Audit Report

OIG-24-014

FINANCIAL MANAGEMENT

Management Letter for the Audit of the Office of the Comptroller of the Currency's Financial Statements for Fiscal Years 2023 and 2022

December 8, 2023

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D. C. 20220

December 8, 2023

MEMORANDUM FOR MICHAEL J. HSU
ACTING COMPTROLLER OF THE CURRENCY

FROM: Ade Bankole /s/
Director, Financial Statement Audits

SUBJECT: Management Letter for the Audit of the Office of the Comptroller of the Currency's Financial Statements for Fiscal Years 2023 and 2022

We hereby transmit the attached subject management letter. Under a contract monitored by our office, GKA, P.C. (GKA), a certified independent public accounting firm, audited the financial statements of the Office of the Comptroller of the Currency (OCC) as of September 30, 2023, and for the year then ended. OCC's financial statements as of September 30, 2022 were audited by other auditors. The contract required that the audit be performed in accordance with U.S. generally accepted government auditing standards, Office of Management and Budget Bulletin No. 24-01, *Audit Requirements for Federal Financial Statements,* and the Government Accountability Office/Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual.*

As part of its audit, GKA issued the attached management letter dated October 31, 2023, that discusses matters involving deficiencies in internal control over financial reporting that were identified during the audit. These matters involved information system controls.

In connection with the contract, we reviewed GKA's management letter and related documentation and inquired of its representatives. GKA is responsible for the letter and the conclusions expressed in the letter. However, our review disclosed no instances where GKA did not comply, in all material respects, with U.S. generally accepted government auditing standards.

If you wish to discuss this report, please contact me at (202) 927-5329, or a member of your staff may contact Shiela Michel, Manager, Financial Statement Audits, at (202) 486-1415.

Attachment

This Page Intentionally Left Blank

gka, p.c.
Certified Public Accountants
& Consultants

1920 L Street, NW
Suite 425
Washington, DC 20036
Tel: 202-857-1777
www.gkacpa.com

OFFICE OF THE COMPTROLLER OF THE CURRENCY

MANAGEMENT LETTER
FISCAL YEAR 2023

October 31, 2023

SENSITIVE BUT UNCLASSIFIED (SBU)

gka,p.c.
Certified Public Accountants
& Consultants

Principal Deputy Comptroller for Management and Chief Financial Officer
Office of the Comptroller of the Currency

Deputy Inspector General
U.S. Department of the Treasury

We have audited the financial statements of the Office of the Comptroller of the Currency (OCC), which comprise the balance sheet as of September 30, 2023, and the related statements of net costs, changes in net position, budgetary resources and custodial activity for the year then ended, and the related notes to the financial statements, hereinafter referred to as the "financial statements", and have issued our report thereon dated October 31, 2023.

In planning and performing our audit of the financial statements of OCC, we considered OCC's internal control over financial reporting (internal control) as a basis for designing the 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 OCC's internal control. We have not considered the internal control since the date of our report.

During our audit we identified no deficiencies in internal control that we consider to be a significant deficiency. However, we noted certain matters involving the internal control over financial reporting, compliance and other operational matters that are presented in this letter for your consideration. We do not consider these matters to be a material weakness or significant deficiency. The comments and recommendations, all of which have been discussed with the appropriate members of OCC Management, are intended to improve the internal control over financial reporting or result in other operational efficiencies. Appendix A presents the status of the prior year deficiency.

The OCC management's responses to our comments and recommendations have not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we do not express an opinion or provide any form of assurance on the appropriateness of the responses, or the effectiveness of any corrective action described therein.

We appreciate the cooperation and courtesies extended to us. We will be pleased to meet with you or your staff at your convenience to furnish any additional information.

GKA, P.C.
October 31, 2023

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2023

2023-1 Controls for Updating Security Artifacts should be Strengthened

Controls for updating security documentation related to the OCC's financial management system and the Network General Support System (GSS) should be strengthened. Specifically, we noted the following.

- The GSS Information System Contingency Plan (ISCP) was not updated and approved since September 24, 2019. OCC completed plan updates on September 6, 2023; however, the weakness was in place for the majority of the fiscal year.
- The financial management system and GSS System Security Plans (SSP) did not identify the interconnections in place for each system.
- OCC has an open Plans of Actions and Milestones (POA&M) (IPT0021274) stating that the financial management system SSP was outdated and does not reflect the current Audit and Accountability control implementations including outdated referencing to other systems.
- OCC identified in the Network GSS Security Assessment Report that the GSS SSP referenced outdated documentation, subsystems that were no longer applicable and contained incomplete/inaccurate/inadequate implementation statements. We noted that this issue was not yet resolved.

OCC's Control CP-2 Contingency Plan of the Master Security Control Catalog, version 4.0, *Security Controls by Family*, states:

d. Review the contingency plan for the system at least annually and following significant events;
e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to system stakeholders as identified in the security and privacy plan;
g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training;

OCC's Control PL-2 System Security and Privacy Plans of the Master Security Control Catalog, version 4.0, *Security Controls by Family*, states:

a. Develop security and privacy plans for the system that:
1. Are consistent with the organization's enterprise architecture;
2. Explicitly define the constituent system components;
3. Describe the operational context of the system in terms of mission and business processes;
4. Identify the individuals that fulfill system roles and responsibilities;
5. Identify the information types processed, stored, and transmitted by the system;
6. Provide the security categorization of the system, including supporting rationale;
7. Describe any specific threats to the system that are of concern to the organization;
8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

9. *Describe the operational environment for the system and any dependencies on or connections to other systems or system components;*
10. *Provide an overview of the security and privacy requirements for the system;*
11. *Identify any relevant control baselines or overlays, if applicable;*
12. *Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;*
13. *Include risk determinations for security and privacy architecture and design decisions;*
14. *Include security- and privacy-related activities affecting the system that require planning and coordination with stakeholders for interconnected information systems and information sharing partners; and*
15. *Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.*

b. *Distribute copies of the plans and communicate subsequent changes to the plans to key system stakeholders;*
c. *Review the plans at least annually and in response to significant events and system changes;*
d. *Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and*
e. *Protect the plans from unauthorized disclosure and modification.*

OCC Management was aware of deficiencies related to the review and update of contingency plans (ISCP) and security plans (SSP) for the financial management system and the network GSS. The POA&M had been developed to track OCC's efforts to review and update its security plans and contingency plans; however, the due date per OCC POA&M remediation timeframes to complete these changes is outside of the current fiscal year. Also, OCC was migrating the GSS to a new disaster recovery datacenter that also slowed down the update process for the ISCP. Additionally, while the GSS ISCP was updated by September 6, 2023, the prior plan update was September 24, 2019; therefore, the weakness in the review and update controls existed for most of the fiscal year.

Weaknesses in controls over the annual review and update of security documentation increase the risk that Authorizing Officials may not be provided accurate information with respect to control implementation to inform their ongoing authorization decisions. Additionally, a lack of review and update for contingency plans increases the risk that systems may not be able to be recovered timely during a contingency situation due to out of date information or procedures.

Recommendation

We recommend OCC ensure that:

- the GSS Contingency Plan is reviewed annually and updated if changes are needed per the Master Security Control Catalog, and
- the GSS and the financial management system SSPs are reviewed and updated to address the following items:
    - Identify system interconnections.

- Update the incomplete, inaccurate, or inadequate implementation statements.
- Identify the current system components/subsystems in place.

Management Response

The Network GSS is called the Information Technology Infrastructure General Support System (ITI GSS). The OCC will incorporate the annual review of the ITI GSS Contingency Plan into the ITI GSS Information Security Continuous Monitoring Plan (ISCM) activities, including a task to update the Contingency Plan should changes occur per the Master Security Control Catalog, CP-2. e: "*Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing,"* to ensure annual reviews and any necessary updates are being conducted.

Planned Completion Dates:

- ITI GSS ISCM Schedule Updated with CP tasks – December 15, 2023
- FY24 Annual ITI GSS CP Review and Updates (if applicable) – September 15, 2024

The OCC will update the ITI GSS and the financial management system SSP to address the deficiencies specified in the existing System Security Plan POA&Ms (ITIGSS: IPT0021454, IPT0021455, IPT0021452, IPT0021456 and the financial management system: IPT0021274), including documenting interconnections for each system; correcting insufficient implementation statements; and identifying the current system components/subsystems in place.

Planned Completion Date: April 10, 2024

2023-2 Controls for Access Recertification and Audit Logging Reviews should be Strengthened

- There were weaknesses identified in the process for periodically reviewing and recertifying the financial management system end user accounts with default roles and the financial management system database accounts. OCC has a subset of users that access the financial management system infrequently to submit travel and reimbursement requests. These users are provisioned with default roles within the application. OCC has a risk acceptance in place for not disabling the accounts for inactivity; however, the risk acceptance does not cover account recertification controls. Specifically, we noted the following:
  - The financial management system user accounts with Default roles are not recertified semi-annually for end user accounts as required by PSP 310-08-S22, *Account Management Standards* (last updated 6/22/2023).
  - There were two (2) users with financial management system database accounts identified that were not included in the fiscal year 2023 financial management system database access recertification.

- For one (1) out of the three (3) months tested, the SCR Reconciliation Report #12 and the financial management system Summary Report #8 were not reviewed monthly in accordance with the Financial Policies and Procedures (FPP) PBA-016-23, *financial management system – Set up, Maintenance and Audit of the Financial System Application Security*. Specifically, the March 2023 reports were not reviewed until June 1, 2023.

PSP 310-08-S22, *Account Management Standards*, states that:

- *All account types require a semi-annual review for compliance with account management requirements, consistent with the Summary of Account Features by Account Type table in Appendix A…*

- *(b) Non-organizational user accounts for external-facing applications shall not follow the conventional rules of disablement or deletion due to inactivity (stated in section 4.2 above) but shall be locked in accordance with a semi-annual re-certification process. Inactive user accounts shall be disabled/deleted in accordance with system security and privacy plan and as supported by risk assessment…*

- *Collaborating with system owners or their designees to establish a regular review cycle for system access and completion of Privileged Access (X and Service accounts) recertification semi-annually to include disabling and/or deletion of Operating System Authenticated accounts resulting from recertification…*

- *Appendix A: Summary of Account Features by Account Type*

The following table summarizes account characteristics and oversight requirements, by account type:

End user	Standard	Yes	Semiannual	Within 48 hours of reaching 60 days of inactivity	Within 48 hours of reaching 90 days of inactivity	Never expire for PIV
X-Accounts	Privileged	Yes	Semiannual	Within 48 hours of reaching 60 days of inactivity	Within 48 hours of reaching 90 days of inactivity	Never expire for PIV
Cloud Accounts	Standard/ Privileged	NA	Semiannual	NA	NA	NA
Shared	Standard/ Privileged	NA	Semiannual	NA	NA	NA
Service	Standard/ Privileged	NA	Semiannual	NA	NA	NA
Local	Standard/ Privileged	NA	Semiannual	NA	NA	NA
Test Accounts	Standard/ Privileged	NA	Semiannual	Within 48 hours of reaching 60 days of inactivity	Within 48 hours of reaching 90 days of inactivity	NA
Database Logins	Standard/ Privileged	NA	Semiannual	Within 48 hours of reaching 120 days of inactivity	Within 48 hours of reaching 120 days of inactivity	NA

FPP PBA-016-23, *financial management system – Set up, Maintenance and Audit of the Financial System Application Security*, states:

- *Quality Assurance:*
  - *The financial management system Security Administrator performs weekly reviews of employee transfers processed by HR to ensure the financial management system access is updated/removed timely.*
  - *Reviews of the financial management system privilege access and change activity audits to the financial management system Production (OCPFSCPR) database are conducted each month by the financial management system Security Auditor to ensure that security access and system change requests have approvals.*
  - *The financial management system Security Auditor provides evidence of completed audits to the Management Systems & Analytics Manager (MSAM) or a designee monthly.*
  - *The MSAM or designee reviews the financial management system Access audits with the Security Auditor quarterly and signs in acknowledgement that the audits were completed…*

- *Documentation and Records Management:*
  - *Signed documentation of completed monthly audits are uploaded and maintained on the financial management system Financial shared folder.*
  - *Records are retained in accordance with records retention requirements.*

- *The financial management system Security Auditor performs the following audits each month. After the audits are completed, the Auditor signs the audited reports digitally and provides them to the MSAM, and/or designated reviewer who will confirm that the audits were completed by also signing the reports digitally. The Auditor should complete the audits within a reasonable time and save the digitally signed report in the corresponding folder in eDocs.*

- *4. SCR RECONCILIATION REPORT*
  All activity within SCRs that were closed within a month should be documented on one of the monthly security reports, unless the SCR was closed without implementation of a change. All SCRs closed within the last month are reviewed to verify that the change appeared on one of the security reports and that the closed SCR was properly documented or that the SCR was closed without implementation and that this was properly documented.

OCC management indicated that the financial management system users with default accounts are not recertified due to their limited access capabilities and the fact that users disabled at the network level cannot access the system; however, a risk acceptance was not in place for the recertification process and the financial management system Security Plan did not scope the implementation of the control to exclude the financial management system users with default roles from the recertification process.

OCC did not include the two (2) database users in the account recertification because they did not have access to the financial management system database tables and datasets. These users were provisioned with the "Public" role, which limits their access to logging on to the database. The recertification did not include these users due to their level of access. OCC subsequently issued a ticket to remove these accounts.

OCC audit logs were not reviewed monthly due to a lack of adequate backups for when the primary reviewer is out for an extended period of time. As a result, the reviews were not performed until the primary reviewer returns.

Weaknesses in account recertification controls and audit log review controls increases the risk that individuals may have unauthorized access to OCC systems and data, thus putting systems and data at risk of unauthorized disclosure, modification, or destruction of data, possibly without detection.

Recommendation

We recommend that OCC:

- ensure that all financial management system database accounts are included in the semi-annual account recertification process;
- recertify the financial management system users with default accounts semi-annually in accordance with documented policies and procedures. If a decision is made that these accounts should not be recertified, then OCC should document a risk acceptance and identify compensating controls to minimize the residual risk to a level acceptable by management; and
- ensure that backup resources are available to review and approve monthly the financial management system Audits when the primary reviewer is not available.

Management Response

The OCC will complete a Risk Acceptance for the recertification of the financial management system end user accounts with default roles because the financial management system leverages the recertification of network end user accounts. The Risk Acceptance will document compensating controls, e.g., network Personal Identity Verification (PIV) Single Sign On is required to access the financial management system, disabling of inactive network accounts prevents access to the financial management system, etc.

Planned Completion: December 20, 2023

The two referenced database accounts did not have access to the financial management system database tables and datasets and did not require recertification. However, the OCC will update the FPP PBA-016-23, *financial management system – Set up, Maintenance and Audit of the Financial System Application Security* procedures to include the financial management system database accounts in the semi-annually review process to identify and remove unnecessary accounts. The OCC will implement these updates at the next semi-annual review in March 2024.

The OCC will assign a backup reviewer and backup approver for monthly financial management system audits and will update the FPP PBA-016-23, *financial management system – Set up, Maintenance and Audit of the Financial System Application Security* procedures to identify the backup reviewer and backup approver roles. The individuals assigned to these roles will be identified in a supporting audit log review POC list.

Planned Completion: April 30, 2024

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2023

Appendix A – Status of Prior Year Management Letter Comment

Management Letter: 2022-01 – Improper and Untimely Processing of Personnel Actions

FY 2023 Update:
We consider the management letter comment to be closed.

This Page Intentionally Left Blank

REPORT WASTE, FRAUD, AND ABUSE

Submit a complaint regarding Treasury OIG Treasury Programs and Operations using our online form: https://oig.treasury.gov/report-fraud-waste-and-abuse

TREASURY OIG WEBSITE

Access Treasury OIG reports and other information online: https://oig.treasury.gov/