Fiscal Year 2024 Financial Statements Audit Management Letter

OIG-AR-25-02
December 20, 2024

MEMORANDUM

To: Ravi Singh
Acting, Chief Financial Officer

Howard Spira
Senior Vice President and Chief Information Officer

From: Eric Rivera
Assistant Inspector General for Audits ERIC RIVERA Digitally signed by ERIC RIVERA Date: 2024.12.20 14:31:22 -05'00'

Subject: Fiscal Year 2024 Financial Statements Audit Management Letter (Report No. OIG-AR-25-02)

Date: December 20, 2024

This memorandum transmits the subject management letter on the financial statements of the Export-Import Bank of the United States (EXIM) for fiscal years ended September 30, 2024, and 2023. Under a contract monitored by our office, we engaged KPMG LLP, an independent public accounting firm, to perform the audit of EXIM's financial statements.[1] The contract required the audit to be performed in accordance with U.S. generally accepted government auditing standards and the Office of Management and Budget Bulletin No. 24-02, Audit Requirements for Federal Financial Statements.[2]

The attached report contains comments and recommendations relating to internal control deficiencies. The five internal control deficiencies identified by KPMG LLP were not significant and therefore, the deficiencies were not required to be reported in EXIM's independent auditors' report. KPMG LLP's observations and recommendations, and management's responses regarding such matters are presented in the attachment.

KPMG LLP is responsible for the attached management letter dated December 20, 2024, and the conclusions expressed therein. OIG does not express opinions on EXIM's financial statements, internal control, or conclusions on compliance and other matters.

OIG appreciates the cooperation and courtesies provided to KPMG LLP and this office during the audit. If you have questions, please do not hesitate to contact Eric Rivera, Assistant Inspector General for Audits, at (202) 565-3219 or eric.rivera@exim.gov.

---

[1] *Independent Audit of the Export-Import Bank of the United States' Financial Statements as of and for the Fiscal Years Ended 2024, and 2023*

[2] Office of Management and Budget, Audit Requirements for Federal Financial Statements (Bulletin No. 24-02, July 29, 2024).

CONTENTS

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

KPMG Management Letter

December 20, 2024

Office of Inspector General Export-Import Bank of the United States Washington, DC

Office of the Chief Financial Officer Export-Import Bank of the United States Washington, DC

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of Export-Import Bank of the United States (EXIM) as of and for the years ended September 30, 2024 and 2023, 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, and in accordance with Office of Management Budget (OMB) Bulletin No. 24-02, *Audit Requirements for Federal Financial Statements*, as amended, we considered EXIM'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 EXIM's internal control. Accordingly, we do not express an opinion on the effectiveness of EXIM'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 November 15, 2024, on our consideration of EXIM'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 deficiencies in internal control, which are summarized in Exhibit I. EXIM's responses to the findings identified in our audit are also included in Exhibit I. EXIM's responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the responses.

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

FSA-NFR-2024-01 – Timeliness of Recording Guarantee Loan Cancellations

Condition

EXIM's controls over guarantees that were put in to "Cancelled/Paid off" status in (b) (7)(E) were not properly designed to ensure the completeness and accuracy of the total outstanding Working Capital (WC) guarantee exposure balance reported in (b) (7)(E). During the FY 2024 financial statement audit, we noted that EXIM did not identify and record 3 WC class transactions that were cancelled/repaid in (b) (7)(E) in a prior fiscal year.

Criteria

Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* (Green Book) states:

- 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."

Cause

EXIM's management did not fully assess the risk associated with the timely recording of cancelled guarantee loan transactions.

Effect

Control weakness over the timely recording of cancelled guarantee loan transactions resulted in an overstatement of EXIM's outstanding and total guarantee exposure disclosure balance by $3.6 million and $165.6 million respectively as of September 30, 2023.

Recommendation

We recommend that EXIM management:

1. Enhance risk assessment procedures to enable proper identification of processes and controls over Guarantee Loan Cancellations to insure all loans canceled in (b) (7)(E) are completely and accurately recorded in (b) (7)(E).

Management's Response

Management concurred with the factual accuracy of this control deficiency.

FSA-NFR-2024-02 – Inaccurate Subsidy Recordation

Condition

EXIM's controls over the review of the subsidy rate percentages that were inputted into EXIM's (b) (7)(E) were not operating as designed to ensure the accuracy of the subsidy cost recorded to the trial balance. During the FY 2024 financial statement audit we noted that EXIM did not record the correct subsidy obligation amount for a direct loan that was authorized in the current fiscal year.

Criteria

Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (Green Book) states:

- Principle 13.04, Use Quality Information, "Management obtains relevant data from reliable internal and external sources in a timely manner based on the identified information requirements. Relevant data have a logical connection with, or bearing upon, the identified information requirements. Reliable internal and external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent. Management evaluates both internal and external sources of data for reliability. Sources of data can be operational, financial, or compliance related. Management obtains data on a timely basis so that they can be used for effective monitoring."

Cause

An incorrect data file was used in the recordation of the transaction due to multiple versions of the file being in the same folder.

Effect

Control weakness over the accurate review of the subsidy rates within (b) (7)(E) resulted in an overstatement of $600,923.15 to EXIM's Borrowing Authority, and New Obligations and Upward Adjustments.

Recommendation

We recommend that EXIM management:

2. Reinforce controls over the review of the subsidy rates inputted into (b) (7)(E) to address gaps identified in this NFR.

Management's Response

Management concurred with the factual accuracy of this control deficiency.

FSA-NFR-2024-03 – Timeliness of Recording Insurance Transactions

Condition

EXIM's controls over the timely cancellation of insurance amounts outstanding or undisbursed were not properly designed to ensure the completeness and accuracy of the total outstanding insurance exposure balance reporting in EXIM's (b) (7)(E) .

Criteria

Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (Green Book) states:

- Principle 07.08, Identify, Analyze, and Respond to Risk, "Management designs responses to the analyzed risks so that risks are within the defined risk tolerance for the defined objective. Management designs overall risk responses for the analyzed risks based on the significance of the risk and defined risk tolerance.
- 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."

Cause

EXIM's management did not identify the risks associated with the code within (b) (7)(E) that is responsible for recording the cancellation of insurance amounts outstanding or undisbursed. Moreover, EXIM did not have specific policies in place for monitoring insurance policies that have passed maturity with outstanding or undisbursed exposure.

Effect

Control weakness over the timely recording of cancelled insurance resulted in an overstatement of EXIM's outstanding and total insurance exposure disclosure balances by $3.5 million and $6.7 million, respectively, as of September 30, 2023. This also resulted in an overstatement of EXIM's outstanding and total insurance exposure disclosure balance by $8.2 million respectively as of June 30, 2024. The identified insurance issues were adjusted for in the re-estimate calculation, as of August 31, 2024, and corrected in the portfolio as of September 30, 2024.

Recommendation

We recommend that EXIM management:

3. Enhance processes and controls over insurance cancellations to ensure all transactions are recorded by (b) (7)(E) and are completely and accurately recorded in (b) (7)(E) .

Management's Response

Management concurred with the factual accuracy of this control deficiency.

FSA-NFR-2024-04 Insufficient Password Configurations – (b) (7)(E)

Condition

Exim management did not sufficiently design and implement (b) (7)(E) password configurations. Specifically, the limits for the following password configurations were not designed and documented:

- (b) (7)(E) limit was not defined and documented for the (b) (7)(E) profile types
- (b) (7)(E) limit was not defined and documented for the (b) (7)(E) profile types
- (b) (7)(E) limit was not defined and documented for the (b) (7)(E) profile types
- (b) (7)(E) limit was not defined and documented for the (b) (7)(E) profile types
- (b) (7)(E) limit was not defined and documented for the (b) (7)(E) profile types
- (b) (7)(E) limit was not defined and documented for the (b) (7)(E) profile types

Additionally, the limits for the following password configurations were not implemented in accordance with policies and procedures:

- (b) (7)(E) was not properly implemented for the (b) (7)(E) profile types.
- (b) (7)(E) was not properly implemented for the (b) (7)(E) profile type.
- (b) (7)(E) was not properly implemented for the (b) (7)(E) profile type.
- (b) (7)(E) was not properly implemented for the (b) (7)(E) profile types.
- (b) (7)(E) was not properly implemented for the (b) (7)(E) profile types.

Criteria

United States Government Accountability Office, Standards for Internal Control in the Federal Government (the Green Book), Principle 11 Design Activities for the Information System states:

- 11.11 Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system.

The Green Book, Principle 16 Perform Monitoring Activities states:

- 16.05 Management performs ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions. Ongoing monitoring may include automated tools, which can increase objectivity and efficiency by electronically compiling evaluations of controls and transactions.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5.1, Release 5.1.1, states:

IA-5: Authenticator Management

Control: Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

(b) (7)(E) , states:

a. (b) (7)(E)

Cause

EXIM management did not have sufficient monitoring controls in place to help ensure that password configurations for the (b) (7)(E) servers adhered to the Standard Operating Procedures (b) (7)(E) and NIST SP 800-53, Revision 5.1, Release 5.1.1.

Effect

Without proper password requirements configured within the (b) (7)(E), the risk exists that unauthorized individuals may gain access to the (b) (7)(E); thus adversely impacting the integrity of the (b) (7)(E) and its data.

Recommendation

We recommend that EXIM management:

4. We recommend that EXIM management design and implement monitoring controls to help ensure that password configurations for the (b) (7)(E) are in compliance with the Standard Operating Procedures for (b) (7)(E) Procedures and NIST SP 800-53, Revision 5.1, Release 5.1.1.

Management's Response

Management concurred with the factual accuracy of this control deficiency.

FSA-NFR-2024-05 Incompatible Access Combination to Develop and Implement Changes – (b) (7)(E)

Condition

One individual was granted an incompatible combination of accesses, which could allow the individual to develop and implement changes into the (b) (7)(E) production environment without following the required testing and approval processes.

Criteria

United States Government Accountability Office, Standards for Internal Control in the Federal Government (the Green Book), Principle 10 Design Control Activities Section Segregation of duties states:

- 10.03 Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event.

The Green Book, Principle 16 Perform Monitoring Activities states:

- 16.05 Management performs ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions. Ongoing monitoring may include automated tools, which can increase objectivity and efficiency by electronically compiling evaluations of controls and transactions.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5.1, Release 5.1.1, states:

> CM-5: Access Restrictions for Change:
> Control: Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system

AC-5: Separation of Duties:
Control: a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and
b. Define system access authorizations to support separation of duties.

(b) (7)(E), states:
"Users with only developer roles should not perform any configuration changes to production environments.

Cause

The condition was caused due to error and oversight by the individuals responsible for granting and monitoring user access to the development and production environments.

Effect

Without proper logical access restrictions between the development and production environments the risk increases that untested and/or unauthorized changes are implemented into the (b) (7)(E) production environment, which could adversely impact the integrity of the (b) (7)(E) and its data.

Recommendation

We recommend that EXIM management:

5. We recommend that EXIM management design and implement monitoring controls to help ensure that access to develop and implement changes into production is appropriately segregated.

Management's Response

Management concurred with the factual accuracy of this control deficiency.

Office of Inspector General
Export-Import Bank of the United States

811 Vermont Avenue, NW
Washington, DC 20571

Telephone 202-565-3908
Facsimile 202-565-3988

HELP FIGHT

FRAUD, WASTE, AND ABUSE

1- 888-OIG-EXIM
(1-888-644-3946)

https://eximoig.oversight.gov/contact-us

https://eximoig.oversight.gov/hotline

If you fear reprisal, contact EXIM OIG's Whistleblower Protection Coordinator at oig.whistleblower@exim.gov

For additional resources and information about whistleblower protections and unlawful retaliation, please visit the whistleblower's resource page at oversight.gov.