OFFICE OF INSPECTOR GENERAL
EXPORT-IMPORT BANK
of the **UNITED STATES**

Fiscal Year 2015 Financial Statement Audit - Management Letter

February 12, 2016
OIG-AR-16-03

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: David Sena, Senior Vice President and Chief Financial Officer
Howard Spira, Chief Information Officer

From: Terry Settle
Assistant Inspector General for Audits

Subject: Fiscal Year 2015 Financial Statement Audit - Management Letter OIG-AR-16-03

Date: February 12, 2016

This memorandum transmits Deloitte and Touche LLP's Management Letter related to the audit of the Export-Import Bank of the United States' (Ex-Im Bank) financial statements for the fiscal year ended 2015. Under a contract monitored by this office, we engaged the independent public accounting firm of Deloitte and Touche LLP to perform the audit. The contract required the audit to be performed in accordance with United States generally accepted government auditing standards and Office of Management and Budget Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*.

The Management Letter contains comments and recommendations related to internal control deficiencies and other matters. Deloitte and Touche LLP identified nine deficiencies in Ex-Im Bank's internal control over financial reporting. The nine internal control deficiencies noted in this report were not significant and therefore, the deficiencies were not required to be reported in the Ex-Im Bank's independent audit report. Deloitte and Touche LLP's observations and recommendations, and management's responses regarding such matters are presented in the Attachment.

Deloitte and Touche, LLP is responsible for the attached management letter dated December 29, 2015 and the conclusions expressed in the letter. We do not express opinions on Ex-Im Bank's financial statements, internal control, or conclusions on compliance with laws and regulations.

We appreciate the cooperation and courtesies provided to Deloitte and Touche LLP and this office during the audit. If you have questions, please contact Terry Settle, (202) 565-3498 or Terry.Settle@exim.gov. You can obtain additional information about the Export-Import Bank Office of Inspector General and the Inspector General Act of 1978 at www.exim.gov/oig.

cc: Fred P. Hochberg, Chairman and President
C.J. Hall, Executive Vice President
Angela Freyre, General Counsel
Audit Committee
Nathalie Herman, Treasurer, Office of the Chief Financial Officer
Patricia Wolf, Controller, Office of the Chief Financial Office
John Lowry, Director, Information Technology Security and Systems Assurance
Inci Tonguch-Murray, Deputy Chief Financial Officer
Duncan Barks, Partner, Deloitte and Touche LLP

Deloitte & Touche LLP
7900 Tysons One Place
Suite 800
McLean, VA 22102-5971
USA

Tel: +1 703 251 1000
www.deloitte.com

December 29, 2015

Mr. Michael McCarthy, Inspector General
Export-Import Bank of the United States
811 Vermont Avenue NW
Washington, D.C. 20571

Dear Mr. McCarthy:

We have performed an audit of the financial statements of the Export-Import Bank of the United States ("Ex-Im Bank" or the "Bank") as of and for the year ended September 30, 2015 (the "financial statements"), in accordance with auditing standards generally accepted in the United States of America, the standards applicable to the financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and Office of Management and Budget Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements* (collectively, "generally accepted auditing standards") and have issued our report thereon dated November 12, 2015.

We have prepared the following comments to assist you in fulfilling your obligation to oversee the financial reporting and disclosure process for which management of Ex-Im Bank is responsible. These matters were communicated orally to Ms. Terry Settle, assistant inspector general, on November 12, 2015.

This report is intended solely for the information and use of the Office of Inspector General ("OIG"), management, and others within the organization and is not intended to be and should not be used by anyone other than these specified parties.

Yours truly,

Deloitte & Touche LLP

cc: The management of Export-Import Bank of the United States

Our Responsibility under Generally Accepted Auditing Standards

Our responsibility under generally accepted auditing standards has been described in our engagement letter dated July 10, 2015. As described in that letter, the objective of a financial statement audit conducted in accordance with generally accepted auditing standards is to express an opinion on the fairness of the presentation of Ex-Im Bank's financial statements as of and for the year ended September 30, 2015, in conformity with accounting principles generally accepted in the United States of America ("generally accepted accounting principles"), in all material respects. Our responsibilities under generally accepted auditing standards include forming and expressing an opinion about whether the financial statements that have been prepared by management with the oversight of the OIG are presented fairly, in all material respects, in conformity with generally accepted accounting principles. The audit of the financial statements does not relieve management or OIG of its responsibilities.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on our judgment, including the assessment of the risks of material misstatement of the financial statements, whether caused by fraud or error. In making those risk assessments, we considered internal control over financial reporting relevant to Ex-Im Bank's preparation and fair presentation of the financial statements in order to design audit procedures that were appropriate in the circumstances but not for the purpose of expressing an opinion on the effectiveness of Ex-Im Bank's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of Ex-Im Bank's internal control over financial reporting. Our consideration of internal control over financial reporting was not designed to identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses.

Significant Accounting Policies

Ex-Im Bank's significant accounting policies are set forth in Note 1 to Ex-Im Bank's 2015 financial statements. We are not aware of any significant changes in previously adopted accounting policies or their application during the year ended September 30, 2015.

We have evaluated the significant qualitative aspects of Ex-Im Bank's accounting practices, including accounting policies, accounting estimates and financial statement disclosures and concluded that the policies are appropriate, adequately disclosed, and consistently applied by management.

Accounting Estimates

Accounting estimates are an integral part of the financial statements prepared by management and are based on management's current judgments. Those judgments are ordinarily based on knowledge and experience about past and current events and on assumptions about future events. Significant accounting estimates reflected in Ex-Im Bank's 2015 financial statements include the allowances for losses on loans receivable, subrogated claims receivable, guarantees, and insurance. The allowances for losses reduce the recorded balances to their estimated net present value. The allowances are established through a provision charged to earnings. These estimates for losses are based upon collectability of individual credits and their related cash flow forecasts, historical and current market loss experience, adverse situations that may affect the borrower's ability to repay, estimated value of any underlying collateral, expected defaults, fees and recoveries, and prevailing world-wide economic and political conditions. Therefore, the value used to determine the allowances for losses are subject to the reasonableness of these estimates. Although management believes the estimates underlying the calculation of allowances for losses reflected in Ex-Im Bank's 2014 financial statements are reasonable, there can be no assurances that Ex-Im Bank could ultimately realize these values. The basis for our conclusions as to the reasonableness of these estimates when considered in the context of the financial statements taken as a whole, as expressed in our auditors' report on the financial statements, is our understanding and testing of the process used by management to develop the estimates.

Uncorrected Misstatements

Our audit of the financial statements was designed to obtain reasonable, rather than absolute, assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. There were no uncorrected misstatements or disclosure items passed identified during our audit.

Material Corrected Misstatements

Our audit of the financial statements was designed to obtain reasonable, rather than absolute, assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. There were no material misstatements that were brought to the attention of management as a result of our audit procedures.

Disagreements with Management

We have not had any disagreements with management related to matters that are material to Ex-Im Bank's 2015 financial statements.

Our Views about Significant Matters that were the Subject of Consultation with Other Accountants

We are not aware of any consultations that management may have had with other accountants about auditing and accounting matters during 2015.

Significant Findings or Issues Discussed, or Subject of Correspondence, with Management prior to Our Initial Engagement or Retention

Throughout the year, routine discussions were held, or were the subject of correspondence, with management regarding the application of accounting principles or auditing standards in connection with transactions that have occurred, transactions that are contemplated, or reassessment of current circumstances. In our judgment, such discussions or correspondence were not held in connection with our retention as auditors.

Other Significant Findings or Issues Arising from the Audit Discussed, or Subject of Correspondence, with Management

Throughout the year, routine discussions were held, or were the subject of correspondence, with management. In our judgment, such discussions or correspondence did not involve significant findings or issues requiring communication to the OIG.

Significant Difficulties Encountered in Performing the Audit

In our judgment, we received the full cooperation of Ex-Im Bank's management and staff and had unrestricted access to Ex-Im Bank's senior management in the performance of our audit.

Management's Representations

We have made specific inquiries of Ex-Im Bank's management about the representations embodied in the financial statements. In addition, we have requested that management provide to us the written representations Ex-Im Bank is required to provide to its independent auditors under generally accepted auditing standards. We have attached to this letter, as Appendix B, a copy of the representation letter we obtained from management.

Emphasis-of-Matter Paragraphs and Other-Matter

Emphasis-of-Matter Paragraphs

As discussed in Note 1 to the financial statements, the Export-Import Bank Reauthorization Act of 2012 (P.L.112-122) extended the Bank's authority until September 30, 2014. This date was subsequently extended to June 30, 2015, by Public Law 113-164 on September 19, 2014. The administration has requested a five-year extension of the Bank's full authority under its charter through FY2019; however, as of September 30, 2015, such authority had not been extended. During a period of a lapse in full authority, the Bank could not authorize new financing transactions. Under the terms of its charter, the Bank would continue to manage and service existing loans, guarantees, and insurance policies and engage in other permitted functions and activities.

In light of the various bills introduced in the Senate and the House of Representatives to reauthorize the Bank as of the date of our report issuance, as well as votes and other actions taken in both houses of Congress in support thereof, management believed that the Bank would be reauthorized. Ex-Im Bank was reauthorized by Congress on December 4, 2015. The reauthorization is in effect until September 30, 2019.

Control-Related Matters

We have identified, and included in Appendix A, other deficiencies involving Ex-Im Bank's internal control over financial reporting as of September 30, 2015, that we wish to bring to your attention.

The definitions of a deficiency, a material weakness, and a significant deficiency are also set forth in Appendix A.

Although we have included management's written response to our comments in Appendix A, such responses have not been subjected to the auditing procedures applied in our 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 actions described therein.

* * * * * *

- Appendix A: Matters Related to Internal Control over Financial Reporting
- Appendix B: Representations from Management

APPENDIX A

DEFICIENCIES

We identified the following deficiencies involving Ex-Im Bank's internal control over financial reporting as of September 30, 2015, that we wish to bring to your attention:

2015-001 EXIM Online ("EOL") Change Management

Condition—During our testing of EOL change management, the following deficiencies were noted

- The EOL change management process was not documented at the level of precision such that it can be consistently executed,

- Regarding EOL centralized change management documentation:

    a. Evidence of user acceptance testing ("UAT") testing is not centrally maintained or readily available upon request and the status of each change migrated to production in FY2015 was not updated appropriately to reflect the completion of required steps in the change management process, including UAT testing and approval, and

    b. The initial population of EOL changes did not contain any changes in the "Production" status. Once we brought this to management's attention, the status of the changes was updated retroactively to indicate the current status of the change, including the indication of completed required steps in the process, and

- For two of 25 selected changes of a total population of 88 enhancements and defects, evidence of UAT testing performed prior to the change was not available. However, validation of these changes was performed as part of remediation. Additionally, management confirmed for any of the total 88 changes where they could not find the evidence of UAT testing they performed the testing and noted no exceptions. Therefore, there is no actual impact on the financial statements due to this deficiency.

Criteria—Below are criteria for our consideration according to the Federal Information System Controls Audit Manual ("FISCAM"):

- Change management policies and procedures are designed to reasonably assure that changes to application functionality in production are authorized and appropriate and unauthorized changes are detected and reported promptly. The policies are designed such that they provide a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process, are sufficiently documented to provide guidance to staff with varying levels of skill and experience; provide a means of controlling changes in requirements that occur over the system life; and include documentation requirements,

- Authorizations for changes are documented and maintained. Change request forms are used to document requests and related projects and change requests must be approved by both system users and IT staff, and

- Application changes are appropriately approved and tested before being moved into the production environment and management reviews the changes on a regular basis to ascertain that they are appropriate and approved by management.

Cause—The root cause of deficiencies are due to the followings:

- The current application "Change Management Process Guide" includes high-level required steps to be performed, but does not include sufficient detail regarding the criteria for each required step to be met and does not specify the requirements for formal management review and approval prior to the next required step, including production migration. Through creation and periodic review of the process documentation, management has accepted a high-level policy and has not required a detailed policy,

- Documentation was not maintained for each required step in the change management process and the status of the changes was not updated to reflect that each step was completed, including UAT testing results and approvals. If steps were performed, the documentation was not appropriately associated with the change or included with the change for appropriate review and authorization. The current change management process does not specifically require that the documentation is maintained and associated with the change and the final check/management review for production migration approval does not require documentation to be centralized and readily available for review, and

- Consistent documentation is not maintained centrally and the ticketing system was not updated appropriately throughout the change management process. The approvals are based on first-hand knowledge or dependence on others and not based on review of evidence.

Effect or Potential Effect:

- As the process documentation does not clearly specify criteria required for each change, there is not a standardized approach, which leads to a process with an increased risk of errors which may not be detected,

- If change management documentation is not centralized, posted to the associated (b) (4) t ticket and readily available for review, it precludes detailed management review of each request prior to migration to the production environment. Additionally, as the ticketing system is not updated appropriately throughout the change management process, the approvals are not based on review of status and evidence, and

- As the final approval of changes to move to production does not include a detailed review of each step and the associated documentation for the required steps, there is a risk that inappropriate/unauthorized changes, or changes that have not fully followed the process, are migrated into production.

Recommendation—We recommend that Ex-Im Bank perform the following measures:

- Ex-Im Bank updates its change management policy and procedure to reflect the specific requirements for each change and the required documentation of the final review and approval prior to production migration.

- Documentation for each change migrated to production is maintained and associated with the change in the ticketing system for verification and approval. Additionally, we recommend that each change is updated to reflect the current status of the change.

- Ex-Im Bank implements a formal control to document the review and approval that each required step in the change management process is followed prior to implementation into production, including a review of documentation to show that each step was followed.

Ex-Im Bank's Response to Finding—Management agrees with the recommendation. Management will review and update the current Change Control policy and procedure documents to ensure they have the specificity required to ensure auditability and clear standards for what is compliant. Management is also implementing a new change control repository and work flow system which will ensure that artifacts required for the process are in place in order to move the workflow forward. This will be completed by May 1, 2016.

2015-002 Firewall/IPS System Change Management Process Documentation

Condition—D&T noted that for three out of five sample selections for the patches applied to the firewall/IPS system, there was no evidence documenting the testing and approval of the patches before they were migrated into production.

Criteria—According to FISCAM, change management policies and procedures are designed to reasonably assure that changes to application functionality in production are authorized and appropriate and unauthorized changes are detected and reported promptly. The policies are designed such that they provide a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process; are sufficiently documented to provide guidance to staff with varying levels of skill and experience; provide a means of controlling changes in requirements that occur over the system life; and include documentation requirements.

Cause—The root cause of the patches not having supporting evidence for testing and approval is that the changes were implemented during a period where the Network and Systems Engineering office was in transition as the primary tester and primary approver were leaving the agency. Therefore, for the period between the departure of the primary tester and approver of patches, the patching process was not executed as designed until a new primary tester and approver were identified.

Effect or Potential Effect—If testing and approval documentation is not maintained for changes migrated into production, there is a risk that inappropriate changes are made to application systems or programs that contain relevant automated controls (i.e., configurable settings, automated algorithms, automated calculations, and automated data extraction) and/or report logic.

Recommendation—We recommend that Ex-Im Bank document the change management process for firewall/IPS system patches at the level of precision such that it can be consistently executed, including a description of the users who will take over the process should the current tester and approver be unable to perform their duties.

Ex-Im Bank's Response to Finding—Management agrees with this recommendation. While we are assured that the security posture of the Bank's primary firewall and intrusion protection system (IPS) was maintained throughout this time, we agree that there were adverse impacts as a consequence of staff turnover on change management associated with this critical device. In recognition of this, we will (a) develop specific change management procedures for the Bank's firewall/IPS and (b) define and assign roles and responsibilities for change management of the Bank's firewall/IPS assets. This effort will be completed by May 1, 2016.

2015-003 Privileged Level Access

Condition—During our testing of privileged level access security, the following deficiencies were noted:

- Active user and system accounts with inappropriate access privileges no longer required for assigned job responsibilities and/or system functionality, and

- Separated employee with an active account.

Criteria—According to FISCAM, access to sensitive/privileged accounts is restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose. Use of sensitive/privileged accounts is adequately monitored

Cause—In all cases, oversight on behalf of the administrator with access removal responsibilities contributed to privileged users maintaining access no longer required, either as a result of separation or change in job function.

Effect or Potential Effect—If users have access privileges beyond those necessary to perform their assigned duties, this may create improper segregation of duties or allow users to materially affect data and financial information.

Recommendation—We recommend that Ex-Im Bank follow their current access deprovisioning process but enhance the process by including each system administrator on separation notifications and use the notification to check the systems they are responsible for to determine if user access rights need to be changed. Finally, Ex-Im Bank should consider increasing the frequency of the current Annual Access Review to ensure all user and system/service account access privileges are based on assigned job responsibilities and/or required system functionality. An annual review may not be frequent enough to catch inappropriate access in a timely manner. Additionally, we recommend that Ex-Im Bank enhance the current review process to document and review certain privileged access levels to ensure all user and system/service account access privileges are based on assigned job responsibilities and/or required system functionality.

Ex-Im Bank's Response to Finding—Management agrees with this recommendation. As part of the Bank's ongoing response to the OMB mandated '30-day sprint', Ex-Im Bank IT staff have undertaken a comprehensive effort to identify, manage and track all privileged user accounts within the Bank (whether on premises or in the cloud). This program includes a requirement for all privileged users to use a specific token credential employing two-factor authentication for all privileged network device and server access (beyond the use of a PIV for two-factor authentication to the network). As part of this effort, we are developing policy and procedures for privileged user and account management, including privileged user rules of behavior that go beyond the basic rules of behavior for all non-privileged user accesses in recognition of the additional responsibilities that privileged users carry. This policy also requires a quarterly review process for all existing privileged user accounts and permissions for recertification by the Bank's IT Managers. We already have a wide distribution of employee and contractor termination notices within the IT staff; however, we will review the distribution to determine if all system administrators are covered by the distribution. This effort will be completed by April 1, 2016.

2015-004 User Provisioning

Condition—During the initial testing period of October 1, 2014, to March 10, 2015, we noted that 25 of our sample of 35 users did not adhere to the provisioning process:

- Access request and approval documentation was not available for 21 out of 35 sampled new users granted access to the Financial Management System - Next Generation ("FMS-NG") application and

- Approval evidence for access request was not available for an additional four of the 35 sampled new users granted access to the FMS-NG application.

Access for each of these users was required based on assigned job responsibilities, and based on additional testing performed during the final audit period, user provisioning (request and approval) processes were followed (i.e., control was operating effectively as of year-end).

Criteria—According to FISCAM, resource owners have identified authorized users and the access they are authorized to have. Access is limited to individuals with a valid business purpose (least privilege).

Cause—The FMS-NG system was commissioned October 1, 2014 (the start of the audit period) and the client had not yet created a routine process for determining how users should gain access to the system. An overall approach for converting user access from legacy systems to the new system was not documented.

Effect or Potential Effect—If users do not have documented approval of access to systems prior to being granted access, users could be granted inappropriate roles or privileges that are not required for the user's job responsibilities.

Recommendation—We recommend Ex-Im Bank consider including a user access conversion strategy with activities, such as:

- Document a plan for converting user access from the legacy system to the new system;
- Document a mapping of roles within the legacy system and corresponding role within the new system, if applicable;
- Create a complete list of users who need access to the new system and the level of access required; and
- Obtain final approval from key stakeholders that the identified users should be granted the corresponding access in the new system.

Ex-Im Bank's Response to Finding—Management agrees with the observations that underlie this recommendation. Management notes this was a one-time issue related to the complex migration to our new financial system in October 2014. All historical user provisioning noted under this deficiency have been remediated and all current system access grants follow our user provisioning process. Management will ensure this is an important lesson learned to be applied to any future project with similar characteristics.

2015-005 User Deprovisioning

Condition—During our testing of user deprovisioning, the following deficiencies were noted

- Separated employees maintained active accounts after their separation dates. These accounts were not accessed after separation and were removed on identification.
- Four of 15 selected full-time employees separated during the period (October 1, 2014, to September 30, 2015) did not have separation emails sent out upon their departure. These users did not maintain privileged access to in-scope systems and the associated active directory accounts were either removed or disabled.

- 26 users maintained VPN accounts after their separation date. 22 of the 26 users did not maintain network accounts beyond separation, and therefore, could not use the remote access. The remaining four of 26 users, (b) (4) were disabled on or before the separation date.

Criteria—According to FISCAM, inactive accounts and accounts for separated individuals are disabled or removed in a timely manner. Unnecessary accounts (default, guest accounts) are removed, disabled, or otherwise secured.

Cause—In all cases, oversight on behalf of the Security Office responsible for notifying the administrators that the user is no longer employed/contracted and on behalf of the administrator with access removal responsibilities contributed to separated user notifications not being sent and/or separated users maintaining access.

Effect or Potential Effect—If access were to be exploited, unauthorized changes could have been made to Ex-Im Bank's financial reporting systems. Nevertheless, compensating controls, such as the annual access review, were in place and operating effectively and the users did not retain elevated privileges in the systems and did not login after separation, making the risk of a material misstatement as a result of these deficiencies low.

Recommendation—We recommend that Ex-Im Bank enhances and follows the process for removing user access as part of the employee separation process. As a part of this process, we recommend that follow-up action is taken for each Separated user to confirm that access was removed.

Ex-Im Bank's Response to Finding—Management agrees with this recommendation. In our management response to 2015-003, we have committed to an expansion of the email distribution list for all privileged user terminations, so that all system administrators receive notifications of the departure of a privileged user. We will expand this distribution to all employee and contractor terminations as well. Additionally, we already conduct monthly account reviews for network accounts. We will expand this effort to include VPN accounts as well as major application accounts including FMS-NG and EXIM Online. This effort will be completed by June 1, 2016.

2015-006 Password Configurations

Condition—(b) (7)(E)

Criteria—According to FISCAM, password-based authenticators are not displayed when entered;· are changed periodically (e.g., every 30 to 90 days); contain alphanumeric and special characters;· are sufficiently long (e.g., at least eight characters in length);· have an appropriate life (automatically expire);· are prohibited from reuse for a specified period of time (e.g., at least 6 generations); and· are not the same as the user ID.

Cause—The root cause of the password configurations not being applied are:

- Database servers: This was an open exception from the FY14 Audit as of 9/30/2014, and research was still being performed to determine the impact of changing the password settings for the servers supporting the in-scope applications and appliances.

- FMS-NG: Tests were in process to determine the impact of the new settings on the server. The password setting for (b) (7)(E) was not initially set when the application went live on October 1, 2015, the start of the testing period.

Effect or Potential Effect (b) (7)(E)

Recommendation—We recommend that Ex-Im Bank configures the password settings for its systems in accordance with its access control policy and reviews settings for new systems upon installation and on a periodic basis to ensure compliance with associated policies.

If necessary, we recommend Ex-Im Bank consider documenting each password setting that deviates from policy, as well as how the risk is still being addressed.

Ex-Im Bank's Response to Finding—Management agrees with this recommendation. We completed this effort on March 18, 2015. We document all deviations from password policy in the System Security Plan for the specific IT system. The original version of the SSP for FMS-NG was developed prior to the launch of FMS-NG and is being updated to reflect the current production system. Going forward, exceptions to password configuration policy (if any) will be captured in this manner.

2015-007 Security Monitoring

Condition—Out of our sample selection of 25 days, we noted that daily security reports were not compiled and distributed from March 4, 2015, through June 10, 2015. However, we noted that alternate methods of network monitoring, scanning, vulnerability assessment, and threat alert configurations were still operating during this period and that identified potential issues or vulnerabilities were documented, escalated, and remediated as necessary during this period.

Criteria—According to FISCAM, management initiates prompt action to correct deficiencies. Action plans and milestones are documented. Deficiencies are analyzed in relation to the entire agency/entity and appropriate corrective actions are applied entity-wide. Corrective actions are tested and are monitored after they have been implemented and monitored on a continuing basis.

Cause—The root cause was that personnel responsibilities for distributing the daily security report were not defined during the restructuring of the security office after key members of the team were separated.

Effect or Potential Effect—If the daily security report is not compiled and distributed, it is possible that the appropriate personnel responsible for taken action for security vulnerabilities and breaches may not be made aware in a timely manner to mitigate or remediate the security issue.

Recommendation—We recommend that Ex-Im Bank determine backups for the users who are primarily responsible for distributing the daily security report so that the report is sent out on a consistent frequency, or otherwise determine another method of documenting and communicating the review for each day's monitoring, scanning, investigation, and resolution activities to management.

Ex-Im Bank's Response to Finding—Management agrees with this recommendation. Ex-Im Bank will define and assign primary and backup responsibility for preparing the daily security report. This will include any required cross-training of our System Administrator staff. This activity will be completed by March 1, 2015.

2015-008 Background Employment Credentials

Condition—A full-time employee from the sample selection, maintained a background investigation file ("MBI) that expired during the testing period from October 1, 2014 to September 30, 2015. The user, therefore, did not have a valid background check on file required for employment at Ex-Im Bank.

Criteria—According to FISCAM, for prospective employees, references are contacted and background checks performed. Individuals are screened before they are given authorization to access organizational information and information systems. Periodic reinvestigations are performed as required by law, and implementing regulations (at least once every five years), consistent with the sensitivity of the position per criteria from the Office of Personnel Management.

Cause—The root cause was that the user's security clearance credentials expired during the testing period and the process for renewing the credentials had not yet been started (the annual recertification review is performed at the end of the calendar year).

Effect or Potential Effect—If users do not maintain the appropriate security clearance credentials and actively renew their credentials when they expire, it is possible that users could have inappropriate knowledge and access to information and data that is out of their grade.

Recommendation—We recommend that Ex-Im Bank keep track of the security status of employees who have clearances that are close to expiring and perform checks more frequently than annually, so that they can proactively start the renewal process. This can be accomplished through a security credential review on a quarterly basis or other frequency deemed appropriate by the Bank.

Ex-Im Bank's Response to Finding—Management agrees with the recommendation. Ex-Im Bank is required by OPM to perform an annual review of required background investigation. This investigation looks ahead one year to determine which employees require the update background check. Additionally, when Ex-Im onboard employees who have existing background checks from other agencies, Ex-Im ensures they have valid and not expired background checks. Ex-Im will investigate this instance and take any appropriate action to resolve it.

2015-009 Improper Certification of Disbursements

Condition—D&T noted that for one out of 45 disbursement selections a disbursement being certified and sent without a proper supporting documentation.

Criteria—All disbursements should be substantiated with valid supporting documentation prior to being sent.

Cause—Due to the implementation of the new FMS-NG, disbursements were not initially processed through the system and were instead handled manually. This resulted in an amount that should have been treated as noncash being disbursed.

Effect or Potential Effect—Subsequent to the incident and prior to our testing, Ex-Im Bank identified the incident through a compensating controls and recovered the funds. While approximately $1,400,000 was improperly disbursed, the potential effect of this control deficiency is $0 due to the presence of compensating controls. Since then, Ex-Im Bank Separated the manual disbursement process and implemented an automated disbursement process.

Recommendation—We recommend that Ex-Im Bank maintain an automated disbursement process to ensure that there is no confusions regarding the amounts requested to be disbursed.

Ex-Im Bank's Response to Finding—Management agrees with the recommendation. Manual disbursements were only in place for very short period of time and for only limited scenarios once the new system was implemented. As mentioned above, the issue was detected via internal controls. At the point in time D&T tested the certification process, Ex-Im Bank had already implemented the automation of the disbursement process.

SECTION II—DEFINITIONS

The definitions of a deficiency and a material are as follows:

A *deficiency* in internal control over financial reporting 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. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met. A deficiency in operation exists when (a) a properly designed control does not operate as designed or (b) the person performing the control does not possess the necessary authority or competence to perform the control effectively.

A *material weakness* is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

* * * * * *

EXPORT-IMPORT BANK
OF THE UNITED STATES

November 12, 2015

Deloitte & Touche LLP
7900 Tysons One Place
McLean, VA 22102-4219

We are providing this letter in connection with your audits of the balance sheets of the Export-Import Bank of the United States, ("EXIM", "Bank", "EXIM Bank", or "we") as of September 30, 2015 and 2014 and the related statements of net costs, changes in net position, and combined statements of budgetary resources for the years then ended, and the related notes to the financial statements, (hereinafter referred to collectively as the "financial statements") for the purpose of expressing an opinion as to whether the financial statements present fairly, in all material respects, the financial position of EXIM Bank, its net costs of operations and changes in net position, and combined budgetary resources, in conformity with accounting principles generally accepted in the United States of America applicable to federal agencies (government GAAP).

We confirm that we are responsible for the following:

a. The preparation and fair presentation in the financial statements of financial position, net costs of operations and changes in net position, and combined budgetary resources in conformity with accounting principles generally accepted in the United States of America.

b. The fair presentation of the required supplemental information, including Management's Discussion and Analysis and additional information accompanying the financial statements that is presented for the purpose of additional analysis of the financial statements.

c. The design, implementation, and maintenance of internal controls

   - Relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error; and

   - To prevent and detect fraud.

d. Establishing and maintaining effective internal controls over financial reporting.

Certain representations in this letter are described as being limited to matters that are material. Items are considered material, regardless of size, if they involve an omission or misstatement of accounting information that, in light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would be changed or influenced by the omission or misstatement.

We confirm, to the best of our knowledge and belief, the following representations made to you during your audits.

1. The financial statements referred to above are fairly presented in conformity with accounting principles generally accepted in the United States of America applicable to federal agencies, and include all disclosures necessary for such fair presentation and disclosures otherwise required to be included by the laws and regulations to which EXIM Bank is subject, including the Export-Import Bank Act of 1945, as amended, and the Federal Credit Reform Act of 1990.

2. The required supplemental information (Management's Discussion and Analysis), accompanying the financial statements is fairly presented and are consistent with the financial statements.

3. EXIM Bank has provided to you all relevant information and access as agreed in the terms of the audit engagement letter.

4. EXIM Bank has provided you:

   a. Financial records and related data;

   b. Minutes of the meetings of board of directors and committees of the board of directors or summaries of actions of recent meetings for which minutes have not yet been prepared; and

   c. Regulatory examination reports, supervisory correspondence or agreements, enforcement actions, and similar materials from applicable regulatory agencies, (particularly, communications concerning supervisory actions or noncompliance with, or deficiencies in, rules and regulations).

5. There has been no communication from regulatory agencies or from the Office of Management and Budget (OMB) concerning noncompliance with or deficiencies in financial reporting practices or other matters that could have a material effect on the financial statements. Further, we have advised you that there are not any regulatory examinations in process or completed for which reports have not yet been issued.

6. We have disclosed to you the latest results of management's risk assessment, including the assessment of the risk that the financial statements may be materially misstated as a result of fraud.

7. We have no knowledge of any fraud or suspected fraud affecting EXIM Bank involving:

   a. Management;

   b. Employees who have significant roles in internal control over financial reporting; or

   c. Others, when the fraud could have a material effect on the financial statements.

8. We have no knowledge of any allegations of fraud or suspected fraud affecting EXIM Bank received in communications from employees, former employees, analysts, regulators, lenders, exporters, or others except for allegations of fraud deemed non-credible or deemed credible enough to have been referred to the Office of the Inspector General as of the date of this letter and which we have disclosed to you.

9. There are no unasserted claims or assessments that legal counsel has advised us are probable of

assertion and must be disclosed in accordance with the Statement of Federal Financial Accounting Standard ("SFFAS") No. 5, Accounting for Liabilities of the Federal Government, that have not been disclosed to you.

10. Significant assumptions used by us in making accounting estimates are reasonable.

11. Except for the pending Omnibus Appropriation Bill for fiscal year 2016 and the extension of EXIM Bank's authority as disclosed in footnote 1, we are not aware of any recent or pending legislation having direct effects on the operations of EXIM Bank that are required to be accrued or disclosed in the financial statements.

12. According to OMB Circular A-136, Financial Reporting Requirements, we are not required to prepare the Schedule of Spending.

13. We have no intention of terminating our participation in the Civil Service Retirement System (CSRS) or the Federal Employees Retirement System (FERS) or taking any other action that could result in an effective termination or reportable event of any of the plans. We are not aware of any occurrences that could result in the termination of our participation in the CSRS or FERS. Although EXIM Bank funds a portion of pension benefits under the CSRS and FERS relating to its employees and makes the necessary payroll withholdings for them, EXIM Bank has no liability for future payments to employees under these programs and does not account for the assets of the CSRS and FERS, nor does EXIM Bank have actuarial data with respect to accumulated plan benefits or the unfunded pension liability relative to its employees. These amounts are reported by the Office of Personnel Management (OPM) for the Retirement Systems and are not allocated to the individual employers. OPM also accounts for the health and life insurance programs for current and retired civilian federal employees. Similar to the accounting treatment afforded the retirement programs, the actuarial data related to the health and life insurance programs is maintained by OPM and is not available on an individual employer basis.

14. We have disclosed to you the accounting conventions used when preparing our financial statements. We believe that the effect of applying these accounting conventions and the use of such applications, in particular the use of (a) August 31, 2015 outstanding balances, and (b) June 30, 2015 default rates, to compute the subsidy re-estimate as of September 30, 2015 are immaterial to the financial statements.

15. We are responsible for compliance with applicable local, state, and federal laws, rules, and regulations, including compliance with the requirements of the Federal Credit Reform Act of 1990. We are responsible for establishing and maintaining the components of internal control relating to our activities in order to achieve the objectives of providing reliable financial reports, effective and efficient operations, and compliance with laws and regulations. We are responsible for maintaining accounting and administrative control over revenues, obligations, expenditures, assets, and liabilities.

16. We have disclosed to you all deficiencies in the design or operation of internal control over financial reporting identified as part of our evaluation, including separately disclosing to you all such deficiencies that are significant deficiencies or material weaknesses in internal control over financial reporting.

17. We have included in the corrective action plan for current-year findings, the name of the person in our organization responsible for implementation of the actions, the actions to be taken, and the estimate of a completion date. We have taken timely and appropriate steps to remedy findings that

you report.

18. Management has identified and disclosed to you all laws and regulations that have a direct and material effect on the determination of financial statement amounts.

19. We believe that substantial doubt regarding the ability of EXIM Bank to continue as a going concern does not exist as of September 30, 2015.

20. We believe that EXIM will receive a full year appropriation when Congress approves funding for the entire U.S. Government. EXIM is currently appropriated through a government wide continuing resolution through December 11, 2015. In accordance with its Charter (12 USC 635 et seq.) continuation of EXIM's functions in furtherance of its objects and purposes is subject to periodic extensions granted by Congress.

21. We believe the various bills introduced in the Senate and House of Representatives to reauthorize the Bank as well as votes and other actions taken in both Houses of Congress in support thereof, indicates that the Bank will be reauthorized.

22. The lapse in full authority did not terminate the Bank or its Charter but changed the mission of the Bank from one based on financing U.S. exports in support of U.S. jobs, to one primarily focused on managing its portfolio to maturity. The Charter of the Bank remains in full force and effect.

23. We believe that the reclassification of exposure by geographical region within footnote 6 to the financial statements better illustrates information of the region and current geography.

Except where otherwise stated below, matters less than $ 40,520,000, in the aggregate, are not considered to be exceptions that require disclosure for the purpose of the following representations. This amount is not necessarily indicative of amounts that would require adjustment to, or disclosure in, the financial statements.

24. There are no transactions that have not been properly recorded in the accounting records underlying the financial statements.

25. Regarding required supplementary information:

    a. We confirm that we are responsible for the required supplementary information;

    b. The required supplementary information is measured and presented in accordance with U.S. Government GAAP; and

    c. The methods of presentation of the supplementary information have changed from those used in the prior period and, the reasons for such changes are to better represent budgetary information.

26. We have disclosed to you any changes in EXIM Bank's internal control over financial reporting that occurred during EXIM Bank's most recent fiscal year that has materially affected, or is reasonably likely to materially affect, EXIM Bank's internal control over financial reporting.

27. EXIM Bank has no plans or intentions that may affect the carrying value or classification of assets and liabilities.

28. Regarding related parties:

    a. We have disclosed to you the identity of the EXIM's related parties and all the related party relationships and transactions of which we are aware.

    b. To the extent applicable, related parties and all the related-party relationships and transactions, including sales, purchases, loans, transfers, leasing arrangements, and guarantees (written or oral) have been appropriately identified, properly accounted for, and disclosed in the financial statements.

29. Arrangements with financial institutions involving compensating balances or other arrangements involving restrictions on cash balances, line of credit, or similar arrangements have been properly disclosed in the financial statements.

30. For financial instruments with off-balance-sheet credit risk, we have disclosed the following:

    a. The face or contract amount

    b. The nature and terms, including a discussion of the following:

    - Credit and market risks of those instruments
    - Cash requirements of those instruments
    - Related accounting policy pursuant to OMB Circular A-136

    c. EXIM's policy for requiring collateral or other security to support financial instruments subject to credit risk, information about the EXIM's access to that collateral or other security, and the nature and brief description of the collateral or other security supporting those financial instruments.

31. EXIM Bank believes that it does not have any derivative instruments that require identification or any embedded derivative instruments that require bifurcation.

32. Loan receivables and claims recorded in the financial statements represent valid claims against debtors for sales or other charges arising on or before the balance-sheet date and have been appropriately reduced to their estimated net realizable value and disclosed in the financial statements.

33. All impaired loan receivables have been properly recorded and disclosed in the financial statements.

34. Loans that have been restructured to provide a reduction or deferral of interest or principal payments because of borrower financial difficulties have been properly recorded and disclosed in the financial statements.

35. All intra-entity transactions and balances have been appropriately identified and eliminated for financial reporting purposes, unless otherwise noted. All intra-governmental transactions and balances have been appropriately recorded, reported, and disclosed. We have reconciled intra-governmental transactions and balances with the appropriate trading partners for the four fiduciary transactions identified in Treasury's Intra-governmental Fiduciary Transactions Accounting Guide, and other intra-governmental asset, liability, and revenue amounts as required by the applicable OMB Bulletin.

36. In preparing the financial statements in conformity with accounting principles generally accepted in the United States of America applicable to federal agencies, management uses estimates. All estimates have been disclosed in the financial statements for which known information available prior to the issuance of the financial statements indicates that both of the following criteria are met:

    a. It is at least reasonably possible that the estimate of the effect on the financial statements of a condition, situation, or set of circumstances that existed at the date of the financial statements will change in the near term due to one or more future confirming events; and

    b. The effect of the change would be material to the financial statements.

37. Risks associated with concentrations, based on information known to management, that meet all of the following criteria have been disclosed in the financial statements:

    a. The concentration exists at the date of the financial statements;

    b. The concentration makes the enterprise vulnerable to the risk of a near-term severe impact; and

    c. It is at least reasonably possible that the events that could cause the severe impact will occur in the near term.

38. There are no:

    a. Instances of identified or suspected noncompliance with laws or regulations whose effects should be considered when preparing the financial statements or as a basis for recording a loss contingency;

    b. Known actual or possible litigation and claims whose effects should be considered and accounted for and disclosed in the financial statements and that have not been disclosed to you and accounted for and disclosed in accordance with government GAAP; or

    c. Other liabilities or gain or loss contingencies that are required to be accrued or disclosed by SFFAS No. 5, Accounting for Liabilities of the Federal Government.

39. EXIM Bank has satisfactory title to all owned assets, and there are no liens or encumbrances on such assets nor has any asset been pledged as collateral.

40. EXIM Bank has complied with all aspects of contractual agreements that may have an effect on the financial statements in the event of noncompliance.

41. No division of the EXIM Bank has reported a material instance of noncompliance to us.

42. EXIM Bank is responsible for determining and maintaining the adequacy of the allowance for losses, as well as estimates used to determine such amounts. Management includes the undisbursed exposure as part of the outstanding balances in re-estimating the subsidy cost allowance for direct loans and the liability for loan guarantees, claims, and insurance. Management believes the allowance is adequate to absorb currently estimated credit losses in EXIM Bank portfolio as of September 30, 2015. Management believes the allowance for losses has been determined in accordance with accounting principles generally accepted in the United States of

America applicable to federal agencies as of September 30, 2015. At September 30, 2015, management made its best judgment of identifiable probable losses in the loan, claim, insurance, and guarantee portfolios. Management believes that the assumptions, including the budget cost level for each individual credit exposure, used to determine the allowance are appropriate in the circumstances as of September 30, 2015.

43. The allowance for losses provides for expected losses inherent in the loan, claim, guarantee, and insurance portfolios. The allowance is established as losses are estimated to have occurred through a provision charged to earnings. Write-offs are charged against the allowance when management believes the uncollectibility of a loan or claim balance is confirmed. Subsequent recoveries, if any, are credited to the allowance.

44. The information presented on EXIM Bank's statement of budgetary resources ("SBR") agrees with the information submitted on EXIM Bank's year-end Reports on Budget Execution and Budgetary Resources (SF 133s). This information will be used as input for the fiscal year 2015 actual column of the Program and Financing Schedules reported in the fiscal year 2015 Budget of the U.S. Government. Such information is supported by the related financial records and related data.

45. With regard to the fair value measurements and disclosures of certain assets, liabilities, and specific components of equity, such as pre-credit reform loan receivables, pre-credit reform guarantees, receivables from subrogated claims, claims payable, we believe that:

    a. The measurement methods, including the related assumptions, used in determining fair value were appropriate and were consistently applied;

    b. The completeness and adequacy of the disclosures related to fair values are in conformity with accounting principles generally accepted in the United States of America applicable to federal agencies; and

    c. No events have occurred after September 30, 2015, but before November 12, 2015, the date the financial statements were available to be issued, that require adjustment to the fair value measurements and disclosures included in the financial statements.

46. There have been no changes in the amount of capital stock held by the U.S. Treasury during the fiscal year.

47. EXIM Bank is not obligated to repay the U.S. Treasury borrowings on a set payment schedule. EXIM Bank will repay the full amount of the borrowings by 2033.

48. We have complied in all material respects with certain provisions of law, regulations, contracts, and grants, noncompliance with which could have a direct and material effect on the determination of the financial statements amounts. We represent that the applicable laws and regulations with which noncompliance could have a direct and material effect are the following:

    a. Export-Import Bank Act of 1945, as amended;

    b. Federal Credit Reform Act of 1990;

    c. OMB Circular A-136;

d. OMB Circular A-11;

e. Federal Financial Management Improvement Act of 1996;

f. Federal Acquisition Regulations (48 CFR Chapter 1);

g. Federal Information Security Management Act of 2002 (FISMA);

h. Government Corporation Control Act; and

i. OMB Bulletin No. 07-04 Appendix E.

49. As of September 30, 2015, EXIM Bank was named in several legal actions, virtually all of which involved claims under guarantee and insurance programs. It is not possible to predict the eventual outcome of the various actions, however, it is management's opinion that these claims will not result in liabilities which would materially affect the financial position or results of operations of EXIM Bank.

50. EXIM Bank does not have earmarked funds as defined by SFFAS No. 27, "Identifying and Reporting Earmarked Funds."

51. We believe our allowance for losses is sufficient to cover any losses that EXIM Bank may incur with respect to transactions that may be the subject of fraud. For non-monitored transactions, when there is a payment default (under a direct loan) or claim payment (under a guarantee), EXIM Bank writes down the receivable to a Budget Cost Level 11 or 12. We are not aware of any credible evidence of fraud relating to monitored loans or guarantees, except as set forth in paragraph 8 above.

52. We are not aware of any violations of the Anti-deficiency Act that we must report to the Congress and the President (and provide a copy of the report to the Comptroller General) for the years ended September 30, 2015 and 2014 and through the date of this letter.

53. EXIM Bank is not a party to major treaties or other international agreements except for an international agreement with the Government of Vietnam. We believe that the agreement does not result in any claims or contingencies which are required to be disclosed in Note 14, Commitments and Contingencies as required by OMB Circular No. A-136.

54. No events or transactions have occurred after September 30, 2015, but before November 12, 2015, the date the financial statements were available to be issued, that require consideration as adjustments to or disclosures in the financial statements.

Fred P. Hochberg
Chairman & President

David M. Sena
Chief Financial Officer

Patricia Wolf
Controller

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