U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

MANAGEMENT LETTER
REPORT NUMBER 20-04

Information Technology Management Letter FY2019 Financial Statements

December 13, 2019

U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

Date

December 13, 2019

To

Director, U.S. Government Publishing Office

From

Inspector General

Subject:

Information Technology Management Letter – Fiscal Year 2019 Financial Statements
Report Number 20-04

In connection with the audit of the U.S. Government Publishing Office (GPO) FY 2019 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 W. Hall, Assistant Inspector General for Audits at (202) 512-1597 or me at (202) 512-0039.

Michael P. Leary
Inspector General

Attachment
Cc:
Acting Deputy Director
Chief Financial Officer
Acting Chief of Staff
Acting General Counsel

KPMG

United States Government Publishing Office

Finding over Information Technology Controls Identified During the Fiscal Year 2019 Consolidated Financial Statement Audit

Table of Contents

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

December 12, 2019

Director
United States Government Publishing Office

Inspector General
United States Government Publishing Office:

In planning and performing our audit of the financial statements of the United States Government Publishing Office (GPO), as of and for the year ended September 30, 2019, 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 12, 2019 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 a deficiency in internal control related to Information Technology (IT) which is described in Appendix A of this letter. Deficiencies in internal control related to Non-IT will be presented in a separate letter addressed to you. Appendix B presents the status of prior year findings.

The purpose of this letter is solely to describe the deficiency in IT internal control identified during our audit. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

Appendix A – Finding and Recommendation

I. Summary of Finding and Recommendation

Implementing effective Information Technology (IT) controls and continuously monitoring those controls is an ongoing challenge at the GPO and other Federal entities. Our IT finding and recommendation is related to the Federal Information Systems Audit Controls Manual (FISCAM) area of access controls.

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) 2019 IT control testing, we noted that access controls could be improved. Noted below is a specific area for improvement:

- NFR IT-2019-01 Weakness Identified in the PROBE Server Administrator Recertification Process

II. Detailed Finding and Recommendation

Access Control

NFR-IT-2019-01 Weakness Identified in the PROBE Server Administrator Recertification Process

During our FY 2019 audit, we inspected the access recertification evidence for PROBE Server Administrators and determined there were seven administrators, out of 86 total administrators, who did not have their access recertified in FY 2019.

However, in response to our finding, management updated the excel file used for recertification during the last week of the fiscal year to include the users who were previously not listed, and those users' administrator access rights were reviewed and verified by the Chief Information Security Officer (CISO).

GPO Directive 825.33B: Information Technology (IT) Security Program Statement of Policy, dated May 2011, page 11 states:

> "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. Further, this section applies to contractors or others working on behalf of the GPO where the Government information assets are being used regardless of whether they are working on-site or off-site."

National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, Control AC-2, Account Management, states:

> "The organization manages information system accounts, including:
>
> j. Reviewing accounts for compliance with account management requirements [Assignment: organization-defined frequency}"

GPO IT Security management stated that the Active Directory (AD) group, that contains these particular server administrators for PROBE application administrator access, was inadvertently not included in the queries that created the Excel file which listed the administrators for recertification.

Without a periodic review of the appropriateness of privileged user access rights or permissions increases the risk that unauthorized access to the PROBE infrastructure and users performing functions that do not match their job descriptions, and potential segregation of duties conflicts, will not be detected and prevented timely. These issues also increase the risk that the confidentiality, integrity, and availability of GPO financial data and other sensitive information could be compromised.

We recommend that management periodically review the queries used to generate the Excel file for the administrator recertification process to ensure no users are excluded.

Appendix B – Status of Prior Year IT Findings

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