GPO U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

MANAGEMENT LETTER
REPORT NUMBER 19-04

Information Technology
FY 2018 Financial Statements

January 31, 2019

GPO

U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

Date

January 31, 2019

To

Acting Deputy Director, U.S. Government Publishing Office

From

Acting Inspector General

Subject:

Information Technology — FY 2018 Financial Statements
Report Number 19-04

In connection with the audit of the U.S. Government Publishing Office's FY 2018 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 Mr. Freddie Hall, Assistant Inspector General for Audits and Inspections at (202) 512-1597 or me at (202) 512-1512.

JAMES R. IVES
Acting Inspector General

Attachment
cc:

Acting Chief Financial Officer, GPO
Acting Chief of Staff, GPO
Acting General Counsel, GPO

United States Government Publishing Office

Findings over Information Technology Controls Identified During the Fiscal Year 2018 Consolidated Financial Statement Audit

U.S. Government Publishing Office
Findings over Information Technology Controls Identified During the
FY 2018 Consolidated Financial Statement Audit

Table of Contents

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

December 14, 2018

Acting Deputy Director
United States Government Publishing Office

Office of the Inspector General
United States Government Publishing Office:

In planning and performing our audit of the financial statements the United States Government Publishing Office (GPO), as of and for the year ended September 30, 2018, 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, we considered the 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.

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 and/or significant deficiencies and therefore, material weaknesses and/or significant deficiencies may exist that were not identified. In accordance with *Government Auditing Standards*, we issued our report dated December 14, 2018 on our consideration of GPO's 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. During our audit we noted deficiencies in internal control related to Information Technology which are described in Appendix A of this letter. Deficiencies in internal control related to Non-Information Technology will be presented in a separate letter addressed to you. Appendix B presents the status of prior year Information Technology findings.

The purpose of this letter is solely to describe the deficiencies in internal control identified during our audit. 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) 2018 IT control testing, we noted that access controls could be improved. Noted below is a specific area for improvement:

- NFR IT 2018-03 – Weaknesses Identified in the GBIS Separated 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, *Managing Information as a Strategic Resource* and supporting National Institute of Standards and Technology (NIST) publications provide guidance related to the maintenance of technical access controls.

During our FY 2018 IT control testing, we noted that segregation of duties controls could be improved. Noted below is a specific area for improvement:

- NFR IT 2018-01 – 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 2018 IT control testing, we noted that contingency planning controls could be improved. Noted below is a specific area for improvement:

- NFR IT 2018-02 – Lack of Finalized and Approved GSS Contingency Plan

II. Detailed Findings and Recommendations

Access Control

NFR-IT-2018-03: Weaknesses Identified in the GBIS Separated User Process

During the FY 2018 audit, we obtained a listing of 121 former employees that separated from the GPO during the current year and determined that 2 of these users retained active access to their account for 53 and 66 days after their Human Capital separation date, which is 8 and 21 days longer than GPO's timeliness policy of 45 days. However, we determined these users 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.

The information of these two separated individuals were not provided to GPO IT Security management in the separations reports timely to disable their accounts. Additionally, GPO's timeliness policy is not as restrictive as best practices that use bi-weekly payroll separation report.

Although the users did not access their GPO Oracle Financials (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.

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."

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"

We recommend that the Chief Information Officer:

1. Update Standard Operating Policies and 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.

Segregation of Duties

NFR-IT-2018-01: Weaknesses Identified in the GBIS Separation of Duties Policy

During the FY 2018 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, to fix bugs identified in Oracle R12. Testing is scheduled to be completed in early FY2019.

Without the proper alignment of the separation of duties procedures and the system user listing it is difficult for management to effectively 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: 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."

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;"

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 2018-02: Lack of Finalized and Approved GSS Contingency Plan

During the FY 2018 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 and authorized due to outstanding testing that is being completed and finalized.

Without an effective, and approved 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.

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."

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];

We recommend that the Chief Information Officer:

1. Complete the GSS Contingency Plan testing; and
2. Finalize and approve the new GSS contingency plan once testing is complete.

Appendix B – Status of Prior Year Information Technology Findings

Prior Year Finding Number	Applicable FISCAM Section	Description of Control Weakness	Status of Recommendation	Current Year NFR Number
NFR-IT-2017-01	Segregation of Duties	Weaknesses Identified in the GBIS Separation of Duties Policy	Open	NFR-IT-2018-01
NFR IT 2017-02	Contingency Planning	Lack of Finalized and Approved GSS Contingency Plan	Open	NFR-IT-2018-02
NFR IT 2017-03	Access Controls	Weakness Identified in the GBIS Separated User Process.	Open	NFR-IT-2018-03
NFR-IT-2017-04	Access Control	Weakness Identified in the GBIS New User Process	Closed	N/A