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

Independent Audit of Export-Import Bank's Information Security Program for Fiscal Year 2014

February 9, 2015
OIG-AR-15-03

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: 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 2014 (Report No. OIG-AR-15-03)

Date: February 9, 2015

This memorandum transmits Cotton & Company LLP's audit report of Export-Import Bank's (Ex-Im Bank) Information Security Program for Fiscal Year 2014. 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 adequate and effective information security policies, procedures, and practices in compliance with the Federal Information Security Management Act of 2002 (FISMA).

Cotton & Company determined that overall Ex-Im Bank is in substantial compliance with FISMA. Ex-Im 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 2014 FISMA review. However, Ex-Im Bank is not compliant with all FISMA requirements. The report contains three new recommendations and three 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: C.J. Hall, Executive Vice President and Chief Risk Officer
Michael Cushing, Senior Vice President and Chief Operating Officer
Audit Committee
John Lowry, Director, Information Technology Security and Systems Assurance
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

February 9, 2015

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

Subject: Independent Auditor's Report for Fiscal Year 2014 FISMA Compliance

Dear Ms. Settle:

We are pleased to submit this report in support of audit services provided pursuant to Federal Information Security Management 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 for the fiscal year ended September 30, 2014. Cotton & Company performed the work from May through November 2014.

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

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

C&A	Certification & Accreditation
CIO	Chief Information Officer
DHS	Department of Homeland Security
F&AS	Financial and Administrative System
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
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
PIV	Personal Identity Verification
SA&A	Security Assessment & Authorization
SP	Special Publications
FedRAMP	Federal Risk and Authorization Management Program

Executive Summary

OIG-AR-15-03
February 9, 2015

Independent Audit of Export-Import Bank's Information Security Program for Fiscal Year 2014

Why We Did This Audit

The Federal Information Security Management Act of 2002 (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, as well as an assessment of their compliance with FISMA. 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, and its overall compliance with FISMA requirements.

What We Recommended

We made three recommendations to further improve Ex-Im Bank's information security program and ensure compliance with FISMA requirements. Please see the 'Results' section, pages 4-16, for details regarding the recommendations. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

What Cotton & Company LLP Found

Overall, we found that Ex-Im Bank is in substantial compliance with FISMA. 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 Office of Management and Budget identified for the fiscal year 2014 FISMA review. During the past year, Ex-Im Bank rolled out a pilot program to begin the implementation of personal identity verification (PIV) card usage for logical system access. Additionally, Ex-Im Bank documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including those residing in the cloud. Furthermore, Ex-Im Bank defined and documented auditable events that systems are required to track, and implemented a security tool to parse through logs and report on specific events of interest. Ex-Im Bank also documented policies and procedures for accessing and using wireless technologies within the Bank's environment. Finally, Ex-Im Bank strengthened its tracking of security training to ensure that it retains evidence to show that individuals with specialized security roles have participated in required role-based training.

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

- While Ex-Im Bank has implemented multifactor authentication for remote access and has rolled out a pilot program for PIV access for multifactor network authentication, this authentication is not currently being implemented agency-wide, as required by HSPD-12. *(2012 and 2013 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 prior-year finding)*
- While Ex-Im Bank has documented policies and procedures for (b) (7)(E) , it has not yet completed a risk assessment of (b) (7)(E) to ensure that it has considered all risks associated with introducing this technology into its network. *(2013 prior-year finding)*
- Bank management has not implemented appropriate security controls over (b) (7)(E) .
- Bank management has not implemented (b) (7)(E) in compliance with established Bank policies.
- Bank management has not implemented an adequate vulnerability management program to ensure that (b) (7)(E) vulnerabilities identified are tracked, assessed, and remediated as appropriate.

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

TABLE OF CONTENTS

INTRODUCTION

Objective

This report presents the results of the Independent Audit of Export-Import Bank's Information Security Program for Fiscal Year 2014 conducted by Cotton & Company LLP. The objective was to determine whether Ex-Im Bank developed adequate and effective information security policies, procedures, and practices in compliance with the Federal Information Security Management Act of 2002 (FISMA).

Scope and Methodology

We performed the audit to determine whether Ex-Im Bank developed adequate and effective information security policies, procedures, and practices in compliance with FISMA requirements. Specifically, we evaluated Ex-Im Bank's security program, plans, policies, and procedures in place as of September 30, 2014, for compliance with applicable federal laws and regulations and guidance issued by OMB and National Institute of Standards and Technology (NIST). We performed a high-level review of each of the Bank's four major systems (F&AS, Infrastructure GSS, Ex-Im Online, and Oracle GSS) and performed detailed steps, as outlined in Office of Management and Budget (OMB) and Department of Homeland Security (DHS) FISMA questionnaire (OMB/DHS FISMA questionnaire), 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, (x) contractor system oversight, and (xi) security capital planning.

In addition, we assessed whether Ex-Im Bank had implemented selected minimum security controls from NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for its Infrastructure GSS, as required by FISMA. NIST 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 the GSS were chosen from selected security control families through a collaborative effort between the Ex-Im Bank OIG and Cotton & Company.

We conducted interviews 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 2014. 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 18, 2014 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 (Ex-Im Bank or the Bank) 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 provides 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 and Administrative System (F&AS)
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 includes the Federal Information Security Management Act of 2002 (FISMA). FISMA 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. The National Institute of Standards and Technology (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 Special Publications (SP). FIPS provides 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 provides 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 the 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.

RESULTS

The objective of this audit was to determine whether Ex-Im Bank developed adequate and effective information security policies, procedures, and practices in compliance with FISMA. Overall, we found that Ex-Im Bank is in substantial compliance with FISMA. Specifically, we noted that Ex-Im Bank continued to improve its information security program during fiscal year (FY) 2014. For example, the CIO:

- Rolled out a pilot program to begin the implementation of personal identity verification (PIV) card usage for logical system access.
- Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including those residing in the cloud.
- Defined and documented auditable events that systems are required to track, and implemented a security tool to parse through logs and report on specific events of interest.
- Documented policies and procedures for accessing and using wireless technologies within the Bank's environment
- Strengthened Ex-Im Bank's tracking of security training to ensure that it retains evidence to show that individuals with specialized security roles have participated in required role-based training.

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

- While Ex-Im Bank has implemented multifactor authentication for remote access and has rolled out a pilot program for PIV access for multifactor network authentication, this authentication is not currently being implemented agency-wide, as required by HSPD-12. *(2012 and 2013 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 period of specified inactivity. *(2013 prior-year finding)*
- While Ex-Im Bank has documented policies and procedures for (b) (7)(E) within the Bank's environment, it has not yet completed a risk assessment of (b) (7)(E) to ensure that it has considered all risks associated with introducing this technology into its network. *(2013 prior-year finding)*

- Bank management has not implemented appropriate security controls over (b) (7)(E)

- Bank management has not implemented (b) (7)(E) in compliance with established Bank policies.

- Bank management has not implemented an adequate vulnerability management program to ensure that (b) (7)(E) vulnerabilities identified are tracked, assessed, and remediated as appropriate.

We made three 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. We did not audit Ex-Im Bank management's responses, and accordingly, we express no opinion on them.

Finding: Ex-Im Bank Needs to 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 2014, we determined that Ex-Im Bank is not using multifactor authentication in accordance with federal requirements. During our testing, we noted that Ex-Im Bank had developed a plan for the implementation and use of PIV cards to achieve multifactor authentication. The Bank has rolled out a pilot program to begin the implementation, with several users actively using PIV cards to obtain logical access to the network; however, this program has not been fully deployed throughout the agency. Ex-Im's CIO stated that there were resource constraints that prevented full deployment. Until Ex-Im Bank has fully implemented the use of PIV cards, 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).*

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

Recommendation:

As of FY 2014, 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 status of prior year FISMA audit recommendations.

Finding: Ex-Im Bank Needs to Improve Controls over Infrastructure GSS Account Management

As initially identified in our FY2013 FISMA audit report, we found during our FY 2014 testing that controls remained inadequate to ensure that user accounts are deactivated in a timely manner. Specifically, we found the following issues:

- For (b) (7)(E) , we found that 1 out of 45 accounts remained active 49 days after the individual left the agency.
- For (b) (7)(E), we identified one account that was disabled 193 days after the individual left the agency, and another account that was disabled 68 days after the individual left the agency.
- For (b) (7)(E), we identified one account that was disabled 411 days after the individual left the agency, and another account that was disabled 441 days after the individual left the agency. Neither user had access to the Active Directory; however, their accounts should have been disabled in (b) (7)(E).
- For (b) (7)(E) , we identified one account that was disabled 89 days after the individual left the agency.

Ex-Im Bank is not carrying out its documented account management policy and procedures consistently. 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 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.

NIST provides the following guidance related to account management:

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

<u>Control</u>: 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 FY2013 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 FY2014, the recommendations noted remain open; therefore, we are not issuing any new recommendations related to this finding. See Appendix A for a complete status of prior year FISMA audit findings.

Finding: Ex-Im Bank Needs to Improve Controls over Security Assessment and Authorization

As initially identified in our FY2013 FISMA audit report, we found the controls to ensure that Ex-Im Bank conducts Security Assessment and Authorization (SA&A) activities in accordance with agency and NIST requirements remain inadequate. Specifically, we noted that Ex-Im Bank implemented (b) (7)(E) in FY2013 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.

During our FY2014 testing, we found that management had adequately identified, documented and tested affected security controls, as well as documented policies and procedures for (b) (7)(E) . However, while the Bank was in the process of performing a risk assessment, it was not completed by the end of the fiscal year. As a result, we are re-issuing this finding.

Although management has fully rolled out (b) (7)(E) , it has not completed an assessment of the risk that this additional technology introduces to the Bank's environment. Without performing an appropriate SA&A for new systems or significant changes, management may not have a clear understanding of the risks present in their environment, resulting in increased susceptibility to significant vulnerabilities.

NIST provides the following guidance related to security assessment and authorization:

NIST SP 800-53, Rev. 4, *CA-2, Security Assessments*, states:

> *<u>Control</u>: The organization:*
> *a. Develops a security assessment plan that describes the scope of the assessment including:*
> *- Security controls and control enhancements under assessment;*
> *- Assessment procedures to be used to determine security control effectiveness; and*
> *- Assessment environment, assessment team, and assessment roles and responsibilities;*
> *b. Assesses the security controls in the information system [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;*
> *c. Produces a security assessment report that documents the results of the assessment; and*
> *d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.*

NIST SP 800-53 Rev. 4, *CM-4, Security Impact Analysis*, states:

> *<u>Control</u>: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.*

(b) (7)(E)

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

Recommendation:

As of FY 2014, Ex-Im Bank only partially addressed our FY 2013 audit recommendation for the CIO to follow the established security assessment and authorization policy and procedures document, as well as implement and test security controls over (b) (7)(E) , and lastly, develop policies and procedures over (b) (7)(E) . This recommendation remains open; therefore, we are not issuing any new recommendations related to this finding. See Appendix A for a complete status of prior year FISMA audit recommendations.

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

Controls are not adequate to ensure that Ex-Im Bank data (b) (7)(E) is adequately protected. Specifically, we noted:

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

This weakness exists because management has not deployed a solution to implement security controls over (b) (7)(E)

Without proper security controls over (b) (7)(E), there is increased risk that (b) (7)(E) could be compromised or accessed by unauthorized individuals.

The following guidance is relevant for this control activity:

(b) (7)(E)

NIST SP 800-53, Rev. 4, *CM-11, User-Installed Software,* states:

> *Control: The organization:*
>
> *c. Establishes [Assignment: organization-defined policies] governing the installation of software by users;*
>
> *d. Enforces software installation policies through [Assignment: organization-defined methods]; and*
>
> *e. Monitors policy compliance at [Assignment: organization-defined frequency].*

NIST SP 800-53, Rev. 4, *SC-28, Protection of Information at Rest,* states:

> *Control: The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].*

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 1:

We recommend that the Ex-Im Bank CIO deploy (b) (7)(E) that:

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

Management's Response:

Management agrees with the recommendation. During the past year, the Bank's IT staff conducted market surveys of software products to perform the security functions identified in this audit report. The result of this effort was the selection of (b) (7)(E) to conduct a limited pilot test last summer. The pilot was successful and a contract was issued in September 2014 to purchase (b) (7)(E) for Bank wide use in (b) (7)(E) . The deployment of (b) (7)(E) has entered a planning and testing stage in support of (b) (7)(E) . The full deployment of (b) (7)(E) will address (b) (7)(E)

This effort will be completed by June 1, 2015.

Evaluation of Management's Response:

If implemented properly, we believe the process management has defined above for remediating this issue can adequately address (b) (7)(E)

.

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

Controls are not adequate to ensure that (b) (7)(E) in accordance with Ex-Im Bank policy. Specifically, we found:

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

This weakness exists because when Ex-Im Bank performed security testing and evaluation (ST&E) exercises, Bank personnel primarily used interviews to confirm control implementations, rather than performing detailed testing to assure that controls were in place and operating effectively. As a result, our testing revealed that management was unaware of this issue, and subsequent investigation revealed that (b) (7)(E)

Without (b) (7)(E) , 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)(E)

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

(b) (7)(E)

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

Recommendation 2:

We recommend that the Ex-Im Bank CIO:

1. Ensure that remote access policies and settings are appropriately configured and implemented.
2. Test all NIST SP 800-53 rev. 4 security controls to ensure that they are appropriately operating as intended

Management's Response:

Management agrees with this recommendation. We will be enhancing our continuous monitoring and testing to ensure the efficacy of (b) (7)(E) controls and compliance with policy. As regards (b) (7)(E) , the Bank continues to follow its documented policy, as quoted in the auditors ' report, of a (b) (7)(E) . There had been confusion as to whether the policy on (b) (7)(E) had been changed (b) (7)(E) , but this is not the case and it was never implemented.

(b) (7)(E)

We have already implemented this change for most users and will apply it to all users once we complete testing for all combinations of (b) (7)(E)

This work will be completed by February 1, 2015.

Evaluation of Management's Response:

If implemented properly, we believe the process management has defined above for remediating this issue can adequately address ensuring remote access policies and settings are appropriately configured.

Finding: Ex-Im Bank Needs to Improve Controls over Vulnerability Management

Controls are not adequate to ensure that known vulnerabilities are effectively tracked and remediated in a timely fashion. Specifically, we noted (b) (7)(E) vulnerabilities found in Ex-Im Bank scans that management was not formally tracking to remediation. Of the (b) (7)(E) vulnerabilities, (b) (7)(E) were commonly known vulnerabilities (b) (7)(E) We noted that management is planning to remediate (b) (7)(E) vulnerabilities as a result of our inquiry. The remaining (b) (7)(E) vulnerabilities were determined to be false positives or vulnerabilities that management did not intend to address; however, we noted that Ex-Im Bank had not documented formal acceptance of these issues prior to our testing.

This weakness exists because management does not have documented policies or procedures for tracking or remediating moderate-level vulnerabilities. The current process only requires tracking of critical and high-level vulnerabilities. Ex-Im Bank does not assess whether moderate-level vulnerabilities identified pose any additional risk to its environment.

Without an effective vulnerability management program in place, Ex-Im Bank systems and data are more susceptible to unauthorized access, modification, or destruction. In addition, without a formal process in place for regularly tracking and remediating known vulnerabilities, management's understanding of their current exposure to risk is likely inaccurate.

NIST provides the following guidance related to vulnerability management:

NIST SP 800-53, Rev. 4, *RA-5, Vulnerability Scanning,* states:

> *Control: The organization:*
> *a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;*

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

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

Recommendation 3:

We recommend that the CIO update the existing vulnerability management policies and procedures to address tracking, assessing, and remediating (b) (7)(E) vulnerabilities.

Management's Response:

Management agrees with the recommendation. The Bank is examining the workload imposed by closing all (b) (7)(E) vulnerabilities and availability of resources. The Bank will weigh the effort of closing (b) (7)(E) vulnerabilities against the value obtained, given that the Bank:

(b) (7)(E)

Based on the above, while (b) (7)(E) level vulnerabilities may exist in devices on the network, they may be largely theoretical given the general lack of an exploitable attack vector. Regardless, the Bank will examine these more closely and either close these

(b) (7)(E)vulnerabilities or make a risk-based assessment of which to pay more attention to for remediation. This will be completed by August 1, 2015.

Evaluation of Management's Response:

If implemented properly, we believe the process management has defined above for remediating this issue can adequately address tracking, assessing, and remediating (b) (7)(E) vulnerabilities.

APPENDIX A

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:

- E-Government Act of 2002 (FISMA and privacy provisions)
- FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- 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*
    - SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*
    - SP 800-63-2, *Electronic Authentication Guideline*
    - FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*

Prior Coverage

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

Finding	Recommendation	FY Identified	FY 2014 Status
Controls are not adequate to ensure that Ex-Im Bank has developed and documented policies and procedures for information security oversight of systems operated on the Bank's behalf by contractors or other entities. We found that Ex-Im Bank utilizes several externally hosted systems operated by the General Services Administration, Research in Motion, and Microsoft, but has not documented policies to ensure proper security oversight of these or any other externally hosted systems.	We recommend that the Ex-Im Bank CIO develop and document policies and procedures for information security oversight of externally hosted services and systems.	2013	Closed
Controls are not adequate to ensure that Ex-Im Bank has fully implemented audit logging and monitoring controls. Specifically, we found the following: • Ex-Im Bank has not clearly defined all auditable events and reviewed the list of events on a periodic basis. We noted vague auditable events such as "required audit records" and "standard syslog data" that do not clearly address risk or areas of concern specific to the GSS, and that are not clearly identified or defined in Ex-Im Bank policies. • While Ex-Im Bank is logging events, they have not clearly defined which events are appropriate to be logged for Ex-	We recommend that the Ex-Im Bank CIO: 1. Clearly define, document, and review a list of events required to be captured by the system. 2. Ensure audit logs are maintained or generated in an easily reviewable format. 3. Review audit logs on a periodic basis and take appropriate corrective action as necessary.	2013	Closed

Finding	Recommendation	FY Identified	FY 2014 Status
Im Bank's systems. Ex-Im Bank audit logs do not contain appropriate information to support an after-the-fact investigation. Specifically, we determined that, while Ex-Im Bank is capturing events, the logs are very voluminous and are currently presented in Notepad, which is not separated or broken down into an easily readable format. Ex-Im Bank personnel are not reviewing logs due to the current format. Ex-Im Bank has stated that they are currently transitioning to a new tool that will be capable of parsing through audit logs and compiling them into a reviewable report.			
Controls are not adequate to ensure that Ex-Im Bank is completing annual specialized security training for individuals with significant security responsibilities. Specifically, we found that one out of five individuals who were required to take specialized training had not taken it. Tracking efforts have therefore not been effective in ensuring that all required individuals take the necessary training.	We recommend that the Ex-Im Bank CIO ensure that all individuals with significant security responsibilities complete annual security training in accordance with Ex-Im Bank policies and procedures.	2013	Closed
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	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.	2012	Re-Issued

Finding	Recommendation	FY Identified	FY 2014 Status
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. Until Ex-Im Bank has fully implemented the use of PIV cards, it will not be in compliance with OMB 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) Specifically, we noted the following: • Ex-Im Bank is not consistently conducting account reviews to ensure that user access remains appropriate. The auditors were informed that contractors/temporary employees are not consistently reviewed for appropriate system access. These types of users are also not included in periodic termination notifications from Ex-Im Bank Human Resources.	We recommend 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.	2013	Re-Issued

Finding	Recommendation	FY Identified	FY 2014 Status
• Ex-Im Bank is not consistently disabling accounts that have been inactive for a period of 90 days. Specifically, we noted two accounts that were inactive for longer than 90 days and were not disabled. After follow-up, the auditors determined that 90 days is the threshold for following up on inactive accounts, not for disabling them. However, these accounts were not disabled per Ex-Im Bank policies. • Ex-Im Bank is not effectively disabling or deleting accounts when individuals leave the agency. Specifically, we noted that 1 out of 45 users had retained an active network account following termination. After follow-up, we determined that this account was meant to be retained only as a mailbox account and this account was not disabled per Ex-Im Bank policies.			
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 (b) (7)(E) 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	We recommend that the Ex-Im Bank CIO: 1. Follow the established security assessment and authorization policy and procedures document, as well as implement and test security controls over (b) (7)(E) . 2. Develop policies and procedures over (b) (7)(E)	2013	Re-Issued

Finding	Recommendation	FY Identified	FY 2014 Status
obtaining official authority to operate from the authorization official based on the completion of the SA&A.	(b) (7)(E)		

Management Comments

EXPORT-IMPORT BANK
OF THE UNITED STATES

January 23, 2014

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

Dear Inspector General McCarthy,

Thank you for providing the Export-Import Bank of the United States ("Ex-Im Bank" or "the Bank") Management with the Office of the Inspector General's (OIG) report on "Independent Audit of Export-Import Bank's Information Security Program for Fiscal year 2014" (OIG-AR-15-0x, January, 2015). Management appreciates and continues to support the OIG's work and audits which complement the Bank's efforts to continually improve its processes. Ex-Im Bank is proud of the strong and cooperative relationship it has with the OIG.

Cotton & Company LLP conducted the independent audit on behalf of the Bank's OIG and made the following three new recommendations:

Recommendation 1: We recommend that the Ex-Im Bank CIO deploy (b) (7)(E)
(b) (7)(E)

Management response: Management agrees with the recommendation. During the past year, the Bank's IT staff conducted market surveys of software products to perform the security functions identified in this audit report. The result of this effort was the selection of (b) (7)(E) to conduct a limited pilot test last summer. The pilot was successful and a contract was issued in September 2014 to purchase (b) (7)(E) for Bank wide use in (b) (7)(E)
(b) (7)(E) The deployment of (b) (7)(E) has entered a planning and testing stage in support of (b) (7)(E) The full deployment of (b) (7)(E) will address (b) (7)(E)
(b) (7)(E)

811 VERMONT AVENUE, N.W. WASHINGTON, D.C. 20571

(b) (7)(E) This effort will be completed by June 1, 2015.

Recommendation 2: We recommend that the Ex-Im Bank CIO:

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

Management response: Management agrees with this recommendation. We will be enhancing our continuous monitoring and testing to ensure the efficacy of (b) (7)(E) (b) (7)(E) compliance with policy. As regards the (b) (7)(E) (b) (7)(E), the Bank continues to follow its documented policy, as quoted in the auditors' report, of (b) (7)(E) There had been confusion as to whether the policy on (b) (7)(E) had been changed to (b) (7)(E), but this is not the case and it was never implemented.

Finally, we have altered and implemented a change in our (b) (7)(E) security policy, due to (b) (7)(E)

(b) (7)(E) This work will be completed by February 1, 2015.

Recommendation 3: We recommend that the CIO update the existing vulnerability management policies and procedures to address tracking, assessing, and remediating (b) (7)(E) vulnerabilities.

Management response: Management agrees with the recommendation. The Bank is examining the workload imposed by closing all (b) (7)(E) vulnerabilities and availability of resources. The Bank will weigh the effort of closing (b) (7)(E) vulnerabilities against the value obtained, given that the Bank:

(b) (7)(E)

(b) (7)(E)

Regardless, the Bank will examine these more closely and either close these (b) (7)(E) vulnerabilities or make a risk-based assessment of which to pay more attention to for remediation. This will be completed by August 1, 2015.

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

Cotton and Company found that the Bank, although using a pilot program to implement the use of PIV cards to achieve multi-factor authentication to the Bank's network for all access, still needed to fully implement the use of PIV cards Bank-wide. The Bank's management continues to move towards implementing this recommendation.

On October 21, 2014, Ex-Im Bank's Enterprise Risk Committee (ERC), comprised of key members of the Bank's senior staff, was briefed on the PIV requirement and approved a recommendation for implementation of two-factor authentication using PIV cards. While a revised implementation plan is under preparation, the Bank's goal is to implement two-factor authentication using PIVs to the Bank's network for all users by the end of fiscal year 2015. The Bank has HSPD-12 PIV cards deployed to all employees and contractors and continues to use two-factor authentication using RSA tokens and Radius server for remote access to the Bank's network. Additionally, the Bank increased the number of Bank users enabled with two-factor authentication using their PIV card and has pilot tested the use of PIV cards in conjunction with Adobe Acrobat Pro for internal use to electronically sign documents within the Office of the CFO.

Cotton & Company also found that the FY 2013 recommendation regarding the need for better controls to ensure accounts are deactivated in a timely manner remains open and identified additional issues found during this audit.

(b) (7)(E)

(b) (7)(E) In three of these five cases, the separated users would not have the ability to access the application because the

(b) (7)(E) account was disabled on a timely basis and the applications are not accessible without an active (b) (7)(E) account. In the other two cases, the Bank verified that these accounts were not used since the employee separated. In reviewing each of the six accounts the Bank concluded that none of these accounts were used after the separation date of the user.

In the case of the one (b) (7)(E) account that was not terminated on a timely basis, Bank staff will work with the OIG to obtain timely notification of separations, as this user was an OIG intern. Bank staff will also determine why this (b) (7)(E) user account was not automatically disabled; however, it was identified in the Bank's monthly (b) (7)(E) account review (a manual spreadsheet-assisted process), which flags an account for inspection only after it has been inactive for 90 days. This account was inactive for 49 days. Absent the identification of any specific defect in the Bank's account management process, the Bank will examine greater awareness on the receipt of timely notifications of employee and contractor separations from the Bank. This effort will be completed by August 1, 2015.

Cotton and Company found in FY 2013 that the Bank needed to improve controls over security assessment and authorization. The Bank appreciates Cotton and Company noting in this audit that management has adequately identified, documented and tested affected security controls as well as documented policies and procedures for (b) (7)(E) In addition, they noted that the Bank had not completed its risk assessment for additional technology introduced to the Bank.

The Bank completed a thorough vulnerability and risk assessment of the (b) (7)(E) (b) (7)(E) in September 2014 and the report of the assessment was completed in October. The report has been provided to the auditors for their review.

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 Ex-Im funds from fraud, waste, and abuse. We look forward to continuing to work closely with the Office of the Inspector General.

Sincerely,

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

APPENDIX C

Selected Security Controls and Testing Results

800-53 Control	Control Title	Results
AC-2	Account Management	(b) (7)(E)
AC-19	Access Control For Mobile Devices	(b) (7)(E)
AT-2	Security Awareness Training	(b) (7)(E)
AU-6	Audit Review, Analysis, And Reporting	(b) (7)(E)
CP-2	Contingency Plan	(b) (7)(E)
CP-4	Contingency Plan Testing	(b) (7)(E)
CM-11	User-Installed Software	(b) (7)(E)
MP-5	Media Transport	(b) (7)(E)
MP-6	Media Sanitization	(b) (7)(E)
MP-7	Media Use	(b) (7)(E)
SA-7	User-Installed Software	(b) (7)(E)
SC-8	Transmission Confidentiality And Integrity	(b) (7)(E)
SC-28	Protection Of Information At Rest	(b) (7)(E)
SC-13	Use Of Cryptography	(b) (7)(E)
SI-8	Spam Protection	(b) (7)(E)

800-53 Control	Control Title	Results
PM-5	Information System Inventory	(b) (7)(E)
PM-9	Risk Management Strategy	(b) (7)(E)
PM-11	Mission/Business Process Definition	(b) (7)(E)
PM-12	Insider Threat Program	(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, Acting 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