EXPORT-IMPORT BANK OF THE UNITED STATES

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

Fiscal Year 2020 Financial Statements Audit Management Letter

November 13, 2020
OIG-AR-21-02

Information about specific vulnerabilities in IT systems has been redacted from the publicly released version of this report. The information withheld was compiled in connection with OIG law enforcement responsibilities and consists of information that, if released publicly, could lead to the circumvention of the law.

To: Mary Jean Buhler, Chief Financial Officer

Howard Spira, Senior Vice President and Chief Information Officer

From: Jennifer Fain
Acting Inspector General

Subject: Fiscal Year 2020 Financial Statements Audit Management Letter (OIG-AR-21-02)

Date: November 13, 2020

This memorandum transmits KPMG LLP's management letter on the Export-Import Bank of the United States' (EXIM) financial statements for fiscal years ended September 30, 2020 and 2019. Under a contract monitored by this office, we engaged the independent public accounting firm of KPMG to perform an audit of EXIM's financial statements. 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. 19-03, *Audit Requirements for Federal Financial Statements.*

This report contains comments and recommendations relating to internal control deficiencies and other matters. KPMG identified eight deficiencies in EXIM's internal control over financial reporting. The internal control deficiencies noted in this report were not significant and therefore, the deficiencies were not required to be reported in EXIM's independent audit report. KPMG'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 November 13, 2020, and the conclusions expressed therein. We do not express opinions on EXIM's financial statements or internal control, or conclusions on compliance and other matters.

We appreciate the cooperation and courtesies provided to KPMG LLP and this office during the audit. If you have questions, please contact me at (202) 565-3439 or jennifer.fain@exim.gov. or Courtney Potter at (202) 565-3976 or courtney.potter@exim.gov. You can obtain additional information about the EXIM OIG and the Inspector General Act of 1978 at www.exim.gov/about/oig.

Attachment

cc: Kimberly A. Reid, President and Chairman
Ryan McCormack, Senior Vice President and Chief of Staff
Adam Martinez, Chief Management Officer
Lauren Fuller, Senior Advisor to the President and Chairman
Stephen Renna, Chief Banking Officer
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
David Slade, Senior Vice President and General Counsel
David Sena, Senior Vice President of Board Authorized Financed
Inci Tonguch-Murray, Senior Vice President and Deputy Chief Financial Officer
Patricia Wolf, Vice President and Controller
Nathalie Herman, Vice President and Treasurer
Maria Fleetwood, Vice President of Acquisition and Business Services
Cristopolis Dieguez, Director, Internal Controls and Compliance
James P Hauer III, Partner, KPMG LLP
Courtney Potter, Deputy AIG for Audits and Evaluations, OIG
Amanda Myers, Senior Counsel, OIG

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

November 13, 2020

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, 2020 and 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, and in accordance with Office of Management Budget (OMB) Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements*, 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 13, 2020 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

EXIM-FISMA-2020-02 – Weakness in Information Security Continuous Monitoring (ISCM)

Condition

In fiscal year (FY) 2019, we reported that EXIM has implemented (b) (4) their chosen DHS CDM (Department of Homeland Security's Continuous Diagnostics and Mitigation) SIEM (Security Information and Event Management) tool, however; for the reporting period, the tool was not configured to log and report activity across EXIM's information systems, in such a manner that the software alerts or reports activity that is deemed unusual or suspicious. Additionally, for the full reporting period, EXIM had not staffed its continuous monitoring program to help with the configuration of the SIEM.

FY 2020 Status

EXIM has implemented and configured (b) (4) to log activity across servers and applications across the network and has staffed the continuous monitoring program to help with the configuration of (b) (4) is a commercial software platform to search, analyze, and visualize system generated data gathered from servers, applications, and networked devices across the EXIM's computing environment.

EXIM has not fully implemented policies and procedures for the monitoring and independent review of logged activity.

Criteria

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137 Revision 1, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, Section 2.3 which requires:

> Consideration is given to ISCM tools that:
>
> - Pull information from a variety of sources;
> - Use open specifications such as the Security Content Automation Protocol (SCAP);
> - Offer interoperability with other products such as help desk, inventory management, configuration management, and incident response solutions;
> - Support compliance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidelines;
> - Provide reporting with the ability to tailor output and drill down from high-level, aggregate metrics to system-level metrics; and
> - Allow for data consolidation into SIEM tools and dashboard products.

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control AU-6, Audit Review, Analysis, and Reporting which requires:

The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Audit review, analysis, and reporting covers information.

Cause

During FY 2020, EXIM successfully implemented and configured (b) (4) however, has not completed activities associated with audit log monitoring and review.

Effect

Without the full implementation of EXIM's SIEM solution, the agency's ability to identify and mitigate the impact of emerging cybersecurity threats on an automated, continuous, and comprehensive basis may be impacted.

Recommendation

We recommend that EXIM management:

1. Define audit review, analysis and reporting policies and procedures for the (b) (4) and the independent review of logged activity on a periodic basis (performed by one who is knowledgeable but not performing the activity).

2. Implement the defined audit review, analysis, and reporting policies and procedures for the (b) (4) and ensure operational effectiveness and compliance.

Management's Response

Management concurs with the Notification of Finding and Recommendation (NFR) and will develop a corrective action plan, with milestone dates, to address the condition.

IT-NFR-2020-01 – Entity Wide (b) (4) Issue

Condition

EXIM management has not designed and implemented a consistent process and controls for (b) (4) in accordance with its' approved policies.

Specifically, during our testing and review, we noted the following:

1. Required approvals were not received and documented, (b) (4)

2. Documentation to evidence (b) (4) was lacking (b) (4)

Criteria

NIST SP 800-53 Revision 4, Security Controls and Assessment Procedures for Federal Information Systems and Organizations, control CM-3 states:

> The organization:
>
> [...]
> b) Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
> c) Documents configuration change decisions associated with the information system;

[...]
g) Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

Export Import Bank of the United States, (b) (4) states:

(b) (4)

Export Import Bank of the United States, (b) (4) states:

(b) (4)

Cause

In the current year, EXIM management implemented revised policies and procedures to (b) (4) however, the documented policies and procedures were not updated to reflect the change.

Effect

Lack of documented review and approval for (b) (4) increases the risk that (b) (4)

, increasing the risk to the (b) (4)

Recommendation

We recommend that EXIM management:

3. Align its process for (b) (4) to its approved (b) (4) policies to ensure they are congruent.
4. Perform and document (b) (4) and maintain audit evidence supporting (b) (4)

Management's Response

Management concurs with the factual accuracy of all NFR conditions.

IT-NFR-2020-02 – (b) (4) **Issue**

Condition

Controls over the remediation of identified vulnerabilities were not operating effectively during the period. Specifically, (b) (4) In addition, the identified vulnerabilities were not appropriately tracked (b) (4)

Criteria

NIST SP 800-53 Revision 4, Security Controls and Assessment Procedures for Federal Information Systems and Organizations, control RA-5 states:

> The organization:
>
> [...]
> c. Analyzes vulnerability scan reports and results from security control assessments;
> d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk.

NIST SP 800-53 Revision 4, Security Controls and Assessment Procedures for Federal Information Systems and Organizations, control CA-5 states:

> The organization:
>
> a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
> b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Export Import Bank of the United States, (b) (4) states:

(b) (4)

(b) (4)

Export Import Bank of the United States, (b) (4)
states:

(b) (4)

(b) (4)

Cause

EXIM management did not (b) (4) to allow for appropriate tracking and to ensure the vulnerabilities were remediated.

Effect

Without effective controls in place to remediate (b) (4) vulnerabilities that have been identified, or a documented plan of action to address the required mitigations, there is an increased risk that the vulnerability is exploited by intruders and attackers trying to gain access to the information system, which could potentially compromise of the confidentiality, integrity, and availability of the data residing on the information system.

Recommendation

We recommend that EXIM management:

5. Ensure that all identified vulnerabilities are appropriately remediated per EXIM's policies.

6. Formally document and track all identified vulnerabilities that will not be mitigated in accordance with (b) (4)

Management's Response

Management concurs with the factual accuracy of all NFR conditions.

IT-NFR-2020-03 – (b) (4) Users Recertification Issue

Condition

Controls over the periodic recertification of (b) (4) were not implemented effectively during the period. Specifically, (b) (4)

and the recertification for (b) (4) was not formally documented/evidenced.

Criteria

Export Import Bank of the United States, (b) (4) states:

(b) (4)

NIST SP 800-53 Revision 4, Security Controls and Assessment Procedures for Federal Information Systems and Organization, control AC-2 Account Management states:

> Control: The organization:
> j. Reviews accounts for compliance with account management requirements *[Assignment: organization-defined frequency]*

Cause

EXIM management assigned the annual recertification review of (b) (4) to (b) (4) As a result, the annual recertification of (b) (4) was not completed within the fiscal year as required. (b) (4)

management did not follow policies and procedures to formally document and retain evidence of the completed reviews.

Effect

The lack of a documented review and/or an effective review control in place for the recertification of (b) (4) there is an increased risk that unauthorized, or inappropriate activity could be performed without being timely detected. Such unauthorized activity could lead to a compromise in data confidentiality, integrity, and availability.

Recommendation

We recommend that EXIM management:

7. Enforce EXIM's existing policies and procedures regarding access control management related to recertification and formally document the performance of the timely review.

Management's Response

Management concurs with the factual accuracy of all NFR conditions.

FSA-NFR-2020-01 Subsidy Re-estimate Source Data (b) (4) Review

Condition

Controls are not properly designed and implemented to ensure the accuracy of the data inputs within (b) (4) Specifically, during our testing of (b) (4) we identified that the end of year cash balances, by cohort, for the insurance program, were incorrect.

Criteria

Government Accountability Office (GAO) Standards for Internal Control in the Federal Government 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."

- Principle 10.04, *Design Control Activities,* "Control activities can be either preventive or detective. The main difference between preventive and detective control activities is the timing of a control activity within an entity's operations. A preventive control activity prevents an entity from failing to achieve an objective or address a risk. A detective control activity discovers when an entity is not achieving an objective or addressing a risk before the entity's operation has concluded and corrects the actions so that the entity achieves the objective or addresses the risk."

FASAB Technical Release 6, Preparing Estimates for Direct Loan and Loan Guarantee Subsidies under the Federal Credit Reform Act -Amendments to Technical Release No. 3 Preparing and Auditing Direct Loan and Loan Guarantee Subsidies under the Federal Credit Reform Act, states the following:

- Paragraph 17, "Agencies must accumulate sufficient relevant and reliable data on which to base cash flow projections. It is important to note that agencies should prepare all estimates and re-estimates based upon the best available data at the time the estimates are made. Agencies should prepare and report re-estimates of the credit subsidies, in accordance with SFFAS No. 2, 18, and 19, to reflect the most recent data available as discussed in the re-estimate section of this technical release.

- Paragraph 35, "In addition, the data used as input or generated as output should also be safeguarded and reviewed for errors."

Cause

Review controls were not designed, at the appropriate level of precision, to prevent and/or detect data input errors within (b) (4)

Effect

Ineffective control activities resulted in an overstatement of the upward re-estimate by $37.5 million and an overstatement of the downward re-estimate by $38.9 million as of September 30, 2020. This misstatement was corrected by management prior to the issuance of this letter.

Recommendation

We recommend that EXIM management:

8. Enhance the precision of the review control over the (b) (4) of the re-estimate model to ensure all relevant data is input accurately.

Management's Response

Management concurs with the factual accuracy of all NFR conditions.

Office of Inspector General
Export-Import Bank *of the* United States
811 Vermont Avenue, NW
Washington, DC 20571
202-565-3908
www.exim.gov/about/oig