U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

MANAGEMENT LETTER
REPORT NUMBER 18-08

Information Technology
FY 2017 Financial Statements

January 19, 2018

Date

January 19, 2018

To

Acting Director, U.S. Government Publishing Office

From

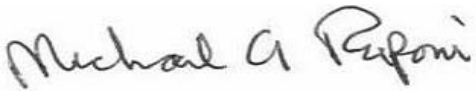
Inspector General

Subject:

Information Technology—FY 2017 Financial Statements
Report Number 18-08

In connection with the audit of the U.S. Government Publishing Office's FY 2017 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 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:
Acting General Counsel
Chief of Staff
Chief Financial Officer
Chief Administrative Officer

United States Government Publishing Office

Findings over Information Technology Controls Identified During the Fiscal Year 2017 Consolidated Financial Statement Audit

Table of Contents

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

December 15, 2017

Acting 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, 2017, 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 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 operation matters that do not relate to information technology systems were communicated to you in a separate letter dated December 15, 2017.

Our audit procedures are designed primarily to enable us to form an opinion on the consolidated 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 the 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 over information technology 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) 2017 IT control testing, we noted that access controls could be improved. Noted below are specific areas for improvement:

- NFR IT 2017-03 – Weaknesses Identified in the GBIS Separated User Process
- NFR IT 2017-04 – Weaknesses Identified in the GBIS New User 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 2017 IT control testing, we noted that segregation of duties controls could be improved. Noted below is a specific area for improvement:

- NFR IT 2017-01 – Weaknesses Identified in the GBIS Separation 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 2017 IT control testing, we noted that contingency planning controls could be improved. Noted below is a specific area for improvement.

- NFR IT 2017-02 – Lack of Finalized and Approved GSS Contingency Plan

II. Detailed Findings and Recommendations

Access Control

NFR-IT-2017-03 Weaknesses Identified in the GBIS Separated User Process

During the FY 2017 audit, we obtained a listing of 98 former employees that separated from the GPO during the current year and determined that one of these users retained active access to their account 53 days after their Human Capital separation date, which is eight days longer than GPO's timeliness policy of 45 days. However, we determined this user did not access their GBIS account after their separation date.

Additionally, we noted that GPO's timeliness policy is not restrictive enough to protect against the threat of a separated user accessing GPO systems.

We have noted similar issues related to Separated Users since FY 2011.

GPO IT Security management stated that this user was not listed on Separations Reports from the Human Capital Office during June or on the first report in July. IT Security finally got notification of this user's separation at the end of July, and the account was disabled within a week. Additionally, GPO's timeliness policy is not as restrictive as best practices that use the bi-weekly payroll separation report.

Although the user did not access their GBIS account after their separation date, failure to disable user access timely upon termination increases the risk that the confidentiality and integrity of information and information systems may be compromised.

NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, 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"

GPO Directive 825.33B: IT Security Program Statement of Policy, dated May 2011, pages 11-14, states:

> "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.
> [...]
> 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."

GPO's Procedure for Removing Access for Separated GPO Employees to Select IT Systems (LAN, PICS, Mainframe, Remote Access, GBIS and NFC), page 2, states:

> "The overall GPO requirement for access removal for Separated GPO Employees is within 45 days of official Separation Date for that GPO Employee as listed on the official Separation Report from the Human Capital Office."

We recommend that the Chief Information Officer:

1. Update Standard Operating Procedures around user separations to align with the promulgation of the bi-weekly Human Capital separations report; and

2. Validate that the bi-weekly Human Capital separation reports are pulling complete and accurate separated user data.

NFR-IT-2017-04 Weaknesses Identified in the GBIS New User Process

During the FY 2017 audit, we determined that one of five users selected was provisioned the wrong combination of roles during the GBIS account creation process.

GPO IT Security Management informed us that the wrong role was provisioned for one user due to a mismatch between what the Access Form shows the role name as, and what the actual GBIS system shows. Management also stated that the form has been updated to match the system role for this instance.

Without consistent, appropriate provisioning of roles and privileges of new GBIS application accounts there is a risk that users are granted unauthorized access to perform functions in GBIS, increasing the risk that the confidentiality and integrity of information and information systems will be compromised.

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, Control AC-2, Account Management, states:

> "The organization:
> i. Authorizes access to the information system based on:
> 1. A valid access authorization;
> 2. Intended system usage; and
> 3. Other attributes as required by the organization or associated missions/business functions;"

GPO Directive 825.33B: IT Security Program Statement of Policy, dated May 2011, states:

> "The GPO will safeguard its IT systems through the implementation of the GPO IT Security Program, which will accomplish the following:
> d. Ensure that only authorized personnel have access to information;"

We recommend that the Chief Information Officer performs a periodic review of system roles to ensure that all of the roles on the GBIS access request forms can be tied back to an access privilege within the GBIS application.

Segregation of Duties

NFR-IT-2017-01 Weaknesses Identified in the GBIS Separation of Duties Policy

During the FY 2017 audit, we determined the GBIS separation of duties (SOD) matrix is documented based on user responsibilities whereas the GBIS user listing is documented based on user roles. Therefore, it is difficult for management to effectively identify and monitor users with conflicting roles and responsibilities.

We have had similar findings since FY 2011.

The GBIS SOD Matrix has not been updated due to the continued testing of the Oracle Governance, Risk, and Compliance (GRC) Module which is scheduled to be fully implemented in FY 2018.

Without the proper alignment of the separation of duties procedures and the system user listing it is 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.

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

> "The organization:
> a. Separates [Assignment: organization-defined duties of individuals];
> b. Documents separation of duties of individuals;"

GPO Directive 825.33B: IT Security Program Statement of Policy, dated May 2011, states:

"Access controls will enable the user 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."

We recommend that the Chief Information Officer:
1. Complete testing and implementation of the GRC module into the GBIS application; and
2. Update the GBIS SOD Matrix to clearly identify conflicting system roles in the GBIS application.

Contingency Planning

NFR IT 2017-02 Lack of Finalized and Approved GSS Contingency Plan

During the FY 2017 audit, we determined that GPO had not finalized, approved, and tested the draft contingency plan for its general support system.

We have had similar findings since FY 2011.

GPO informed us that the GSS contingency plan has not been finalized, authorized, and tested due to competing business responsibilities for the resources required to perform these tasks in FY 2017.

Without an effective contingency plan and testing process in place for the GSS, GPO may not be able to successfully recover data files and systems to maintain business functions during the event of a service disruption.

In addition, without documentation of contingency plan test results, the effectiveness of management's oversight of contingency plan testing is diminished. Specifically, a lack of documented results diminishes management's ability to verify that the scope of testing and test procedures were performed consistent with their intent. Also, without documented results, management may be unaware of weaknesses in the disaster recovery capabilities that would be revealed by disaster testing.

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, 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];

GPO Directive 825.33B: IT Security Program Statement of Policy, dated May 2011, states:

> "The GPO will safeguard its IT systems through the implementation of the GPO IT Security Program which will accomplish the following: Define, documents, 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 even 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."

We recommend that the Chief Information Officer:

1. Finalizes and approves the contingency plans for GPO's General Support System.
2. Performs periodic contingency plan testing and document the test plans and the results for GPO's General Support System.

Appendix B – Status of Prior Year Findings

Prior Year Finding Number	Applicable FISCAM Section	Description of Control Weakness	Status of Recommendation	Current Year NFR Number
NFR IT 2016-01	Contingency Planning	Lack of Finalized and Approved GSS Contingency Plan	Open.	NFR-IT-2017-02
NFR IT 2016-02	Access Controls	Weakness Identified in the New GSS Administrator Process	Closed.	N/A
NFR IT 2016-03	Access Controls	Weakness Identified in the GBIS Separated User Process	Open.	NFR-IT-2017-03
NFR IT-2016-04	Segregation of Duties	Weaknesses Identified in the GBIS Separation of Duties Policy	Open	NFR-IT-2017-01

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
KPMG	KPMG LLP
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