



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

**Independent Audit of Export-
Import Bank's Information
Security Program for
Fiscal Year 2015**

February 2, 2016
OIG-AR-16-02

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.



EXPORT-IMPORT BANK
of the UNITED STATES

INSPECTOR GENERAL

To: Howard Spira, Chief Information Officer

From: Terry Settle, Assistant Inspector General for Audits

Subject: Independent Audit of Export-Import Bank's Information Security Program for Fiscal Year 2015 (OIG-AR-16-02)

Date: February 2, 2016

This memorandum transmits Cotton & Company LLP's audit report of Export-Import Bank's (Ex-Im Bank) Information Security Program for Fiscal Year 2015. Under a contract monitored by this office, we engaged the independent public accounting firm of Cotton & Company to perform the audit. The objective of the audit was to determine whether the Ex-Im Bank developed and implemented effective information security programs and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA).

Cotton & Company determined that overall Ex-Im Bank's information security program and practices are substantially effective. Ex-Im Bank continued to improve and strengthen its information security program during fiscal year 2015. However, Ex-Im Bank has a few areas in which additional improvements can be made. The report contains four new recommendations and four re-issued recommendations from prior years for corrective action. Management concurred with the recommendations and we consider management's proposed actions to be responsive. The recommendations will be closed upon completion and verification of the proposed actions.

We appreciate the cooperation and courtesies provided to Cotton & Company and this office during the audit. If you have questions, please contact me at (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 Hochberg, Chairman and President
C.J. Hall, Executive Vice President
Angela Freyre, General Counsel
Audit Committee
John Lowry, Director, Information Technology Security and Systems Assurance
Inci Tonguch-Murry, Deputy Chief Financial Officer
Cristopolis Dieguez, Business Compliance Analyst
George Bills, Partner, Cotton & Company LLP



Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

January 29, 2016

Terry Settle
Assistant Inspector General for Audits
Export-Import Bank
811 Vermont Avenue, NW
Washington, DC 20571

Subject: Independent Audit of Export-Import Bank's Information Security Program for Fiscal Year 2015

Dear Ms. Settle:

We are pleased to submit this report in support of audit services provided pursuant to Federal Information Security Modernization Act (FISMA) requirements. Cotton & Company LLP conducted an independent audit of the Export-Import Bank of the United States (Ex-Im Bank)'s information security program and practices for the fiscal year ended September 30, 2015. Cotton & Company performed the work from May through November 2015.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as amended, promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Please feel free to contact me with any questions.

Sincerely,

COTTON & COMPANY LLP

A handwritten signature in blue ink that reads "George E. Bills".

George E. Bills, CPA, CISSP, CISA, CIPP
Partner

The Export-Import Bank of the United States (Ex-Im Bank) is the official export-credit agency of the United States. Ex-Im Bank is an independent, self-sustaining executive agency and a wholly-owned U.S. government corporation. Ex-Im Bank’s mission is to support jobs in the United States by facilitating the export of U.S. goods and services. Ex-Im Bank provides competitive export financing and ensures a level playing field for U.S. exports in the global marketplace.

The Office of Inspector General, an independent office within Ex-Im Bank, was statutorily created in 2002 and organized in 2007. The mission of the Ex-Im Bank Office of Inspector General is to conduct and supervise audits, investigations, inspections, and evaluations related to agency programs and operations; provide leadership and coordination as well as recommend policies that will promote economy, efficiency, and effectiveness in such programs and operations; and prevent and detect fraud, waste, abuse, and mismanagement.

ACRONYMS

CIO	Chief Information Officer
DHS	Department of Homeland Security
EOL	Ex-Im Online
FISMA	Federal Information Security Modernization Act of 2014
FMS-NG	Financial Management System – Next Generation
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act of 2000
GSS	General Support System
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
PIV	Personal Identity Verification
SA&A	Security Assessment & Authorization
SP	Special Publications
SSP	System Security Plan

Executive Summary

Independent Audit of Export-Import Bank's Information Security Program for Fiscal Year 2015

OIG-AR-16-02
February 2, 2016

Why We Did This Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to develop, document, and implement agency-wide information security programs to protect their information and information systems. FISMA also requires agencies to undergo an annual independent evaluation of their information security programs and practices to determine their effectiveness. To fulfill its FISMA responsibilities, the Office of the Inspector General contracted with Cotton & Company LLP for an annual independent evaluation of the Export-Import Bank (Ex-Im Bank or the Bank)'s information security program and practices.

What We Recommended

We made four new recommendations for the Chief Information Officer to (1) update the (b) (7)(E) System Security Plan, (2) document configuration management plans for the (b) (7)(E) systems that address specific requirements, (3) implement a process to ensure that all system Plans of Action and Milestones (POA&Ms) are reviewed on an organization-defined frequency and that milestones are updated to reflect actions taken to remediate POA&M items, and (4) ensure that testing of the Continuity of Operations Plan is performed on an annual basis to ensure that Ex-Im Bank is prepared to continue operations and appropriately respond to potential disasters.

What Cotton & Company LLP Found

Overall, we found that Ex-Im Bank's information security program and practices are substantially effective. Specifically, we noted that Ex-Im Bank continues to improve and strengthen its information security program and is addressing the challenges in each of the areas that the Department of Homeland Security identified for the fiscal year 2015 FISMA review. During the past year, Ex-Im Bank made substantial progress in the implementation of personal identity verification (PIV) card usage for logical system access. Additionally, Ex-Im Bank updated and implemented its vulnerability management program to ensure that moderate vulnerabilities identified are tracked, assessed, and remediated as appropriate. Finally, Ex-Im Bank completed a risk assessment of the wireless environment to ensure that it has considered risks associated with introducing this technology into its network.

While these efforts have resulted in improvements in Ex-Im Bank's information security program, Ex-Im Bank is not compliant with all FISMA requirements. Specifically:

- While Ex-Im Bank has implemented PIV access for logical network authentication, this authentication is not currently being implemented agency-wide. We found that not all contractors are using PIV cards for logical access as required by HSPD-12. *(2012-2014 prior-year finding)*
- Bank management has not implemented an effective account management process to ensure that accounts are periodically reviewed for appropriateness and disabled when users leave the agency, or after a specified period of inactivity. *(2013 and 2014 prior-year finding)*
- Bank management has not implemented appropriate security controls over (b) (7)(E) used to access Ex-Im Bank data. *(2014 prior-year finding)*
- Bank management has not implemented (b) (7)(E) in compliance with established Bank policies. *(2014 prior-year finding)*
- Bank management has not adequately documented National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4 controls within the (b) (7)(E) security plan (SSP).
- Bank management has not adequately documented configuration management plans for its (b) (7)(E) systems.
- Bank management has not adequately remediated Plan of Action and Milestones (POA&M) items in a timely manner.
- Bank management has not adequately tested its Continuity of Operations Plan (COOP) capabilities and effectiveness.

For additional information, contact the Office of the Inspector General at (202) 565-3908 or visit www.exim.gov/oig.

TABLE OF CONTENTS

INTRODUCTION

Objectives	1
Scope and Methodology	1
Background	2

RESULTS

Finding: Ex-Im Bank Should Fully Implement Multifactor Authentication for Internal Network Access Using PIV	5
Recommendation, Management's Response, and Evaluation of Management's Response	6
Finding: Ex-Im Bank Should Improve Controls over Account Management	7
Recommendation, Management's Response, and Evaluation of Management's Response	8
Finding: Ex-Im Bank Should Improve Security Controls over (b) (7)(E)	9
Recommendation, Management's Response, and Evaluation of Management's Response	10
Finding: Ex-Im Bank Should Improve Controls over (b) (7)(E)	11
Recommendation, Management's Response, and Evaluation of Management's Response	12
Finding: Ex-Im Bank Should Improve Controls over (b) (7)(E) Security Plan Documentation	13
Recommendation, Management's Response, and Evaluation of Management's Response	14
Finding: Ex-Im Bank Should Improve Controls over Configuration Management	14
Recommendation, Management's Response, and Evaluation of Management's Response	15
Finding: Ex-Im Bank Should Improve Controls over Its Plan of Action & Milestones Process	16
Recommendation, Management's Response, and Evaluation of Management's Response	17
Finding: Ex-Im Bank Should Improve Controls over Continuity of Operations	18
Recommendation, Management's Response, and Evaluation of	

Management's Response	18
APPENDIX A	
Federal Laws, Regulations, Policies, and Guidance	20
Prior Coverage	21
APPENDIX B	
Management Comments	25
APPENDIX C	
Selected Security Controls and Testing Results	29

Objective

This report presents the results of the independent audit of the information security program of the Export-Import Bank (Ex-Im Bank or the Bank) for fiscal year (FY) 2015, conducted by Cotton & Company LLP. The objective was to determine whether Ex-Im Bank developed and implemented effective information security programs and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA).

Scope and Methodology

We performed the audit to determine whether Ex-Im Bank developed and implemented effective information security programs and practices as required by FISMA. Specifically, we evaluated Ex-Im Bank's security program, plans, policies, and procedures in place as of September 30, 2015, for compliance with applicable federal laws and regulations and guidance issued by Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST). We performed a high-level review of each of the Bank's four major systems (FMS-NG, Infrastructure GSS, Ex-Im Online, and Oracle GSS) and performed detailed steps, as outlined in the Department of Homeland Security (DHS) FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.2, to evaluate Ex-Im Bank's policies, procedures, and practices for key areas such as (i) continuous monitoring management, (ii) security configuration management, (iii) identity and access management, (iv) incident response, (v) risk management, (vi) security training, (vii) agency-wide and system-specific Plans of Action & Milestones, (viii) remote access management, (ix) contingency planning management, and (x) contractor system oversight.

In addition, we assessed whether Ex-Im Bank had implemented judgmentally selected minimum security controls from NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for its (b) (7)(E)

as required by FISMA. NIST Special Publication (SP) 800-53, Rev. 4 organizes security controls into 18 security control families (e.g., access controls, contingency planning controls). The minimum security controls tested for (b) (7)(E) (b) (7)(E) were chosen from selected security control families through a collaborative effort between the Ex-Im Bank OIG and Cotton & Company.

We conducted interviews with the Chief Risk Officer, as well as with Office of the Chief Information Officer (CIO) personnel. We also reviewed policies, procedures, and practices for compliance with NIST and OMB guidance; reviewed system documentation and evidence; and conducted testing on Ex-Im Bank's controls. For both tasks, we fully documented our testing methodology through creation of a planning memorandum and audit work programs.

Cotton & Company conducted the audit onsite at Ex-Im Bank in Washington, DC, as well as remotely at the Cotton & Company office in Alexandria, VA, with fieldwork from May to

November 2015. Cotton & Company conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as established in the Government Accountability Office (GAO)'s *Government Auditing Standards*, December 2011 Revision. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management officials on December 14, 2015, and included their comments where appropriate.

See Appendix A for details of federal laws, regulations, policies, and guidance, and for a discussion of prior audit coverage.

Background

The Export-Import Bank of the United States is an independent, self-sustaining executive agency and a wholly-owned United States government corporation. Ex-Im Bank's charter, *The Export Import Bank Act of 1945*, as amended through Public Law 112-122, May 30, 2012, states:

It is the policy of the United States to foster expansion of exports of manufactured goods, agricultural products, and other goods and services, thereby contributing to the promotion and maintenance of high levels of employment and real income, a commitment to reinvestment and job creation, and the increased development of the productive resources of the United States.

To fulfill its charter, Ex-Im Bank assumes the credit and country risks that the private sector is unable or unwilling to accept. The Bank authorizes working capital guarantees, export-credit insurance, loan guarantees, and direct loans to counter the export financing provided by foreign governments on behalf of foreign companies and help U.S. exporters remain competitive. The major mission-critical systems supporting these programs and the Bank's mission are:

1. Financial Management System – Next Generation (FMS-NG)
2. Infrastructure General Support System (GSS)
3. Ex-Im Online (EOL)
4. Oracle GSS

Ex-Im Bank's network infrastructure consists largely of networking devices with various servers running different operating system platforms. Standard desktop personal computers and laptops run Windows 7. The networks are protected from external threats by a range of information technology security devices, including firewalls, intrusion detection and prevention, antivirus, and spam-filtering systems.

Federal Laws, Roles, and Responsibilities. On December 17, 2002, the President signed into law the E-Government Act (Public Law 107-347), which included the Federal Information Security Management Act of 2002. FISMA, as amended,¹ permanently reauthorized the framework established in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA continues the annual review and reporting requirements introduced in GISRA. In addition, FISMA includes new provisions aimed at further strengthening the security of the federal government's information and information systems, such as the development of minimum standards for agency systems. NIST has been tasked to work with federal agencies in the development of those standards. The standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) and SPs. FIPS provide the minimum information security requirements that are necessary to improve the security of federal information and information systems, and the SP 800 and selected 500 series provide computer security guidelines and recommendations. For instance, FIPS Publication 200 requires agencies to adopt and implement the minimum security controls documented in NIST SP 800-53.

Federal agencies are required to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over information technology that support operations and assets. FISMA also provides a mechanism for improved oversight of federal agency information security programs, as it requires agency heads, in coordination with their CIOs and Senior Agency Information Security Officers, to report the security status of their information systems to DHS and OMB through CyberScope. CyberScope, operated by DHS on behalf of OMB, replaces the legacy paper-based submission process and automates agency reporting. In addition, Offices of Inspectors General (OIGs) provide an independent assessment of whether the agency is applying a risk-based approach to its information security programs and information systems. OIGs must also report their results to OMB annually through CyberScope.

¹ The Federal Information Security Modernization Act of 2014 amends the FISMA Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

The objective of this audit was to determine whether Ex-Im Bank developed and implemented effective information security programs and practices as required by FISMA. Overall, we found that Ex-Im Bank's information security program and practices are substantially effective. For 8 of 10 control areas tested for the DHS Cyberscope testing, the Bank adequately implemented programs that were consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Additionally, the Bank adequately implemented all but 3 of the 22 NIST controls tested. Finally, we noted that Ex-Im Bank continued to make improvements to its information security program during fiscal year (FY) 2015. For example, Ex-Im Bank:

- Made substantial progress in the implementation of personal identity verification (PIV) card usage for logical system access.
- Updated and implemented its vulnerability management program to ensure that moderate vulnerabilities identified are tracked, assessed, and remediated as appropriate.
- Completed a risk assessment of the wireless environment to ensure that it has considered risks associated with introducing this technology into its network.

While these efforts have resulted in improvements in Ex-Im Bank's information security program, there are areas in which the Bank can make additional improvements. Specifically:

- While Ex-Im Bank has implemented PIV access for logical network authentication, this authentication is not currently being implemented agency-wide, as we found that not all contractors are using PIV cards for logical access as required by HSPD-12. *(2012-2014 prior-year finding)*
- Bank management has not implemented an effective account management process to ensure that accounts are periodically reviewed for appropriateness and disabled when users leave the agency, or after a specified period of inactivity. *(2013 and 2014 prior-year finding)*
- Bank management has not implemented appropriate security controls over (b) (7)(E) used to access Ex-Im Bank data. *(2014 prior-year finding)*
- Bank management has not implemented (b) (7)(E) in compliance with established Bank policies. *(2014 prior-year finding)*
- Bank management has not adequately documented NIST SP 800-53, Rev. 4 controls within the (b) (7)(E) security plan (SSP).

- Bank management has not adequately documented configuration management plans for its (b) (7)(E) systems.
- Bank management has not adequately remediated Plan of Action and Milestones (POA&M) items in a timely manner.
- Bank management has not adequately tested its continuity of operations plan (COOP) capabilities and effectiveness.

We made four new recommendations to address the above issues. These recommendations, if implemented, should strengthen Ex-Im Bank's information security. Ex-Im Bank management agreed with our recommendations and presented actions to address them. Ex-Im Bank management's responses to the findings identified in our audit are included within the report and in Appendix B.

Finding: Ex-Im Bank Should Fully Implement Multifactor Authentication for Internal Network Access using PIV

In our FY 2012 FISMA audit report, we recommended that the CIO fully implement the use of PIV cards to achieve multifactor authentication to the Ex-Im Bank network for all access, as required by OMB M-11-11. For FY 2015, we determined that Ex-Im Bank is still not using multifactor authentication in accordance with federal requirements. During our FY 2015 testing, we found that while the Bank had completed full PIV implementation for logical access for Bank employees, the implementation was not completed until the end of the fiscal year. In addition, the Bank had not fully implemented PIV access for contractors with access to the Bank's networks. Until Ex-Im Bank fully implements the use of PIV cards for all individuals accessing the Bank's network, it will not be in compliance with OMB requirements and will have an increased risk of unauthorized access.

The following guidance is relevant to this control activity:

OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, dated February 3, 2011, states:

This memorandum outlines a plan of action for agencies that will expedite the Executive Branch's full use of the credentials for access to federal facilities and information systems. As of December 2010, agencies reported that approximately 5 of 5.7 million federal employees and contractors have completed background investigations, and 4.5 million have PIV credentials. With the majority of the federal workforce now in possession of the credentials, agencies are in a position to aggressively step up their efforts to use the electronic capabilities of the credentials.

To that end, each agency should develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks,

and information systems. To be effective in achieving the goals of HSPD-12, and realizing the full benefits of PIV credentials, the agency's policy needs to include the following requirements:

- *Effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.*
- *Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.*
- *Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation. In order to ensure government-wide interoperability, OMB Memorandum 06-18, "Acquisition of Products and Services for Implementation of HSPD-12" requires agencies to acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications.*
- *Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.*
- *The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance" (available at www.idmanagement.gov).*

OMB FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity, dated June 12, 2015 states:

Federal agencies must:

- ***Dramatically accelerate implementation of multi-factor authentication, especially for privileged users.*** *Intruders can easily steal or guess usernames/passwords and use them to gain access to Federal networks, systems, and data. Requiring the utilization of a Personal Identity Verification (PIV) card or alternative form of multi-factor authentication can significantly reduce the risk of adversaries penetrating Federal networks and systems.*

Recommendation, Management's Response, and Evaluation of Management's Response

Recommendation:

As of FY 2015, our FY 2012 audit recommendation for the CIO to fully implement the use of PIV cards to achieve multifactor authentication to the Ex-Im Bank network for all access remains open; therefore, we are not issuing any new recommendations related to this

finding. See Appendix A for a complete listing of the status of prior-year FISMA audit recommendations.

Finding: Ex-Im Bank Should Improve Controls over Account Management

As initially identified in our FY 2013 FISMA audit report, we found during our FY 2015 testing that controls remained inadequate to ensure that user accounts are deactivated in a timely manner. Specifically, we found the following issues in FY 2015:

- For the (b) (7)(E) , we found that 11 of the 849 active accounts were not disabled after 90 days of inactivity. All of the identified accounts had been inactive for at least 4 months.
- For (b) (7)(E), we found that 11 of the 119 active accounts were not disabled after 90 days of inactivity.

Ex-Im Bank is not consistently carrying out its documented account management policy and procedures. Specifically, Ex-Im Bank is not disabling accounts within a timely manner or performing periodic account reviews to ensure the continued appropriateness of user access. Without adequately implementing the control to disable accounts for individuals who leave the agency or to review accounts that have been inactive for more than 90 days, there is an increased risk that individuals could obtain unauthorized access to accounts that should have been disabled or deleted.

Ex-Im Bank policies provide the following guidance related to account management:

EXIM Access Control, Identification and Authentication, version 2a, states:

6.1.6. The system owner (or designee(s)) must review annually the access privileges for each user with access to the application for which they are system owner to ensure that the access is still needed in order for the user to perform official duties.

6.1.7. Ex-Im Bank periodically reviews user accounts and tests the effectiveness of technical controls and procedures established to implement this policy.

6.2.9. Individual user IDs and passwords for the LAN and all applications must be immediately deactivated under the following conditions: (1) whenever notified by a user's authorizing official that the user no longer requires access; or (2) whenever notified by a proper authority (e.g., human resources, COTR) that the user's employment with the Bank has been terminated.

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

(b) (7)(E)

(b) (7)(E)

NIST provides the following guidance related to account management:

NIST SP 800-53, Rev. 4, AC-2, Account Management, states:

Control: The organization:

- a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];*
- b. Assigns account managers for information system accounts;*
- c. Establishes conditions for group and role membership;*
- d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;*
- e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;*
- f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];*
- g. Monitors the use of, information system accounts;*
- h. Notifies account managers:*
 - 1. When accounts are no longer required;*
 - 2. When users are terminated or transferred; and*
 - 3. When individual information system usage or need-to-know changes;*
- i. Authorizes access to the information system based on:*
 - 1. A valid access authorization;*
 - 2. Intended system usage; and*
 - 3. Other attributes as required by the organization or associated missions/business functions;*
- j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and*
- k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.*

Recommendation, Management's Response, and Evaluation of Management's Response

Recommendation:

In our FY 2013 FISMA audit report, we recommended that the Ex-Im Bank CIO:

1. Ensure that the account review process is conducted in accordance with organizational policies and procedures.

2. Ensure that inactive accounts are disabled after a period of 90 days in accordance with organizational policy and procedures.
3. Ensure that accounts for terminated individuals are removed immediately upon separation.

As of FY 2015, the recommendations noted remain open; therefore, we are not issuing any new recommendations related to this finding. See Appendix A for a complete listing of the status of prior-year FISMA audit findings.

Finding: Ex-Im Bank Should Improve Security Controls over (b) (7)(E)

As initially identified in our FY 2014 FISMA audit report, we found during our FY 2015 testing that controls are not adequate to ensure that Ex-Im Bank data accessible from (b) (7)(E) is adequately protected. Specifically, in FY 2015 we noted:

- (b) (7)(E)

- (b) (7)(E)

- (b) (7)(E)

(b) (7)(E)

The following guidance is relevant for this control activity:

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

FIPS Publication 140-2 states:

This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract...

Recommendation, Management's Response, and Evaluation of Management's Response

Recommendation:

In our FY 2014 FISMA audit report, we recommended that the Ex-Im Bank CIO deploy (b) (7)(E) security controls that:

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

As of FY 2015, the recommendations noted remain open; therefore, we are not issuing any new recommendations related to this finding. See Appendix A for a complete listing of the status of prior-year FISMA audit findings.

Finding: Ex-Im Bank Should Improve Controls over (b) (7)(E)

In our FY 2014 FISMA audit report, we found that controls were not adequate to ensure that (b) (7)(E) in accordance with Ex-Im Bank policy. Specifically, in FY 2014 we found:

- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)

During our FY 2015 testing, we noted that while the above weaknesses were remediated, controls (b) (7)(E) still need improvement. (b) (7)(E)

Management stated that this weakness exists because an administrator did not follow the established Bank procedures for (b) (7)(E).

Without effective (b) (7)(E) controls in place, Ex-Im Bank is more susceptible to cyber-attacks and data compromise.

Ex-Im Bank provides the following guidance related to (b) (7)(E) :

(b) (7)(F)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

NIST provides the following guidance related to (b) (7)(E)

(b) (7)(E) :

(b) (7)(E)

Recommendation, Management’s Response, and Evaluation of Management’s Response

Recommendation:

In our FY 2014 FISMA audit report, we recommended that the Ex-Im Bank CIO:

(b) (7)(E)

(b) (7)(E)

As of FY 2015, the recommendations noted remain open; therefore, we are not issuing any new recommendations related to this finding. See Appendix A for a complete listing of the status of prior-year FISMA audit findings.

Finding: Ex-Im Bank Should Improve Controls over (b) (7)(E)

Controls are not adequate to ensure that all Ex-Im (b) (7)(E) are appropriately documented to address all applicable NIST 800-53, Rev. 4 controls. Specifically, we noted that the (b) (7)(E) did not address NIST 800-53, Rev. 4 privacy controls, including the following:

- AP-1 Authority to Collect
- AP-2 Purpose Specification
- AR-1 Governance and Privacy Program
- AR-2 Privacy Impact and Risk Assessment
- AR-3 Privacy Requirements
- AR-5 Privacy Awareness and Training
- AR-7 Privacy Enhanced System Design and Development
- DI-1 Data Quality
- DM-1 Minimization of PII
- TR-1 Privacy Notice

The Bank has not followed its own policies and federal requirements to document and implement all applicable NIST controls for (b) (7)(E). Additionally, this cloud based application has not had the applicable NIST SP 800-53 Rev. 4 controls addressed by the third-party service provider. Their controls have not been addressed by Bank as well. Without appropriate selection and documentation of controls, management may be unaware of potential risks to their environment.

NIST provides the following guidance related to SSPs:

NIST SP 800-53, Rev. 4, PL-2, System Security Plan, states:

Control: The organization:

- a. *Develops a security plan for the information system that:*
 - 1) *Is consistent with the organization's enterprise architecture;*
 - 2) *Explicitly defines the authorization boundary for the system;*
 - 3) *Describes the operational context of the information system in terms of missions and business processes;*
 - 4) *Provides the security categorizations of the information system including supporting rationale;*
 - 5) *Describes the operational environment for the information system and relationships with or connections to other information systems;*
 - 6) *Provides an overview of the security requirements for the system;*
 - 7) *Identifies any relevant overlays, if applicable;*
 - 8) *Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and*
 - 9) *Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;*

- b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];
- c. Reviews the security plan for the information system [Assignment: organization-defined frequency];
- d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementations or security control assessments; and
- e. Protects the security plan from unauthorized disclosure and modification.

Recommendation, Management’s Response, and Evaluation of Management’s Response

Recommendation 1:

We recommend that the Ex-Im Bank CIO update the (b) (7)(E) to identify and document all applicable NIST SP 800-53, Rev. 4 controls.

Management’s Response:

Management agrees with this recommendation. The Bank has completed the work required to update the (b) (7)(E) to the NIST SP 800-53, Rev. 4 security controls. (b) (7)(E) is hosted in a private cloud by (b) (7)(E) under an existing FEDRamp certification document that is equivalent to NIST SP 800-53, Rev. 3. The Bank will proceed to revise the (b) (7)(E) to the applicable (b) (7)(E), recognizing that completing this effort before (b) (7)(E) releases its own updated FEDRamp documentation will result in duplication of effort for all shared security controls. This effort will be completed by March 1, 2016.

Evaluation of Management’s Response:

If implemented properly, we believe that the process management has defined above, which is in addition to (b) (7)(E) updated FEDRamp documentation, can adequately ensure that the Bank’s (b) (7)(E) appropriately addresses NIST SP 800-53, Rev. 4 requirements.

Finding: Ex-Im Bank Should Improve Controls over Configuration Management

Controls are not adequate to ensure that Ex-Im Bank has documented configuration management plans for all of its systems that address configuration management requirements. Specifically, we noted that no configuration management plans were provided for the (b) (7)(E). The Bank stated that plans did exist; however, the plans were not consistently updated or were outdated. As a result, the Bank would not provide the plans to the auditors. Without appropriate configuration management plans that address how to move changes through change management

processes; how to update configuration settings and baselines; how to maintain information system component inventories; how to control development, test, and operational environments; and how to develop, release, and update key documents; the Bank may be susceptible to unauthorized and malicious system changes.

NIST provides the following guidance related to configuration management:

NIST SP 800-53, Rev. 4, CM-9, Configuration Management Plan, states:

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

- a. Address roles, responsibilities, and configuration management processes and procedures;*
- b. Establish a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;*
- c. Define the configuration items for the information system and places the configuration items under configuration management; and*
- d. Protect the configuration management plan from unauthorized disclosure and modification.*

Recommendation, Management's Response, and Evaluation of Management's Response

Recommendation 2:

We recommend that the Ex-Im Bank CIO document configuration management plans for the (b) (7)(E) systems respectively, that:

- a. Address roles, responsibilities, and configuration management processes and procedures.
- b. Establish a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
- c. Define the configuration items for the information system and place the configuration items under configuration management.
- d. Protect the configuration management plan from unauthorized disclosure and modification.

Management's Response:

Management agreed with this recommendation. IT management is updating the configuration management (CM) policy and procedures to reflect current best practices. This includes CM for application development, in addition to the (b) (7)(E)

Additionally, the Bank has retired its legacy CM tools, (b) (7)(E)

(b) (7)(E) and replaced them with the best of breed, (b) (7)(E) respectively. These changes will enhance interoperability and data exchange, flexibility of workflow reporting, and asset and version management throughout the life cycle of the asset or system. This effort will be completed by May 1, 2016.

Evaluation of Management's Response:

If implemented properly, we believe that the process management has defined above for remediating this issue can adequately ensure that the Bank has documented and implemented configuration management plans for the (b) (7)(E) systems.

Finding: Ex-Im Bank Should Improve Controls over Its Plan of Action & Milestones Process

Controls are not adequate to ensure that appropriate POA&M management controls are in place. Specifically, we noted the following:

- For the (b) (7)(E), the Bank had not started addressing POA&Ms (b) (7)(E), and the scheduled completion dates passed with no milestone updates.
- For the (b) (7)(E), the Bank had not started addressing POA&M (b) (7)(E), and the scheduled completion date passed with no milestone updates.

We found that the Bank was not adequately following up on POA&M items to ensure that they were remediated in a timely manner. Without adequate POA&M management, the Bank may remain exposed to known vulnerabilities that could be exploited by internal and external threats.

NIST provides the following guidance related to POA&M management:

NIST SP 800-53, Rev. 4, CA-5, *Plan of Action & Milestones*, states:

Control: The organization:

- 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*
- 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.*

NIST SP 800-53, Rev. 4, *PM-4, Plan of Action & Milestones Process*, states:

Control: The organization:

a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:

1. Are developed and maintained;

2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and

3. Are reported in accordance with OMB FISMA reporting requirements.

b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Recommendation, Management's Response, and Evaluation of Management's Response

Recommendation 3:

We recommend that the Ex-Im Bank CIO implement a process to ensure that all system POA&Ms are reviewed on an organization-defined frequency and that milestones are updated to reflect actions taken to remediate POA&M items.

Management's Response:

Management agreed with the recommendation. Over the past year, the Bank has replaced retired IT managers (on both the Government and the contractor side) with new managers and started building a new management framework. Part of this process is identifying roles and responsibilities and ensuring ownership of projects and activities for meeting goals and schedules. POA&M planning for FY 2016 is a major initiative, including POA&M assignment, resource allocation, and meeting schedules for remediation. This effort is ongoing. Additionally, POA&M ^{(b) (7)(E)} for the (b) (7)(E) has been updated to reflect the fact that the Bank needs to replace its current (b) (7)(E) with a (b) (7)(E) that meets the Bank's requirements. Until a replacement (b) (7)(E) (b) (7)(E) is in place, this POA&M will remain in an indefinite status, as it depends on the availability of a (b) (7)(E) system that meets all of the Bank's requirements. The POA&M for these four activities will be revised by February 1, 2016.

Evaluation of Management's Response:

If implemented properly, we believe that the process management has defined above for remediating this issue can adequately ensure that the Bank reviews and updates system POA&Ms in a timely manner.

Finding: Ex-Im Bank Should Improve Controls over Continuity of Operations

Controls are not adequate to ensure that the Bank performed appropriate contingency planning activities in FY 2015. Specifically, we found that in FY 2015, the Bank did not perform its annual continuity of operations plan (COOP) exercise that validates the Bank's ability to continue operations in the event of a disaster. The Bank stated that due to a lapse in its authority, resource constraints and re-prioritization prevented it from coordinating and executing the plan. Without validation of COOP capabilities, the Bank may not be aware of the plan's effectiveness or potential weaknesses that require remediation. Additionally, there is an increased risk that the Bank will be unable to perform its mission in the event that systems are unavailable for extended periods of time.

NIST provides the following guidance related to POA&M management:

NIST SP 800-53, Rev. 4, CP-4, Contingency Plan Testing, states:

Control: The organization:

- a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;*
- b. Reviews the contingency plan test results; and*
- c. Initiates corrective actions, if needed.*

Recommendation, Management's Response, and Evaluation of Management's Response

Recommendation 4:

We recommend that the Ex-Im Bank CIO ensure that testing of the COOP plan is performed on an annual basis to ensure that the Bank is prepared to continue operations and appropriately respond to potential disasters.

Management's Response:

Management agrees with this recommendation. However, management would like to emphasize that due to a lapse in the Bank's full authority on June 30, 2015, a full COOP exercise in FY 2015 was not feasible and, therefore, did not occur. Eagle Horizon 2015 (FEMA's Government-wide annual COOP exercise) was only a tabletop exercise and included the senior executive management of each agency. As such, it was not designed to provide a complete full-scale COOP exercise for any agency, and if Bank executive management had participated in this exercise, it still would not have met the expectations associated with this OIG recommendation. The period of time for this COOP exercise was the time leading up to and including the lapse of the Bank's full authority. Management

does not expect a repeat of this situation in the current fiscal year, given the reauthorization of the Bank on December 4, 2015.

The Bank did conduct the annual Disaster Recovery (DR) exercise in April 2015 for (b) (7)(E) and for the Bank's COOP/DR site (b) (7)(E) in July 2015. A full COOP exercise because it included all IT systems required for the COOP were exercised in the DR exercise ((b) (7)(E)) and the Bank intends to conduct a full COOP/DR exercise as conducted in prior years. This will be completed by July 2016.

Evaluation of Management's Response:

If implemented properly, we believe that the process management has defined above for remediating this issue can adequately ensure that the Bank performs annual COOP testing.

Federal Laws, Regulations, Policies, and Guidance

As part of our tests of internal controls, we reviewed Ex-Im Bank's compliance with applicable federal laws and regulations related to information security, including but not limited to:

- Federal Information Security Modernization Act of 2014
- The Council of the Inspectors General for Integrity and Efficiency (CIGIE) Information Security Continuous Monitoring Maturity Model for FY 2015
- FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.2
- NIST SPs and FIPS, particularly:
 - SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
 - SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
 - SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*
 - SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
 - SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*
 - SP 800-60, Rev. 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*
 - SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*
 - FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*

Prior Coverage

The following table shows the status of all prior-year audit findings and recommendations, including the year of initial discovery and the current status. All re-issued items are addressed in detail in the “Results” section of the report.

<u>Finding</u>	<u>Recommendation</u>	<u>FY Identified</u>	<u>FY 2015 Status</u>
<p>Controls are not adequate to ensure that Ex-Im Bank conducts Security Assessment and Authorization (SA&A) activities in accordance with agency and NIST requirements. Specifically, we noted that Ex-Im Bank implemented a secure wireless network within the Bank without first conducting required SA&A activities, including identifying, documenting, and testing affected security controls; performing a risk assessment to identify, mitigate and/or accept risks introduced into the environment; and obtaining official authority to operate from the authorization official based on the completion of the SA&A.</p>	<p>We recommend that the Ex-Im Bank CIO:</p> <ol style="list-style-type: none"> 1. Follow the established security assessment and authorization policy and procedures document, as well as implement and test security controls over the wireless implementation. 2. Develop policies and procedures over the use of and access to the wireless network. 	2013	Closed
<p>Controls are not adequate to ensure that known vulnerabilities are effectively tracked and remediated in a timely fashion. Specifically, we noted 40 moderate-level vulnerabilities found in Ex-Im Bank scans that management was not formally tracking to remediation. Of the 40 vulnerabilities, 24 were commonly known vulnerabilities ranging from 1-10 years of age since identification by NIST’s National Vulnerability Database (NVD). We noted that management is planning to remediate 7 of the 24 vulnerabilities as a result of our inquiry. The remaining 17 of the 24 vulnerabilities were determined to be false positives or vulnerabilities that management did not intend to address; however, we noted</p>	<p>We recommend that the CIO update the existing vulnerability management policies and procedures to address tracking, assessing, and remediating moderate-level vulnerabilities.</p>	2014	Closed

<u>Finding</u>	<u>Recommendation</u>	<u>FY Identified</u>	<u>FY 2015 Status</u>
that Ex-Im Bank had not documented formal acceptance of these issues prior to our testing.			
<p>During our FY 2012 testing, we found that Ex-Im Bank had not developed and documented a plan for the implementation of PIV cards as the common means of authentication for access to the agency's facilities, networks, and information systems, as directed in OMB-M-11-11. In addition, Ex-Im Bank was not employing PIV multifactor authentication mechanisms for users connecting to the Bank's networks internally. The CIO stated that action had not been taken to implement PIV access to Ex-Im Bank's internal network due to other priorities. Given that a plan had not been developed for PIV implementation, the date for upgrading the network's acceptance for its use was unknown. During our FY 2013 testing, we noted that Ex-Im Bank had developed a plan for the implementation and use of PIV cards to achieve multifactor authentication for access to the Ex-Im Bank network, and had rolled out a pilot program to begin the implementation. However, this program is still in the testing phase, and has not been deployed throughout the agency. For FY 2015, we found that the Bank had completed PIV implementation for logical access for Bank employees; however, this was not fully rolled out until the end of the fiscal year, in September 2015. We also found that the Bank had not yet fully implemented PIV access for all contractors accessing the Bank's networks. Until Ex-Im Bank has fully implemented the use of PIV cards, it will not be in compliance with OMB</p>	<p>We recommended that the CIO fully implement the use of PIV cards to achieve multifactor authentication to the Ex-Im Bank network for all access, as required by OMB M-11-11.</p>	<p>2012</p>	<p>Re-Issued</p>

<u>Finding</u>	<u>Recommendation</u>	<u>FY Identified</u>	<u>FY 2015 Status</u>
requirements and will have an increased risk of unauthorized access.			
Controls are not adequate to ensure that Ex-Im Bank has implemented effective account management processes for the (b) (7)(E).	<p>We recommend that the Ex-Im Bank CIO:</p> <ol style="list-style-type: none"> 1. Ensure that the account review process is conducted in accordance with organizational policies and procedures. 2. Ensure that inactive accounts are disabled after a period of 90 days, in accordance with organizational policy and procedures. 3. Ensure that accounts for terminated individuals are removed immediately upon separation. 	2013	Re-Issued
Controls are not adequate to ensure that Ex-Im Bank data accessible from (b) (7)(E) is adequately protected. In FY 2015, we noted that the Bank has acquired software that will allow it to enforce (b) (7)(E) (b) (7)(E)	<p>We recommended that the Ex-Im Bank CIO deploy (b) (7)(E) :</p> <ul style="list-style-type: none"> • (b) (7)(E) • (b) (7)(E) • (b) (7)(E) 	2014	Re-Issued
In our FY 2014 FISMA audit report, we found that controls were not adequate to	We recommended that the Ex-Im Bank CIO:	2014	Re-Issued

<u>Finding</u>	<u>Recommendation</u>	<u>FY Identified</u>	<u>FY 2015 Status</u>
<p>ensure that (b) (7)(E) from the Ex-Im Bank network in accordance with Ex-Im Bank policy. Specifically, we found:</p> <ul style="list-style-type: none"> • (b) (7)(E) • (b) (7)(E) • (b) (7)(E) <p>During our FY 2015 testing, we noted that, while the above weaknesses were remediated, controls over (b) (7)(E) (b) (7)(E)</p>	<ol style="list-style-type: none"> 1. Ensure that (b) (7)(E) policies and settings are appropriately configured and implemented. 2. (b) (7)(E) to ensure that they are appropriately operating as intended. 		

Management Comments



EXPORT-IMPORT BANK
OF THE UNITED STATES

January 15, 2016

Michael McCarthy
Deputy Inspector General
Office of the Inspector General
Export-Import Bank of the United States
811 Vermont Avenue NW
Washington, DC 20571

Dear Deputy Inspector General McCarthy,

Thank you for providing the Export-Import Bank of the United States (“EXIM” or “the Bank”) Management with the Office of the Inspector General’s (OIG) “Independent Audit of the Export-Import Bank’s Information Security Program for Fiscal Year 2015” (OIG-AR-16-0x, January, 2016) (“FISMA”). Management appreciates OIG’s acknowledgment that the Bank continues to improve and strengthen its information security program and is addressing the challenges in each of the areas that the Office of Management and Budget identified for the fiscal year 2015 FISMA review. The Bank continues to support the OIG’s work which complements the Bank’s efforts to continually improve its processes. The Bank is proud of the strong and cooperative relationship it has with the OIG.

The Bank is committed to full cooperation with the OIG and will work with staff on implementing all four recommendations that resulted from this audit. Cotton and Company LLP conducted the independent audit on behalf of the Bank’s OIG and made the following four new recommendations:

Recommendation 1: We recommend that the EXIM Bank CIO update the (b) (7)(E) to identify and document all applicable NIST SP 800-53 rev. 4 controls.

Management Response: Management agrees with this recommendation. The Bank has completed the work required to update the (b) (7)(E) to the NIST SP 800-53 Revision 4 security controls. (b) (7)(E) is hosted in a private cloud by (b) (7)(E) under an existing FEDRamp Provisional Authorization to Operate (ATO) and as such is grandfathered under FEDRamp certification documentation which is equivalent to NIST SP 800-53 Revision 3. The Bank will proceed to revise the (b) (7)(E) to the applicable Revision 4 security controls with the recognition that completing this effort before (b) (7)(E) releases their own updated FEDRamp documentation will result in the duplication of effort for all shared security controls. This effort will be completed by March 1, 2016.

Recommendation 2: We recommend that the EXIM Bank CIO document configuration management plans for the (b) (7)(E) and (b) (7)(E) systems respectively, that:

- a. Addresses roles, responsibilities, and configuration management processes and procedures;
- b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
- c. Defines the configuration items for the information system and places the configuration items under configuration management; and
- d. Protects the configuration management plan from unauthorized disclosure and modification.

Management Response: Management agrees with this recommendation. IT management is updating configuration management (CM) policy and procedures to reflect current best practices. This includes CM for application development, in addition to (b) (7)(E) and the (b) (7)(E). Additionally, the Bank has retired its legacy CM tools, Remedy and ClearQuest/ClearCase and replaced them with best of breed, (b) (7)(E) (b) (7)(E), respectively. These changes will enhance interoperability and data exchange, more flexible workflow and reporting, and asset and version management throughout the life cycle of the asset or system. This effort will be completed by May 1, 2016.

Recommendation 3: We recommend that the EXIM Bank CIO implement a process to ensure that all system POA&Ms are reviewed on an organization-defined frequency and those milestones are updated to reflect actions taken to remediate POA&M items.

Management Response: Management agrees with this recommendation. The past year the Bank has replaced retired IT managers (on both the Government and the Contractor side) with new managers and started building a new management framework. Part of this process is identifying roles and responsibilities and ensuring ownership of projects and activities and for meeting goals and schedules. POA&M planning for FY2016 is a major initiative including POA&M assignment, resource allocation, and meeting schedules for remediation. This effort is ongoing. Additionally, POA&M (b) (7)(E) or the (b) (7)(E), has been updated to reflect the fact that the Bank needs to replace its current (b) (7)(E) system (b) (7)(E) with a (b) (7)(E) that meets the Bank's requirements. Until a replacement (b) (7)(E) system is in place, this POA&M will remain in an indefinite status as there is a dependency on the availability of a (b) (7)(E) system that meets all of the Bank's requirements. The POA&M for these four activities will be revised by February 1, 2016.

Recommendation 4: We recommend that the EXIM Bank CIO ensure that testing of the COOP plan is performed on an annual basis to ensure that the Agency is prepared to continue operations and appropriately respond to potential disasters.

Management Response: Management agrees with this recommendation. However, management would like to emphasize that due to a lapse in the Bank's full authority on June 30, 2015, a full COOP exercise in FY 2015 was not feasible and, therefore, did not occur. Eagle Horizon 2015

(FEMA's Government-wide annual COOP exercise) was a tabletop exercise only to include the senior executive management of each Agency. As such, it was not designed to provide a complete full-scale COOP exercise for any Agency and if the Bank executive management had participated in the tabletop exercise for the Bank, it would still not have met the expectations associated with this OIG recommendation. The period of time for this COOP exercise was the time leading up to and including the lapse of the Bank's full authority. Management does not expect a repeat of this situation in the current fiscal year, given the reauthorization of the Bank on December 4, 2015.

The Bank did conduct the annual Disaster Recovery (DR) exercise in April 2015 for (b) (7)(E) and for (b) (7)(E) in July 2015. A full COOP exercise because all IT systems required for COOP were exercised in the DR exercise (b) (7)(E) and the Bank intends to conduct a full COOP/DR exercise as conducted in prior years. This will be completed by July 2016.

In addition, Cotton and Company LLP (Cotton) re-issued four recommendations from prior year audits, noting any progress the Bank had made toward implementing those recommendations.

Cotton found that while the Bank has implemented personal identity verification (PIV) access for logical network authentication, this authentication is not currently being implemented agency-wide. The Bank appreciates Cotton noting in this audit that management made substantial progress in the implementation of PIV for logical system access. However, this audit found that not all contractors are using PIV cards for logical access as required by HSPD-12.

As of July 2015, the Bank issued PIV cards and implemented the mandate to authenticate to the Bank's network using a PIV and two-factor authentication to 97% of the Bank staff (employees and contractors). 100% of all privileged account users are authenticating to the Bank network using an assigned PIV. The majority of the staff who continue to use passwords to authenticate to the Bank network is comprised of short-term contractors with an onsite commitment of six months or less, as they are not issued PIVs. In reviewing the best means to achieve 100% of the Bank staff using an assigned PIV for two-factor authentication, EXIM management has decided to issue PIVs to all contractors who require access to the Bank network, regardless of duration. 100% of the Bank staff will be assigned a PIV and use the PIV for two-factor authentication to the Bank network by March 1, 2016.

Cotton also found that the FY 2013 recommendation regarding the need for better controls to ensure accounts are deactivated in a timely manner remains open.

As noted in previous responses to this recommendation, disabling accounts when they are no longer required depends on timely notification of employee and contractor separations. The Bank has comprehensive policy and procedures for account management in place for achieving this. In an effort to further the accomplishment of this goal, the Bank will ensure that 100% of all active network accounts that are not used for 30 days are automatically disabled. Reactivation of disabled accounts will be accomplished by valid users contacting the Helpdesk

and requesting reactivation. Procedures for implementing automatic disabling of accounts not used for 30 days will be completed by March 1, 2016.

Cotton's 2014 audit recommended that the Bank deploy (b) (7)(E) security controls. FY 2015 testing noted that the Bank has acquired software that will allow the enforcement of security controls on (b) (7)(E) (b) (7)(E)
(b) (7)(E)

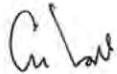
(b) (7)(E)

Cotton found that the FY 2014 recommendation to strengthen controls ensuring that (b) (4) (b) (7)(E) from the Bank's network in accordance with the Bank's policy remains open as such controls still need improvement. The Bank appreciates Cotton noting in this audit that all weaknesses of controls mentioned above identified in the FY 2014 audit were remediated. (b) (7)(E)
(b) (7)(E)

(b) (7)(E)

We thank the OIG for your efforts to ensure the Bank's policies and procedures continue to improve, as well as the work you do with us to protect EXIM funds from fraud, waste, and abuse. We look forward to strengthening our working relationship and continuing to work closely with the Office of the Inspector General.

Sincerely,



Charles J. Hall
Executive Vice President and Chief Operating Officer
Export-Import Bank of the United States

Selected Security Controls and Testing Results

800-53 Control	Control Title	Results
AC-2	Account Management	(b) (7)(E)
AC-5	Separation of Duties	(b) (7)(E)
AC-6	Least Privilege	(b) (7)(E)
AP-1	Authority to Collect	(b) (7)(E)
AP-2	Purpose Specification	(b) (7)(E)
AR-1	Governance and Privacy Program	(b) (7)(E)
AR-2	Privacy Impact and Risk Assessment	(b) (7)(E)
AR-3	Privacy Requirements	(b) (7)(E)
AR-5	Privacy Awareness and Training	(b) (7)(E)

800-53 Control	Control Title	Results
AR-7	Privacy Enhanced System Design and Development	(b) (7)(E)
AU-2	Auditable Events	(b) (7)(E)
AU-3	Content of Audit Records	(b) (7)(E)
AU-6	Review of Logs	(b) (7)(E)
DI-1	Data Quality	(b) (7)(E)
DM-1	Minimization of PII	(b) (7)(E)
PS-7	Third Party Personnel Security	(b) (7)(E)
SI-2	Flaw Remediation	(b) (7)(E)
TR-1	Privacy Notice	(b) (7)(E)
AC-18	Wireless Access	(b) (7)(E)
AC-19	Access Control for Mobile Devices	(b) (7)(E)
IA-2	Identification & Authentication	(b) (7)(E)
RA-2	Vulnerability Management	(b) (7)(E)

To Report Fraud, Waste, or Abuse, Please Contact:

Email: IGHotline@exim.gov

Telephone: 1-888-OIG-Ex-Im (1-888-644-3946)

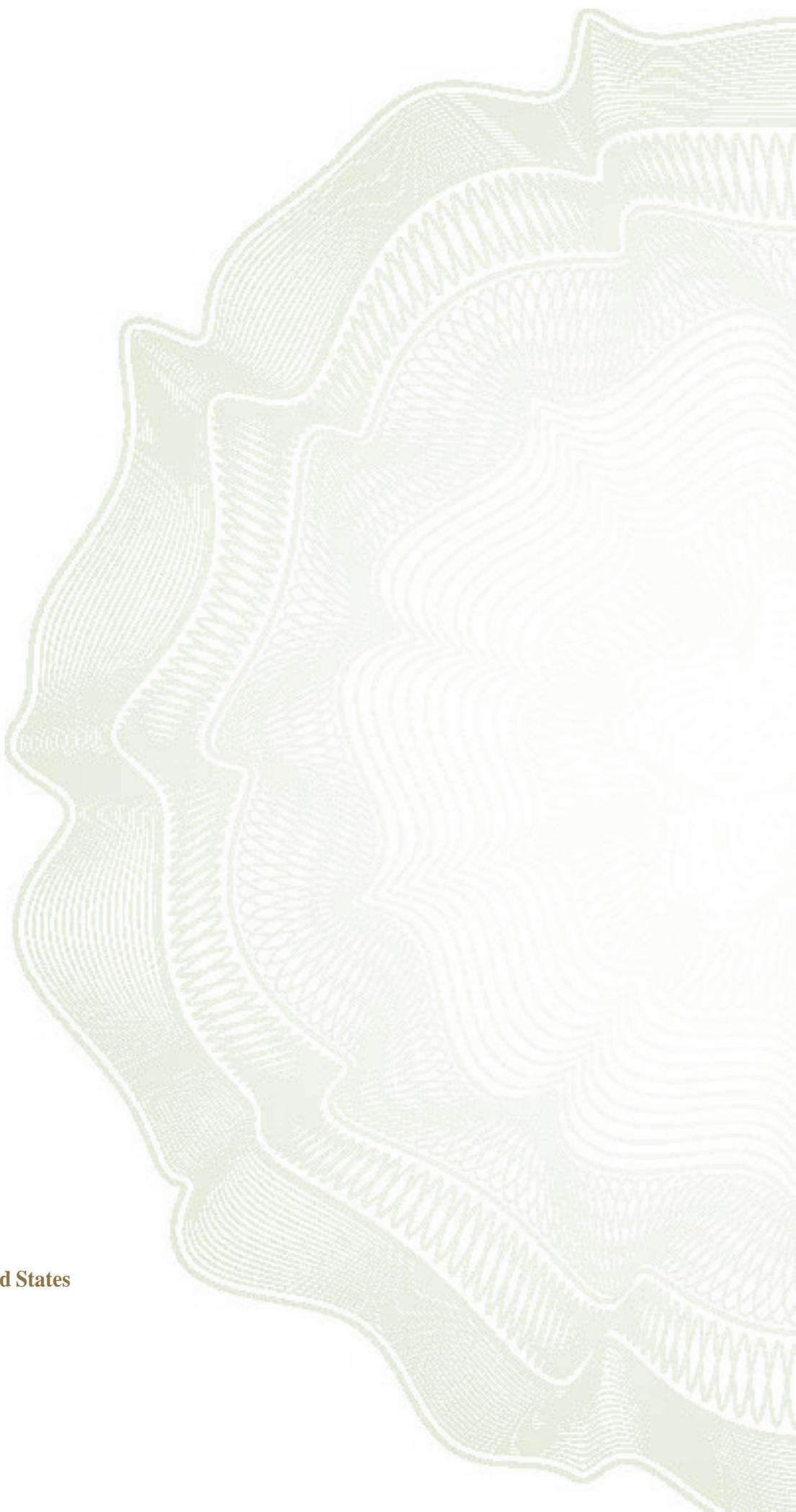
Fax: (202) 565-3988

Address: Office of Inspector General
Export-Import Bank of the United States
811 Vermont Avenue, NW
Suite 138
Washington, DC 20571

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, please contact Terry Settle, Assistant Inspector General for Audits, at Terry.Settle@exim.gov or call (202) 565-3498. Comments, suggestions, and requests can also be mailed to the attention of the Assistant Inspector General for Audits at the address listed above.





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