U.S. GOVERNMENT PUBLISHING OFFICE
OFFICE OF INSPECTOR GENERAL

MANAGEMENT LETTER
REPORT NUMBER 16-05

Information Technology
FY 2015 Financial Statements

January 22, 2016

MEMORANDUM

U.S. GOVERNMENT PUBLISHING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

January 22, 2016

To

Director, U.S. Government Publishing Office

From

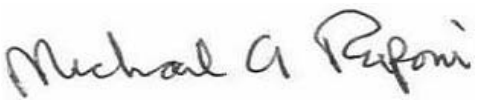
Inspector General

Subject:

Information Technology—FY 2015 Financial Statements
Report Number 16-05

In connection with the audit of the U.S. Government Publishing Office's FY 2015 financial statements, the Office of Inspector General (OIG) is providing the attached letter to describe comments and recommendations intended to improve internal controls associated with financial accounting computer systems. The findings and recommendations are detailed in the attached management letter.

We appreciate the courtesies extended 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 Director, U.S. Government Publishing Office
General Counsel
Chief of Staff
Chief Information Officer
Chief Financial Officer
Chief Administrative Officer

United States Government Publishing Office

Findings over Information Technology Controls Identified During the Fiscal Year 2015 Consolidated Financial Statement Audit

Table of Contents

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

December 23, 2015

Director
United States Government Publishing Office

Office of the Inspector General
United States Government Publishing Office:

In planning and performing our audit of the consolidated financial statements of the United States Government Publishing Office (GPO), as of and for the year ended September 30, 2015, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to the financial audits contained in the *Government Auditing Standards*, issued by the Comptroller of the General of the United States, we considered GPO's internal control over financial reporting (internal control) as a basis for designing 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 GPO's internal control. Accordingly, we do not express an opinion on the effectiveness of GPO's internal control.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in Appendix A to this report. Appendix B presents the status of prior year findings. Comments involving internal control and other operational matters that do not relate to information technology systems were communicated to you in a separate letter dated December 23, 2015.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of GPO's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The purpose of this letter is solely to describe comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

Appendix A – Findings and Recommendations

I. Summary of Findings

Implementing effective IT controls and continuously monitoring those controls is an ongoing challenge at the GPO and other Federal entities. Our IT findings and recommendations are summarized below, by Federal Information Systems Audit Controls Manual (FISCAM) area.

Access Controls

In close concert with an organization's entity-wide information security program, access controls for general support system (GSS) and applications should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized modification, disclosure, loss, or impairment. Access controls are facilitated by an organization's entity-wide security program. Such controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of information.

During our fiscal year (FY) 2015 IT control testing, we noted that access controls could be improved. Noted below are specific areas for improvement:

- NFR IT 2015-01 – Weaknesses Identified in the GPO Oracle Financials (GBIS) Termination Process

Segregation of Duties

Effective segregation of duties starts with effective entity-wide security program and access control policies and procedures that are implemented at the network and application levels. Work responsibilities should be segregated so that one individual does not control all critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, an individual should not be able to create vendors and initiate and approve payments to vendors.

The objectives of limiting access are to ensure that users have only the access needed to perform their duties; that access to sensitive resources, such as security software programs, is limited to few individuals; and that employees are restricted from performing incompatible functions or duties beyond their responsibility. This is reiterated by Federal guidelines. For example, Office of Management and Budget (OMB) Circular A-130 and supporting National Institute of Standards

and Technology (NIST) publications provide guidance related to the maintenance of technical access controls.

During our FY 2015 IT control testing, we noted that segregation of duties controls could be improved. Noted below is a specific area for improvement:

- NFR IT 2015-02 – Weaknesses Identified in the GBIS Segregation of Duties Policy

Contingency Planning

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. For this reason, an agency should have: 1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and 2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

During our FY 2015 IT control testing, we noted that contingency planning controls could be improved. Noted below is a specific area for improvement.

- NFR IT 2015-03 – Lack of Finalized and Approved GSS Contingency Plan

II. Detailed Findings and Recommendations

Access Control

NFR-IT-2015-01 – Weaknesses Identified in the GBIS Termination Process

During the FY 2015 audit, we obtained a listing of 179 former employees that separated from the Government Publishing Office (GPO) during the current year, we noted that 19 separated employees retained active GBIS accounts for a period ranging from 31 to 298 days after their human resources separation date. However, none of the accounts were accessed after the separation date.

We noted issues similar to these since FY 2011.

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

> "Access will be denied to individuals who have been terminated, or at the discretion of management, to those that are subject of adverse personnel actions."
>
> "Each system will have a process in place that ensures individuals are denied access to the system when employment is terminated, at the discretion of management, or are the subject of adverse personnel actions."

NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, Control PS-4, *Personnel Termination*, states:

> "The organization, upon termination of individual employment:
>
> a. disables information system access within [Assignment: organization-defined time period]
> b. Terminates/revokes any authenticators/credentials associated with the individual"

Supervisors are not consistently following the account termination policies and procedures for separated users. Failure to disable user access upon termination increases the risk that the confidentiality and integrity of information and information systems will be compromised.

We recommend that the Chief Information Officer (CIO):

1. Update the policy and procedures for the timely removal of terminated users from GPO systems. This policy should also include a timeframe for removal of terminated users.
2. Communicates to supervisors the importance of submitting access termination request forms timely to system owner to allow for terminated users to be removed timely
3. Increases the frequency of the monitoring control being performed.

Segregation of Duties

***NFR-IT-2015-02* – Weaknesses Identified in the GBIS Segregation of Duties Policy**

During the FY 2015 audit, we noted GBIS separation of duties matrix is documented based on user responsibilities whereas the GBIS user listing is documented based on user roles. Therefore, the procedures and user listing do not align which makes it difficult to determine whether access was appropriately segregated for each user within the GBIS application.

GPO Directive 825.33B states:

> "Access controls will enable the use of only the resources, such as data programs, necessary to fulfill an individual's job responsibilities and will enforce separation of duties based on roles and responsibilities."

NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, Control AC-5, *Separation of Duties*, states:

> "… The organization:
> 1. Separates duties of individuals as necessary, to prevent malevolent activity without collusion,
> 2. Documents separation of duties; and
> 3. Implements separation of duties through assigned information system access authorization."

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.

We recommend that the CIO completes the implementation of the Oracle Governance, Risk and Compliance (GRC) Module that will automate separation of duties by the scheduled completion date of September 30, 2016.

Contingency Planning

***NFR IT 2015-03* – Lack of Finalized and Approved GSS Contingency Plan**

During the FY 2015 audit, we noted the Government Publishing Office (GPO) has not finalized, approved, and fully tested the draft contingency plan for its general support system because the Office 365 project was not complete. This has been reported as an issue since FY 2011.

GPO Publication 825.33, *Information Technology Security Program Statement of Policy*, states:

> "The GPO will safeguard its IT systems through the implementation of the GPO IT Security Program, which will accomplish the following: Define, document, and manage the contingency planning process, including training and testing, to provide IT systems with adequate continuity of operations upon disruption of normal operations.
>
> The Chief Information Officer (CIO) is responsible for developing and maintaining an agency-wide IT Security Program, including providing for the continuity of operations in the event of system disruption. Contingency plan means a plan for emergency response, back-up operations, and post-disaster recovery for IT systems and installations in the event normal operations are interrupted. The contingency plan should ensure minimal impact upon data processing operations in the event the IT system or facility is damaged or destroyed."

NIST Special Publication 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems*, Control CP-2, *Contingency Plan*, states:

> "The organization:
> a. Develops a contingency plan for the information system that;
> 1. Identifies essential missions and business functions and associated contingency requirements;
> 2. Provides recovery objectives, restoration priorities, and metrics;
> 3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
> 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by [Assignment: organization-defined personnel and roles]"

NIST Special Publication 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems*, Control CP-4, *Contingency Plan Testing and Exercise*, states:

> "… The organization:
> a. Tests and/or exercises the contingency plan for the information system … to determine the plan's effectiveness and the organization's readiness to execute the plan; and
> b. Reviews the contingency plan test/exercise results and initiates corrective actions."

GPO management did not finalize, approve, and fully test the contingency plan for the GSS due to the Office 365 project was not complete. Without an effective contingency plan and testing process in place, GPO may not be able to successfully recover critical applications and systems to maintain business functions during the event of a service disruption.

We recommend that the CIO:

1. GPO management finalizes and approves the contingency plans for GPO's General Support System.
2. GPO management periodically performs contingency plan testing and documents the test plans and the results for GPO's General Support System.

Appendix B – Status of Prior Year of Findings

Prior Year Finding Number	Applicable FISCAM Section	Description of Control Weakness	Status of Recommendation	Current Year NFR Number
NFR-IT-2014-01	Access Controls	GSS Session Lock Configuration Weakness	Closed	N/A
NFR-IT-2014-03	Segregation of Duties	Weaknesses Identified in the GBIS Segregation of Duties Policy	Open	NFR IT 2015-02
NFR-IT-2014-04	Access Controls	Weaknesses Identified in the GSS, PICS and GBIS Termination Process	Open for GBIS, Closed for GSS and PICS	NFR IT 2015-01
NFR-IT-2014-05	Contingency Plan	GSS contingency plan not finalized	Open	NFR IT 2015-03
NFR-IT-2014-06	Security Management	Lack of Certification and Accreditation Package	Closed	N/A
NFR-IT-2014-07	Access Controls	Weaknesses Identified in the GPO User Account Review Process	Closed	N/A

Appendix C – Acronyms

Acronym	Definitions
CIO	Chief Information Officer
FISCAM	*Federal Information System Controls Audit Manual*
FY	Fiscal Year
GBIS	GPO Oracle Financials
GSS	General support system
GPO	United States Government Publishing Office
IT	Information Technology
NFR	Notice of Finding and Recommendation
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	Special Publication