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

Date:
December 13, 2024

To:
Director, U.S. Government Publishing Office

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

Subject:
Information Technology Management Letter – Fiscal Year 2024 Consolidated Financial Statements Audit

In connection with the audit of the U.S. Government Publishing Office Fiscal Year 2024 Consolidated 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 one deficiency in internal controls identified during their audit and two recommendations intended to improve internal controls associated with financial reporting. KPMG is responsible for the attached IT management letter dated December 13, 2024.

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 Audit, at llaudillard@gpo.gov, or me at ndeahl@gpo.gov.

Nathan Deahl

NATHAN J. DEAHL
Inspector General

Attachment

UNITED STATES GOVERNMENT PUBLISHING OFFICE

INFORMATION TECHNOLOGY MANAGEMENT LETTER

FOR THE YEAR ENDED SEPTEMBER 30, 2024

United States Government Publishing Office

Information Technology Management Letter

For the Year Ended September 30, 2024

Table of Contents

KPMG

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

December 13, 2024

Director
United States Government Publishing Office

Inspector General
United States Government Publishing Office

To the Director and Inspector General of the 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, 2024, 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 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 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 13, 2024 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 processes will be presented in a separate letter addressed to you.

This 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

Comments and Recommendations

A. Plant Operations Manufacturing System (POMS) Lack of Access Configuration Change Controls Procedures Deficiency (IT 24-NFR-01)

Access and configuration change management controls for POMS were not designed or implemented in FY 2024. Specifically, we identified the following:

1. POMS management was unable to provide documentation to support that provisioned POMS "full access" administrators[1] were appropriate and authorized or that access for all terminated POMS "full access" administrators was removed.
2. POMS management did not design and implement controls over segregation of duties between users who develop in-house configuration changes and users who deploy the configuration changes to the POMS production environment. Additionally, POMS management was unable to provide documentation to support the review, testing, and approval of all in-house configuration changes prior to implementation.

The Government Accountability Office *Standards for Internal Control in the Federal Government* (September 2014), states:

- Principle 7.01, *Identify, Analyze, and Respond to Risks*: Management should identify, analyze, and respond to risks related to achieving the defined objectives. The following attributes contribute to the design, implementation, and operating effectiveness of this principle:
  - Identification of Risks
  - Analysis of Risks
  - Response to Risks
- Principle 10.02, *Design Control Activities*: Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part of the risk assessment component, management identifies the risks related to the entity and its objectives, including its service organizations; the entity's risk tolerance; and risk responses. Management designs control activities to fulfill defined responsibilities and address identified risk responses.
- Principle 11.03, *Design Activities for the Information System*: Management designs the entity's information system to obtain and process information to meet each operational process's information requirements and to respond to the entity's objectives and risks. An information system is the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information. An information system represents the life cycle of information used for the entity's operational processes that enables the entity to obtain, store, and process quality information. An information system includes both manual and technology-enabled information processes. Technology-enabled information

[1] The "full access" system group grants read / write permissions to all POMS objects and reports. These users have full control of all licensed modules and module setups as well as customization tools. Additionally, it provides access to the console where the server logs, diagnostics, and upgrade tools are found.

processes are commonly referred to as information technology. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part of the risk assessment component, management identifies the risks related to the entity and its objectives, including its service organizations; the entity's risk tolerance; and risk responses. Management designs control activities to fulfill defined responsibilities and address the identified risk responses for the entity's information system.

National Institute of Standards and Technology Special Publications 800-53 Revision 5.1.1, *Security and Privacy Controls for Federal Information Systems and Organizations* (November 2023), states:

- Access Control (AC)-2: Account Management:

  d. Specify authorized users of the information system, group and role membership, and access authorization (i.e., privileges) and other attributes (as required) for each account

  e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;

  f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];

  i. Authorize access to the system based on:

     1. A valid access authorization;

     2. Intended system usage; and

     3. [Assignment: organization-defined attributes (as required)].

- Configuration Management (CM)-3 Configuration Change Control:

  b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

  c. Document configuration change decisions associated with the system;

  d. Implement approved configuration-controlled changes to the system;

  e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period].

GPO POMS *System Security Plan*, Version 1.0 (January 2023), states:

- Control AC-5: The POMS systems account and security management is maintained and managed according to the concepts of least privilege and separation of duties. These concepts are implemented for access to the database and other system components.

- Control CM-3: The POMS administrators documents all configuration changes to the POMS system. All POMS application updates go through the GPO Technical Change Control Board process for changes.

  d. After review for system applicability and testing, POMS system administrators apply all applicable system updates/patches to the POMS environment.

  e. POMS administrator retains all emails and correspondence concerning the POMS system updates/patches indefinitely.

  f., g. The POMS administrator is responsible for audits and reviews, coordination and provides the oversight for all configuration control activities involving the POMS system.

- Control CM-3 (2): All hardware and software changes move through a strict approval and testing process, this permits orderly operation and prevents unauthorized actions to POMS that could damage or compromise security. Changes are monitored and documented in accordance with organizational policies and procedures.

POMS management did not perform a sufficient risk assessment to identify risks in access and configuration change management and design control activities in response. Specific to the supporting documentation for review, testing, and approval of changes, the POMS administrators approved changes verbally and therefore did not retain evidence supporting the update to the POMS environment in accordance with standard operating procedures.

The lack of designed and implemented controls for POMS increase the risk that the confidentiality, integrity, or availability of POMS information and data could be compromised. Without sufficient controls in place to provision and deprovision user access, there is a risk that unauthorized POMS administrators leverage their access to make unauthorized changes to the system or its underlying data that are used to execute financial transactions ultimately summarized and reported in GPO's financial statements. In addition, without sufficient controls in place to enforce appropriate separation of duties, there is a risk that malicious or unauthorized changes could be implemented into the production environment without detection. Further, failure to retain documentation for the approval and testing of configuration changes in the POMS production environment could result in POMS management inability to detect ineffective change configuration management policies, procedures, and control activities.

We recommend that POMS management perform a risk assessment in order to design and implement controls to provision and deprovision access to POMS "full access" administrators, enforce segregation of duties, and approve and test configuration changes. Further, we recommend POMS management provide training over the defined procedures relating to access provisioning and deprovisioning for POMS "full access" administrators, segregation of duties, and configuration change management.