OFFICE *of the*
INSPECTOR GENERAL
U.S. GOVERNMENT PUBLISHING OFFICE

Date:
December 15, 2021

To:
Director, U.S. Government Publishing Office

From:
Inspector General, U.S. Government Publishing Office

Subject:
Management Letter on Information Technology – Fiscal Year 2021 Financial Statements

In connection with the audit of the U.S. Government Publishing Office fiscal year (FY) 2021 financial statements, we are providing the attached information technology (IT) management letter issued by the independent public accounting firm of KPMG LLP (KPMG). The IT management letter describes a deficiency in internal controls identified during their audit, and recommendations intended to improve internal controls associated with financial reporting. KPMG is responsible for the attached IT management letter dated December 15, 2021.

We appreciate the courtesies extended to KPMG and our staff. If you have any questions or comments about this report, please do not hesitate to contact Lori Lau Dillard, Assistant Inspector General for Audits, at llaudillard@gpo.gov or me at mleary@gpo.gov.

Digitally signed by Michael P. Leary
Date: 2021.12.15 16:03:47 -05'00'

MICHAEL P. LEARY
Inspector General

Attachment

The United States Government Publishing Office

Information Technology Management Letter

For the Year Ended September 30, 2021

U.S. Government Publishing Office
Information Technology Management Letter
For the Year Ended September 30, 2021

Table of Contents

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

December 15, 2021

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, 2021, in accordance with auditing standards generally accepted in the United States of America and in accordance with 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 15, 2021 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 identified 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.

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 – Comment and Recommendation

Weakness Identified in the GBIS Separated Users Process (NFR-IT-2021-01)

During the fiscal year (FY) 2021 audit, we noted that the GPO's Business Information System (GBIS) access separation control was not operating effectively. We noted that five of 37 GBIS application user accounts were not disabled within 15 calendar days of the date of their separation.

GPO Directive 825.33C: *Information Technology (IT) Security Program Statement of Policy*, dated March 19, 2021, pages 5 states:

> "Managers and supervisors at GPO shall ensure that a request to the IT Service HUB is submitted to remove access for any personnel in their unit that separate from GPO and no longer require GPO IT system access within 15 calendar days of the date of separation."

These user accounts were not timely disabled due to the following:

1. For three users, the GBIS application administrator did not review and deactivate separated employees' GBIS accounts upon receiving the bi-weekly Human Capital separation reports as required by the GPO's policy.
2. For two users, due to employee's name change, the GBIS application administrator did not identify and deactivate separated employees' GBIS accounts upon receiving the bi-weekly Human Capital separation report as required by the GPO's policy.

Without effective controls in place to ensure user access is timely disabled upon separation there is an increased risk that the confidentiality and integrity of GBIS financial data and other sensitive information may be compromised.

We recommend that GPO management:

1. Provide oversight over GBIS control performers to review and monitor the removal of separated user accounts from the application in a timely manner in accordance with GPO Directive 825.33C; and
2. Enhance the existing control by providing more detailed guidance to control performers on the requirements of reviewing and disabling separated employees' application accounts in the case of name changes.