were not adequately documented.

Creating user accounts without the proper documented authorization increases the likelihood that unauthorized users will gain access to information systems, increasing the risk that the confidentiality and integrity of information systems will be compromised.

- User access was not consistently removed after users left GPO or changed job duties (NFR-IT-2013-02). Specifically, we found the following:
 - Four of 99 separated employees retained active GPO Financial System accounts for a period ranging from 114 to 139 days after their separation date as of our test work on September 13, 2013.
 - One of 99 separated employees retained an active account for 136 days after their separation date as of our test work on September 13, 2013.
 - Three of 99 separated employees retained an active account for a period ranging from 51 to 326 days after their separation date as of our test work on September 23, 2013.

Supervisors did not consistently follow the account termination policies and procedures for separated users. In addition, GPO management did not actively monitor the systems to ensure that separated user accounts were disabled from the systems in a timely manner.

Failure to disable user access immediately upon termination increases the likelihood of unauthorized access to GPO systems, which increases the risk of a compromise of the confidentiality and integrity of GPO financial data and other sensitive information.

- Periodic reviews of user access were not consistently documented (NFR-IT-2013-03). Specifically, we found the following:
 - There is no process in place to perform and document a periodic review of personnel with access to the system's Platform to determine whether user access is appropriate.
 - GPO's Finance Department was unable to provide evidence of a completed user account review for the application during the current fiscal year.
 - Through inquiry, GPO management identified that user account reviews occur on a monthly basis. However, GPO was unable to provide evidence of user account reviews for one of the two months selected.

GPO management had not formally documented and defined the frequency with which user accounts should be reviewed and the procedures involved with reviewing the accounts. Therefore, GPO management cannot properly monitor and consistently ensure that user accounts were reviewed appropriately and documentation retained.

Failure to formally document the frequency and procedures involved with reviewing accounts and the failure to appropriately and timely recertify accounts on the network and applications increase the likelihood of unauthorized or inappropriate access. This increases the risk that the confidentiality and integrity of information and information systems will be compromised.

GPO Directive 825.33B *Information Technology (IT) Security Program Statement of Policy*, dated May 24, 2011, states:

- Users and administrators of IT resources are accountable for all activity performed under their unique User ID.
- Each system will have a process in place that ensures individuals are denied access to the system when employment is terminated.
- User lists and privileges will be periodically reviewed. The review will be the basis for modifying access levels, including denying access to individuals as a result of task changes or changes in employment status.
- Access control lists will be reviewed and updated on a periodic basis. Access will be denied to individuals who have been terminated or, at the discretion of management, to those that are the subject of adverse personnel actions.

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:

- Grant access to the system based on a valid access authorization;
- 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.

Recommendation:

We recommend that the CIO:

1. Evaluate, revise as necessary and formally document GPO's procedures for authorizing and granting new users access to the GPO system to help ensure that system access is not granted without the proper authorization.
2. Evaluate, revise as necessary, and enforce policies and procedures regarding timely removal of system access for separated personnel to help ensure that system access is removed immediately at the time personnel leave GPO.
3. Evaluate, revise as necessary and formally document policies and procedures for periodically reviewing access to GPO systems to help ensure that access is reviewed on a defined frequency and that the review is documented.
4. Establish and implement controls to monitor compliance with such policies.

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 the financial system, the procedures are not sufficiently detailed to identify which roles within the system are considered to be conflicting. Not identifying conflicting roles within the system may lead to system 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 (NFR-IT-2013-04).

GPO management stated that in an effort to mitigate the disconnect between the segregation of duties procedures and the system user listing they are in the process of implementing an Oracle Government, Risk, and Compliance module. However, due to resource constraints and other priorities, this issue is not scheduled to be mitigated until February 2014.

Without the proper alignment of the segregation of duties procedures and the system user listing, it makes it difficult for management to identify and monitor users with conflicting roles and responsibilities. This increases the likelihood that users with conflicting roles and responsibilities can go undetected.

GPO Directive 825.33B: *Information Technology (IT) Security Program Statement of Policy*, dated May 2011, states the CIO is responsible for "(11) Ensuring that appropriate senior GPO officials are: (e) Maintaining appropriate segregation of duties and the periodic review of access levels for programs and systems over which they have control."

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:

- Implement separation of duties through assigned information system access authorizations.

Recommendation:

We recommend that the CIO:

1. Continue to implement the Oracle Government, Risk, and Compliance module in order to link the responsibilities of GBIS to user roles to ensure that users do not have conflicting responsibilities.
2. Revise and update GPO's procedures for maintaining segregation of duties within the system so that the procedures include sufficient detail to identify conflicting roles within the system.

Contingency Planning

The contingency plan for GPO's GSS had not been finalized, approved or tested, and was 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. (NFR-IT-2013-01)

GPO management stated that it had not finalized, approved, or fully tested the contingency plan for the GSS due to limited resources and the scope of the project.

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.

Recommendation:

We recommend that the CIO ensure that:

1. GPO management finalize and approve the contingency plans for GPO's GSS.
2. GPO management periodically perform contingency plan testing and document the test plans and the results for GPO's GSS.

Management Response:

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