EXIM
EXPORT-IMPORT BANK
OF THE UNITED STATES

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

Independent Audit of the Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2017

March 8, 2018
OIG-AR-18-04

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, Senior Vice President and Chief Information Officer

From: Erica Wardley, Acting Assistant Inspector General for Audits EW

Subject: Independent Audit of Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2017 (OIG-AR-18-04)

Date: March 8, 2018

This memorandum transmits Cotton & Company LLP's (Cotton & Company) audit report on Export-Import Bank's (EXIM Bank) Information Security Program for Fiscal Year 2017. 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 EXIM 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 while EXIM Bank has addressed several of the challenges identified during previous FISMA audits, its information security program and practices are not effective overall when assessed against revised Department of Homeland Security (DHS) reporting metrics. EXIM Bank has not effectively implemented a mature information security program. The report contains one new recommendation 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) 565-3693 or Erica.Wardley@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/about/oig.

cc: Scott P. Schloegel, First Vice President and Vice Chairman of the Board (Acting)
Kevin Turner, Senior Vice President and General Counsel
Jeff Goettman, Executive Vice President and Chief Operating Officer
Jessie Law, Senior Vice President, Chief of Staff and
White House Liaison
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Inci Tonguch-Murray, Acting Senior Vice President and Chief Financial Officer
David Sena, Senior Vice President of Board Authorized Finance
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 21, 2018

Erica Wardley
Acting Assistant Inspector General for Audits
Export-Import Bank of the United States
811 Vermont Avenue, NW
Washington, DC 20571

Subject: Independent Audit of the Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2017

Dear Ms. Wardley:

We are pleased to submit this report in support of audit services provided pursuant to Federal Information Security Modernization Act of 2014 (FISMA) requirements. Cotton & Company LLP conducted an independent performance audit of the effectiveness of Export-Import Bank of the United States' (EXIM Bank's) information security program and practices for the fiscal year ending September 30, 2017. Cotton & Company performed the work from May through December 2017.

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.

This report is intended solely for the information and use of the Export-Import Bank of the United States, and is not intended to be and should not be used by anyone other than these specified parties.

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 (EXIM Bank) is the official export credit agency of the United States. EXIM Bank is an independent, self-sustaining executive agency and a wholly-owned U.S. government corporation. EXIM Bank's mission is to support jobs in the United States by facilitating the export of U.S. goods and services. EXIM 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 EXIM Bank, was statutorily created in 2002 and organized in 2007. The mission of the EXIM 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.

This audit was conducted in accordance with generally accepted government auditing standards. 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.

EXECUTIVE SUMMARY

Audit of EXIM Bank's Information Security Program Effectiveness for Fiscal Year 2017
OIG-AR-18-04, March 8, 2018

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 and practices 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's (EXIM Bank or the Bank's) information security program and practices.

What We Recommend

We partially reissued three recommendations and made one new recommendation for the Chief Information Officer to (1) implement procedures to evaluate and improve the maturity and effectiveness of the Bank's information security program, (2) improve vulnerability management, (3) adequately document and implement baseline configuration settings for information technology (IT) products, and (4) develop and implement a monitoring and auditing process that identifies and remediates gaps in the Bank's information assurance control implementation and that validates compliance with the Bank's privacy and awareness training program.

What Cotton & Company LLP Found

EXIM Bank's information security program and practices are not effective overall when assessed against revised Department of Homeland Security (DHS) reporting metrics, although we noted that EXIM Bank has addressed several of the challenges identified during previous FISMA audits. During the past year, EXIM Bank improved processes over ensuring that agreements with third-party service providers adequately address security responsibilities; implemented appropriate access management controls before granting users access to systems; updated and implemented effective role-based security training; improved controls around shared system accounts; implemented appropriate account management controls for the Application Processing System; and improved procedures for managing software licenses. However, when evaluating EXIM Bank against the current Office of Inspector General (OIG) DHS metrics, EXIM Bank has not effectively implemented a mature information security program. Specifically, it has not consistently implemented its current Configuration Management (CM), Identity and Credential Access Management (ICAM), Information Security Continuous Monitoring (ISCM), Incident Response, and Contingency Planning (CP) policies, plans, procedures, and strategies organization-wide, impacting the maturity and effectiveness of its overall information security program.

The fiscal year (FY) 2017 DHS metrics also marked a continuation of the work that the Office of Management and Budget (OMB), DHS, and Council of the Inspectors General on Integrity and Efficiency (CIGIE) undertook in FYs 2015 and 2016 to move the Inspector General (IG) assessments to a maturity model approach. DHS significantly revised the IG reporting metrics for agencies in FY 2017, which resulted in more rigorous evaluation criteria and requirements than in previous years. When evaluating EXIM Bank's information security program against the DHS FY 2017 IG FISMA metrics, which use a five-level maturity model scale, we found that the Identify domain scored at Level 4: Managed and Measurable, and is therefore considered effectively implemented. The remaining framework areas – Protect, Detect, Respond, and Recover – scored at Level 3 or below and are therefore considered ineffective, as stipulated by DHS's FY 2017 IG FISMA metrics. However, although the Respond and Recover domains did not meet Level 4 requirements, based on testing performed, we judgmentally determined that they were generally effective. EXIM Bank's overall score for its information security program was Level 3: Consistently Implemented. A summary of the results for the DHS FY 2017 IG FISMA Metric assessment is in Appendix E.

In addition, although the Bank effectively implemented 14 of the 18 NIST SP 800-53, Rev. 4 controls that we tested for the Infrastructure GSS, we identified several areas for improvement. Specifically, Bank management:

- Has not effectively implemented a vulnerability management program. *(2016 prior-year finding)*
- Has not effectively implemented baseline configurations and documented deviations for information technology (IT) products. *(2016 prior-year finding)*
- Has not effectively developed and implemented a monitoring and auditing process that identifies and remediates gaps in the Bank's information assurance control implementation and that validates compliance with the Bank's privacy and awareness training program.
- Did not consistently implement firewall rule capabilities at all Bank locations.

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY I
TABLE OF CONTENTS II
LIST OF FIGURES AND TABLES III
ABBREVIATIONS AND GLOSSARY IV
INTRODUCTION 1
SCOPE AND METHDOLOGY 1
BACKGROUND 2
AUDIT RESULTS 6

Finding: EXIM Bank Should Improve the Maturity of Its Information Security Program 7

Recommendation, Management's Response, and Evaluation of Management's Response 11

Finding: EXIM Bank Should Improve Controls over Its Vulnerability Management Program 11

Recommendation, Management's Response, and Evaluation of Management's Response 14

Finding: EXIM Bank Should Improve Controls over Baseline Configuration Implementation 15

Recommendation, Management's Response, and Evaluation of Management's Response 16

Finding: EXIM Bank Should Improve Controls over Information Assurance Monitoring. 17

Recommendation, Management's Response, and Evaluation of Management's Response 18

Finding: EXIM Bank Should Improve Controls over Firewall Capabilities Implementation 18

Recommendation, Management's Response, and Evaluation of Management's Response 20

CONCLUSION 20
APPENDICES 21

Appendix A: Federal Laws, Regulations, and Guidance 21

Appendix B: Prior Coverage 22

Appendix C: Management's Response 27

Appendix D: Selected Security Controls and Testing Results 31

Appendix E: DHS FY 2017 IG FISMA Metric Results 32

LIST OF FIGURES AND TABLES

Table 1. Aligning the Cybersecurity Framework Security Functions to the FY 2017 IG FISMA Metric Domains

Table 2. IG Assessment Maturity Levels

Table 3. Prior-Year Audit Finding Remediation Status

Table 4. Selected Security Controls and Testing Results

Table 5. EXIM Bank FY 2017 IG FISMA Metric Results

ABBREVIATIONS AND GLOSSARY

CIO	Chief Information Officer
CIGIE	Council of Inspectors General on Integrity and Efficiency
CRO	Chief Risk Officer
DHS	Department of Homeland Security
EOL	EXIM Online
FIPS	Federal Information Processing Standards
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
IG	Inspector General
IT	Information Technology
ISCM	Information Security Continuous Monitoring
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
ROB	Rules of Behavior
SP	Special Publication

INTRODUCTION

This report is intended solely for the information and use of the Export-Import Bank of the United States, and is not intended to be and should not be used by anyone other than these specified parties.

This report presents the results of the independent performance audit of the effectiveness of the information security program and practices of the Export-Import Bank (EXIM Bank or the Bank) for fiscal year (FY) 2017, conducted by Cotton & Company LLP. The objective was to determine whether EXIM Bank developed and implemented effective information security program and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA).

SCOPE AND METHODOLOGY

To determine whether EXIM Bank developed and implemented an effective information security program and practices as required by FISMA, we evaluated its security program, plans, policies, and procedures in place throughout FY 2017 as required by applicable federal laws and regulations and guidance issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). We performed a review of each of the Bank's four major systems (Financial Management System – Next Generation [FMS-NG], Infrastructure General Support System [GSS], EXIM Online, and (b) (7)(E)) and performed detailed steps, as outlined in the Department of Homeland Security (DHS) *FY 2017 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.0*, to evaluate EXIM Bank's policies, and procedures for key areas such as (i) risk management, (ii) contractor system, (iii) configuration management, (iv) identity and access management, (v) security and privacy training, (vi) information security continuous monitoring, (vii) incident response, and (viii) contingency planning.

In addition, we assessed whether EXIM Bank had implemented select minimum security controls from NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for its Infrastructure GSS, as required by Federal Information Processing Standards (FIPS) 200. 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 Infrastructure GSS were judgmentally chosen from selected security control families through a collaborative effort between the EXIM Bank Office of Inspector General (OIG) and Cotton & Company. Appendix D contains a complete list of NIST controls evaluated.

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

We conducted the audit onsite at EXIM Bank in Washington, DC, as well as remotely at the Cotton & Company office in Alexandria, VA, with fieldwork from May to December 2017. Cotton & Company conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as established in the Government Accountability Office's (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 January 29, 2018, and included their comments where appropriate.

See Appendix A for details of federal laws, regulations, and guidance, and Appendix B 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. EXIM Bank's charter, *The Export Import Bank Act of 1945*, as amended through Public Law 114-94, December 4, 2015, 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, EXIM 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. EXIM Online (EOL)
4. (b) (7)(E)

EXIM Bank's network infrastructure consists largely of networking devices with various servers running different operating system platforms. Standard desktop personal

computers and laptops run(b) (7)(E) The networks are protected from external threats by a range of information technology security devices, including data loss prevention tools, firewalls, intrusion detection and prevention systems, 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. NIST issues these standards and guidelines as 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, *Minimum Security Requirements for Federal Information and Information Systems,* 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, which is accomplished through DHS' CyberScope tool. CyberScope, operated by DHS on behalf of OMB, replaces the legacy paper-based submission process and automates agency reporting. In addition, OIGs provide an independent assessment of effectiveness of the information security program. OIGs must also report their results to DHS and OMB annually through CyberScope.

FY 2017 OIG FISMA Metrics. On April 17, 2017, DHS issued *FY 2017 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.0* (the metrics). DHS created the metrics for Inspectors General (IGs) to use in conducting their annual independent evaluations to determine the effectiveness of the information security

[1] The Federal Information Security Modernization Act of 2014 amends FISMA 2002 to: (1) reestablish the oversight authority of the Director of 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.

program and practices of their respective agency. The metrics are organized around the five information security functions outlined in the NIST Cybersecurity Framework[2] and are intended to provide agencies with a common structure for identifying and managing cybersecurity risks across the enterprise, as well as to provide IGs with guidance for assessing the maturity of controls to address those risks. See Table 1 below for a description of the NIST Cybersecurity Framework Security Functions and the associated FY 2017 IG FISMA Metric Domains.

Table 1. Aligning the Cybersecurity Framework Security Functions to the FY 2017 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2017 IG FISMA Metric Domains
Identify – The organization's ability to manage and understand cybersecurity risk to systems, assets, data, and capabilities.	Risk Management
Protect – The ability to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Configuration Management, Identity and Access Management, and Security Training
Detect – The ability to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Information Security Continuous Monitoring
Respond – The ability to develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Incident Response
Recover – The ability to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	Contingency Planning

In the *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed a maturity model for evaluating agencies' Information Security Continuous Monitoring (ISCM) programs. The purpose of this maturity model was to (1) summarize the status of agencies' information security programs and their maturity on a five-level scale; (2)

[2] The President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

provide transparency to agency CIOs, senior management officials, and other interested readers of IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program; and (3) help ensure consistency in the annual IG FISMA evaluations.

In addition to updating the metrics to better align with the Cybersecurity Framework in 2016, DHS continued the effort begun in FY 2015 by developing a maturity model for the Incident Response domain, under the Respond function of the Cybersecurity Framework. This maturity model supplements the ISCM maturity model introduced in 2015, which maps to the Detect function of the Cybersecurity Framework. The FY 2017 IG FISMA Reporting Metrics completed this migration to a maturity model approach by not only transitioning the Identify, Protect, and Recover functions to full maturity models, but also reorganizing the models to be more intuitive.

The maturity model concept presents a continuum for agencies to measure their progress in building an effective information security program. The maturity model includes five levels, as described in Table 2 below. Agencies with programs that score at or above the Managed and Measureable level (Level 4) for a NIST Framework Function have effective programs within that area, in accordance with the definition of effectiveness included in NIST SP 800-53, Rev. 4.

Table 2. IG Assessment Maturity Levels

Maturity Level	Description
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

AUDIT RESULTS

The objective of this audit was to determine whether EXIM Bank developed and implemented an effective information security program and practice as required by FISMA. We noted that EXIM Bank addressed several of the challenges identified during previous FISMA audits. Specifically, EXIM management:

- Improved processes over ensuring that agreements with third-party service providers adequately address security responsibilities.
- Implemented appropriate access management controls before granting users access to systems.
- Updated and implemented effective role-based security training.
- Improved controls around shared system accounts.
- Implemented appropriate account management controls for the Application Processing System (APS).
- Improved procedures for managing software licenses.

However, we found that EXIM Bank's information security program and practices are not effective overall. Specifically, the Bank has not consistently implemented its current ISCM and Incident Response policies, plans, procedures, and strategies organization-wide, which impacts the maturity and effectiveness of the Bank's overall information security program.

DHS significantly revised the IG reporting metrics for agencies in FY 2017, which resulted in more rigorous evaluation criteria and assessments than in previous years. When evaluating EXIM Bank's information security management program against the DHS FY 2017 IG FISMA metrics (a five-level maturity model scale, as outlined in Table 2 above), we found that the Identify domain scored at Level 4: Managed and Measurable, and is therefore considered effectively implemented. The remaining framework areas – Protect, Detect, Respond, and Recover – scored at Level 3 or below and are therefore considered ineffective, as stipulated by DHS's FY 2017 IG FISMA metrics. However, although the Respond and Recover domains did not meet Level 4 requirements, based on testing performed, we judgmentally determined that they were generally effective. EXIM Bank's overall score for its information security program was Level 3: Consistently Implemented. We have included a summary of the results for the DHS FY 2017 IG FISMA Metrics in Appendix E.

EXIM Bank needs to develop and implement manageable and measurable metrics to consistently evaluate and improve the effectiveness of its information security program. By not having a mature and effective information security program, EXIM Bank management is at increased risk of operating without a full understanding of its risk posture, including potential vulnerabilities to which its information systems may be susceptible.

In addition, although the Bank effectively implemented 14 of the 18 NIST SP 800-53, Rev. 4 controls that we tested for the Infrastructure GSS, we identified areas for improvement. Specifically, Bank management:

- Has not effectively implemented a vulnerability management program. *(2016 prior-year finding)*

- Has not effectively implemented baseline configurations and documented deviations for information technology (IT) products. *(2016 prior-year finding)*

- Has not effectively developed and implemented a monitoring and auditing process that identifies and remediates gaps in the Bank's information assurance control implementation and that validates compliance with the Bank's privacy and awareness training program.

- Did not consistently implement firewall rule capabilities at all Bank locations.

We partially reissued three prior-year recommendations and made one new recommendation to address the above issues. These recommendations, if implemented, should strengthen EXIM Bank's information security program and practices. EXIM Bank management's responses to the findings identified in our audit are included within the report and in Appendix C.

Finding: EXIM Bank Should Improve the Maturity of Its Information Security Program

EXIM Bank has not effectively implemented a mature information security program. DHS significantly revised the IG reporting metrics for agencies in FY 2017, which resulted in more rigorous evaluation criteria and requirements than in previous years. When evaluating EXIM Bank's information security program against the DHS FY 2017 IG FISMA metrics (a five-level maturity model scale), we found that only one of the five NIST Cybersecurity Framework areas, the Identify domain, was effectively implemented consistent with FISMA requirements and applicable DHS and NIST guidelines (i.e., was at Level 4: Managed and Measureable or higher). The remaining framework areas – Protect, Detect, Respond, and Recover – were not effectively implemented (i.e., were at Level 3 or below). However, although the Respond and Recover domains did not meet Level 4 requirements, based on testing performed, we judgmentally determined that they were generally effective.

EXIM Bank's overall maturity level for its information security program scored at Level 3: Consistently Implemented. We noted several areas for improvement in the maturity of the following domains, which we describe in more detail below.

- Protect – Configuration Management (CM); Identity, Credential, and Access Management (ICAM)

- Detect – ISCM

- Respond – Incident Response

- Recover – Contingency Planning (CP)

We also identified additional weaknesses related to security controls within the Identify (Risk Management) and Protect (CM and Security and Privacy Training) domains; however, these issues were security weaknesses that individually impacted the effectiveness of the Bank's information security program, and we have therefore addressed them separately within this report, rather than as part of this finding.

- Areas for improvement in the Protect domain include the following:
    - The Bank has not defined or implemented qualitative and quantitative performance measures related to the effectiveness of its CM plan, change control activities, or ICAM program.
    - (b) (7)(E)
    - The Bank has not formalized procedures for consistently capturing and sharing lessons learned regarding the effectiveness of its ICAM program.
    - The Bank does not employ automation to centrally document, track, and share risk designations and screening information with necessary parties; it is only able to perform these tasks manually.
    - The Bank does not employ automated mechanisms (e.g., machine-based or user-based enforcement) to support the management of privileged accounts, including the automatic removal or disabling of temporary, emergency, and inactive accounts, as appropriate.
    - The Bank measures the effectiveness of its awareness program by monitoring the number of security incidents that occur. However, this is an informal process, and the Bank does not have established procedures in place to follow up on security incidents with additional training as necessary.
- Areas for improvement in the Detect domain include the following:
    - The Bank has formally developed and communicated its ISCM strategy. However, we reviewed the strategy document and noted that it primarily focused on the information system level, rather than incorporating ISCM requirements and activities at the business and organization-wide levels.
    - Based on our review of the Bank's ISCM strategy and our discussions with management, the Bank is still in the process of acquiring resources and technology to effectively implement ISCM activities, such as Continuous Diagnostics and Mitigation (CDM) and a security operations center.
    - The Bank has not yet implemented ongoing authorization of systems; instead, it re-authorizes systems every three years.

  - The Bank has not defined qualitative and quantitative performance measures for the effectiveness of its ISCM program.

- Areas for improvement in the Respond domain include the following:
  - The Bank informally reviews security incident trends and the Bank's response times; however, it does not formally monitor or analyze qualitative and quantitative performance measures related to the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate.
  - The Bank has defined roles and responsibilities that it has consistently implemented; however, it is still undergoing efforts to hire additional resources and implement a security operations center to more effectively perform incident monitoring and reporting.
  - The Bank does not monitor and analyze qualitative and quantitative performance measures for the effectiveness of its incident response activities.
  - The Bank is able to identify trends in network bandwidth usage and investigate activity; however, it has not implemented any processes for actively profiling network traffic.
  - The Bank does not currently use technology to measure the effectiveness of its technologies for performing incident response activities.

- Areas for improvement in the Recover domain include the following:
  - The Bank informally reviews security incident trends and the Bank's response times; however, it does not formally monitor and analyze qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate.
  - The Bank has not defined qualitative and quantitative performance measures for the effectiveness of its information system contingency planning program.
  - The Bank has not developed automated mechanisms to effectively test system contingency plans.

These weaknesses exist because management has not developed and implemented manageable and measurable metrics to consistently evaluate and improve the effectiveness of the Bank's information security program.

By not having a mature and effective information security program, EXIM Bank management is at increased risk of operating without a full understanding of its risk posture, including potential vulnerabilities to which its information systems may be susceptible.

The following guidance is relevant to this control activity:

OMB M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, dated November 4, 2016, states:

> *In FY 2016, the FISMA metrics were aligned to the five functions outlined in the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. The NIST Cybersecurity Framework is a risk-based approach to managing cybersecurity, which is recognized by both government and industry and provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise. Additionally, OMB worked with DHS, the Federal Chief Information Officer (CIO) Council, and the Council of Inspectors General on Integrity and Efficiency to ensure both the CIO metrics and Inspectors General metrics align with the Cybersecurity Framework and provide complementary assessments of the effectiveness of agencies' information security programs.*
>
> *Federal agencies are to report all of their cybersecurity performance information through DHS's CyberScope reporting system.*

NIST SP 800-55, Rev. 1, *Performance Measurement Guide for Information Security,* dated July 2008, states:

> *A number of existing laws, rules, and regulations—including the Clinger-Cohen Act, the Government Performance and Results Act (GPRA), the Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA) – cite information performance measurement in general, and information security performance measurement in particular, as a requirement. In addition to legislative compliance, agencies can use performance measures as management tools in their internal improvement efforts and link implementation of their information security programs to agency-level strategic planning efforts.*
>
> *The following factors must be considered during development and implementation of an information security measurement program:*
>
> - *Measures must yield quantifiable information (percentages, averages, and numbers);*
> - *Data that supports the measures needs to be readily obtainable;*
> - *Only repeatable information security processes should be considered for measurement; and*
> - *Measures must be useful for tracking performance and directing resources.*
>
> *… The types of measures that can realistically be obtained, and that can also be useful for performance improvement, depend on the maturity of the agency's information security program and the information system's security control implementation. Although different types of measures can be used simultaneously, the primary focus of information security measures shifts as the implementation of security controls matures.*

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

Recommendation:

In FY 2016, we recommended that the EXIM Bank CIO:

a. Perform an assessment of EXIM Bank's current information security program to identify the cost-effective security measures required to achieve a fully mature program.

b. Implement appropriate processes and procedures to improve the information security program and align it with Level 4: Managed and Measurable IG metrics.

As we noted further issues during the FY 2017 audit, the recommendations will remain open, and we are therefore not issuing any new recommendations related to this finding.

Management's Response:

OCIO completed a gap analysis to achieve ' Level 4, Managed and Measurable' in September 2017, and a copy was provided to the OIG. (b) (7)(E)

Evaluation of Management's Response: If implemented properly, we believe that the process management has defined above for remediating this issue will be able to adequately ensure that the Bank performs an assessment of its current information security program to identify security measures to achieve a fully mature security program, as well as to improve the security program to align it with Level 4: Managed and Measurable IG metrics.

Finding: EXIM Bank Should Improve Controls over Its Vulnerability Management Program

Controls are not adequate to ensure that EXIM Bank (b) (7)(E) in a timely manner. Specifically, during the FY 2016 audit, we noted that as of September 2016, the Bank had not remediated more than (b) (7)(E) related to the operation of (b) (7)(E) nor had it installed (b) (7)(E) released for (b) (7)(E) April through June 2016.

During the FY 2017 audit, we noted that the Bank had retired all operations of (b) (7)(E) However, we reviewed an independent, (b) (7)(E)

(b) (7)(E)

This weakness exists because EXIM Bank did not perform (b) (7)(E) was therefore (b) (7)(E) its environment. In addition, the Bank did not perform (b) (7)(E) as a result, the Bank was unaware that it had not remediated (b) (7)(E) .

EXIM Bank management took immediate steps based on the results of the independent (b) (7)(E)

(b) (7)(E)

The following guidance is relevant to this control activity:

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

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

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).*

NIST SP 800-53, Rev. 4, *SI-2, Flaw Remediation,* states:

The organization:

a. *Identifies, reports, and corrects information system flaws;*

b. *Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;*

c. *Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and*

d. *Incorporates flaw remediation into the organizational configuration management process.*

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

Recommendation:

In FY 2016, we recommended that the EXIM Bank CIO:

a. Continue with their efforts to decommission all unsupported software to reduce their exposure to vulnerabilities that cannot be remediated.

b. Implement available (b) (7)(E) that exist across all operating platforms in the Bank's network environment.

During the FY 2017 audit, we noted that the Bank adequately addressed recommendation A. However, we noted further issues related to recommendation B. As a result, recommendation B will remain open, and we are therefore not issuing any new recommendations related to this finding.

Management's Response:

> *This recommendation involves a two phased effort. The first phase is the development and implementation of a comprehensive vulnerability management policy and program.* (b) (7)(E)

Evaluation of Management's Response: If implemented properly, we believe that the process management has defined above for remediating this issue will be able to adequately ensure that the Bank implements (b) (7)(E)

Finding: EXIM Bank Should Improve Controls over Baseline Configuration Implementation

Controls are not adequate to ensure that EXIM Bank implements baseline configurations for IT systems in accordance with documented procedures, or that it identifies and documents deviations from configuration settings. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

The following guidance is relevant to this control activity:

EXIM Bank Installation/Implementation Procedures for (b) (7)(E)

NIST SP 800-53, Rev. 4, *CM-6, Configuration Settings*, states:

> *Control: The organization:*
>
> *a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;*
>
> *b. Implements the configuration settings;*

c. *Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and*

d. *Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.*

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

Recommendation:

In FY 2016, we recommended that the EXIM Bank CIO:

a. Document and implement baseline configuration settings for all information technology products deployed within the Bank.

b. Document justifications or compensating controls for any deviations from established baseline configuration settings for each of the information technology products deployed within the Bank.

As we noted further issues during the FY 2017 audit, the recommendations will remain open, and we are therefore not issuing any new recommendations related to this finding.

Management's Response:

OCIO agrees with this recommendation, however, in FY2017, OCIO defined a new (b) (7)(E)

following which it is reviewed by the Director, IT Infrastructure Engineering and Operations and the decision is made to either approve the deviation or reject it. Some deviations are grandfathered due to incompatibility or inoperability of legacy systems or devices. In the current fiscal year, OCIO will review all devices authorized on the network for compliance with the baseline configuration and remediate accordingly. This will be completed by August 1, 2018.

Evaluation of Management's Response: If implemented properly, we believe that the process management has defined above for remediating this issue will be able to adequately ensure that the Bank documents and implements baseline configuration settings for all information technology products deployed and documents deviations from established baselines.

Finding: EXIM Bank Should Improve Controls over Information Assurance Monitoring

Controls are not adequate to ensure that EXIM Bank implements effective information assurance monitoring and auditing controls to adequately protect sensitive Bank data and personally identifiable information (PII). Specifically, we performed an after-hours walkthrough of the Bank headquarters to determine whether Bank personnel were adequately storing and protecting sensitive data and noted:

- Fourteen instances in which employees had written down their user IDs and passwords on notes or notebooks and left the information on their desks, under their keyboards, or stuck to their monitors.
- Four instances in which employees had left sensitive PII, including Social Security numbers and passport information, lying in plain sight on desks and in printer areas that were accessible to all employees.
- One instance in which an individual left their Personal Identity Verification (PIV) badge for another federal agency on their desk.
- Multiple instances in which employees left potentially sensitive documents and CDs with commercial entity and/or financial information in unsecured workstations and filing cabinets.

This weakness exists because EXIM Bank's privacy and awareness training program does not include processes or activities to verify that employees are fully aware of and are following privacy and security protection requirements.

Without implementing an effective information assurance training program, the Bank is at additional risk of exposure of sensitive Bank and employee PII data.

The following guidance is relevant for this control activity:

NIST SP 800-53, Rev. 4, *AR-4, Privacy Monitoring and Auditing,* states:

> *<u>Control:</u> The organization monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.*
>
> *<u>Supplemental Guidance</u>: To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in this appendix, organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for*

changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a need-to-know basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).

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

Recommendation 1:

We recommend that the EXIM Bank CIO develop and implement a monitoring and auditing process that identifies and remediates gaps in the Bank's information assurance control implementation and that validates compliance with the Bank's privacy and awareness training program.

Management's Response:

The Bank's Office of Chief Information Officer (OCIO) will review its existing information assurance policy, procedures, and practices and will consult with appropriate personnel in other Federal Agencies to identify best practices to ensure compliance in an efficient and low-cost manner. The OCIO envisions the following activities to reach compliance in this area:

1. *Periodic reminders to the EXIM staff of their obligations and responsibilities under the Bank's information assurance policy (e.g., bank wide messages from the OCIO);*

2. *Review and update to content presented in the annual IT security awareness training with a specific focus on information assurance; and*

3. *Conduct of periodic spot checks and inspections of EXIM office spaces for compliance with information assurance policy, including provision of reports to senior management of individuals who violate inf01mation assurance policy. This work will be completed by September 30, 2018.*

Evaluation of Management's Response: If implemented properly, we believe that the process management has defined above for remediating this issue will be able to adequately ensure that Bank employees comply with appropriate Bank information assurance policies.

Finding: EXIM Bank Should Improve Controls over Firewall Capabilities Implementation

Controls are not adequate to ensure that EXIM Bank implements sufficient firewall capabilities in compliance with agency policy. Specifically, we found that the Bank was

operating a (b) (7)(E), (b) (4) firewall at its M Street office. The (b) (7)(E), (b) (4) firewall has limitations that prevent it from adequately enforcing agency firewall policy; for example, it is unable to block access to personal email sites such as Yahoo, Gmail, and Hotmail. However, during the audit the Bank closed its M Street location and transferred all of its personnel and data to its headquarters office on Vermont Avenue, NW. The headquarters office uses a (b) (7)(E), (b) firewall that is able to adequately enforce agency firewall policy. This transfer effectively remediated the firewall issue, and we are therefore not issuing a recommendation.

EXIM management stated that the (b) (7)(E), (b) (4) firewall at the M Street office was a temporary solution until it received funding to purchase and implement an additional (b) (7)(E), (b) firewall. However, once the Bank became aware that it would be closing the M Street office, it abandoned its plans to purchase and implement the (b) (7)(E), (b) (4) firewall.

The Bank effectively remediated this weakness by closing the M Street office. However, for future consideration, without implementing appropriate firewall capabilities, the Bank is at increased risk of unauthorized access from non-Bank personnel, as well as increased risk of data leakage from internal Bank users.

The following guidance is relevant to this control activity:

(b) (7)(E)

NIST SP 800-53, Rev. 4, *SC-7, Boundary Protection*, states:

> *Control: The information system:*

a. *Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;*

b. *Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and*

c. *Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.*

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

Recommendation:

As this weakness was remediated during the audit, we are not issuing a recommendation.

Management's Response:

We agree with this recommendation. As correctly stated in the text above, we remediated this issue when the EXIM office's at the M Street Annex was closed. No further action is required or planned for this issue.

CONCLUSION

We determined that EXIM Bank addressed several of the challenges identified during previous FISMA audits and effectively implemented 14 of the 18 NIST SP 800-53, Rev. 4 controls that we tested for the Infrastructure GSS; however, its information security program and practices are not effective overall, as the Bank has not effectively implemented a mature information security program. EXIM Bank must develop and implement manageable and measurable metrics to consistently evaluate and improve the effectiveness of its information security program. By not having a mature and effective information security program, EXIM Bank management is at increased risk of operating without a full understanding of its risk posture, including potential vulnerabilities to which its information systems may be susceptible.

APPENDICES

Appendix A: Federal Laws, Regulations, and Guidance

Our evaluation of the effectiveness of EXIM Bank's information security program and practices, was guided by applicable federal laws and regulations related to information security, including but not limited to:

- Federal Information Security Modernization Act of 2014
- FY 2017 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.0
- NIST SPs and FIPS, particularly:
    - SP 800-53, Rev. 4, *Security and Privacy Controls for 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 Revision 1: 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*

Appendix B: 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.

Table 3. Prior-Year Audit Finding Remediation Status

Finding	Recommendation	FY Identified	FY 2017 Status
Controls are not adequate to ensure that EXIM Bank data accessible from mobile devices is adequately protected. In FY 2015, we noted that the Bank has acquired software that will enable it to enforce security controls on mobile devices. This software has been configured and implemented for Bank-owned devices, but has not been fully rolled out for personally owned devices.	We recommend that the EXIM Bank CIO deploy mobile phone security controls that: 1. Enforce FIPS 140-2 encryption of data stored on mobile devices. 2. Restrict the installation of unapproved or malicious software. 3. Prevent mobile phones from connecting to internal EXIM Bank resources.	2014	Closed
Controls are not adequate to ensure that appropriate POA&M [Plan of Action and Milestones] management controls are in place. Specifically, we noted the following: • For the Infrastructure GSS, 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) GSS, the Bank had not started addressing (b) (7)(E) and the scheduled completion date passed with no milestone updates.	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 that milestones are updated to reflect actions taken to remediate POA&M items.	2015	Closed

Finding	Recommendation	FY Identified	FY 2017 Status
Controls are not adequate to ensure that EXIM Bank's agreements specify how information security performance is measured, reported, and monitored on contractor or other entity-operated systems, as appropriate. Specifically, we noted that EXIM Bank currently has a Memorandum of Understanding with the General Services Administration (GSA) for several Human Resources (HR) and payroll-related services. However, the existing agreements do not identify how information security performance should be measured, reported, and monitored.	We recommend that the EXIM Bank CIO review and update all agreements with third-party service providers to ensure that the agreements specify how information security performance is measured, reported, and monitored.	2016	Closed
Controls are not adequate to ensure that individuals requiring access to EXIM information and information systems sign appropriate access agreements prior to obtaining access. Specifically, we noted through the audit on-boarding process that EXIM Bank did not require the auditors to sign the EXIM Rules of Behavior (RoB) document prior to obtaining network access.	We recommend that the EXIM Bank CIO: a. Update their on-boarding process to separate the acknowledgement of the RoB from the security awareness training and require users to acknowledge and sign the RoB prior to obtaining network access, or improve their existing security training procedures to ensure that all personnel receive security training and sign the Bank's RoB agreement prior to obtaining access to the Bank's data. b. Implement procedures to formally track compliance with the updated process.	2016	Closed

Finding	Recommendation	FY Identified	FY 2017 Status
Controls are not adequate to ensure that EXIM Bank identifies and tracks the status of specialized security and privacy training for all personnel (to include employees, contractors, and other organization users) that have significant information security and privacy responsibilities requiring such training.	We recommend that the EXIM Bank CIO: a. Identify and document a comprehensive list of all roles with information security responsibilities. b. Document and implement procedures to ensure that all of the identified roles receive annual role-based security training.	2016	Closed
EXIM Bank has not implemented appropriate controls over the frequency of reviews and updates to shared accounts.	We recommend that the EXIM Bank CIO implement a review and update of shared system account passwords on a frequency that is compliant with EXIM Bank's documented policies and procedures. At a minimum, the Bank should perform this update whenever a DBA [database administrator] leaves the agency.	2016	Closed
Controls are not adequate to ensure that EXIM Bank disables APS accounts for individuals that have not logged into the application for more than 90 days. Specifically, we identified 129 active APS accounts for individuals that have not logged in for more than 90 days, which violates EXIM Bank policy.	We recommend that the EXIM Bank CIO document and implement procedures to periodically review and disable APS accounts that have not been used for more than 90 days.	2016	Closed

Finding	Recommendation	FY Identified	FY 2017 Status
Controls are not adequate to ensure that EXIM Bank appropriately uses software in accordance with contract agreements and copyright laws. Specifically, we noted that as of October 30, 2016, the Bank was usin (b) (7)(E) licenses in excess of its purchased license amounts.	We recommend that the EXIM Bank CIO: a. Remove all instances of (b) (7)(E) software that have not been properly licensed or authorized by the vendor, or make arrangements with (b) (7)(E) to purchase the current excess amount. b. Document and implement procedures to periodically review and reconcile the number of software licenses used for all software products to ensure that the Bank is in compliance with its vendor agreements.	2016	Closed
Controls are not adequate to ensure that EXIM Bank (b) (7)(E) in a timely manner.	We recommend that the EXIM Bank CIO: a. Continue with their efforts to decommission all unsupported software to reduce their exposure to vulnerabilities that cannot be remediated. b. (b) (7)(E) that exist across all operating platforms in the Bank's network environment.	2016	Re-Issue Letter "a" is closed; Letter "b" remains open

Finding	Recommendation	FY Identified	FY 2017 Status
Controls are not adequate to ensure that EXIM Bank implements baseline configurations for IT systems in accordance with documented procedures, or identifies and documents deviations from configuration settings.	We recommend that the EXIM Bank CIO: a. Document and implement baseline configuration settings for all information technology products deployed within the Bank. b. Document justifications or compensating controls for any deviations from established baseline configuration settings for each of the information technology products deployed within the Bank.	2016	Re-Issue
EXIM Bank has not effectively implemented a mature information security program. Specifically, the Bank's current ISCM and IR policies, plans, procedures, and strategies are not consistently implemented organization-wide, impacting the maturity and effectiveness of its overall information security program.	We recommend that the EXIM Bank CIO: a. Perform an assessment of EXIM Bank's current information security program to identify the cost-effective security measures required to achieve a fully mature program. b. Implement appropriate processes and procedures to improve the information security program and align it with Level 4: Managed and Measurable IG metrics.	2016	Re-Issue

Appendix C: Management's Response

EXIM
EXPORT-IMPORT BANK
OF THE UNITED STATES

Reducing Risk. Unleashing Opportunity.

February 13, 2018

Ms. Terry Settle
Acting Inspector General
Office of the Inspector General
Export-Import Bank of the United States
811 Vermont Avenue, NW
Washington, DC 20571

Dear Ms. Settle,

Thank you for providing the Export-Import Bank of the United States ("EXIM Bank" or "the Bank") management with the Office of the Inspector General's ("OIG") "Independent Audit of the Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2017", dated January 31, 2018 (the "Report"). Management continues to support the OIG's work that compliments the EXIM goal of continuous process improvement to achieve the mission of the Bank.

The OIG contracted with Cotton & Company, LLP ("Cotton") to conduct a performance audit of the Bank's IT security programs and practices. The Bank appreciates Cotton recognizing that "the Bank has addressed several of the challenges identified during previous FISMA audits" and that "EXIM Bank improved processes over ensuring agreements with third-party service providers adequately address security responsibilities; implemented appropriate access management controls prior to granting users access to systems; updated and implemented effective role-based security training; improved controls around shared system accounts; implemented appropriate account management controls for the Application Processing System (APS) application; and improved procedures for managing software licenses." While the overall score for its information security program was at a Level 3 based on the DHS FY2017 IG FISMA Metrics, the Bank was pleased to learn that 14 of the 18 NIST SP 800-53, Rev. 4 controls were effectively implemented by EXIM.

The OIG, through Cotton, has made one new recommendation to further enhance current policies to fulfill the responsibilities as outlined in FISMA. The Bank concurs with the recommendation and will move forward with implementation as below.

Recommendation 1: We recommend that the EXIM Bank CIO develop and implement a monitoring and auditing process that identifies and remediates gaps in the agency's information assurance control implementation, and validates compliance with the Bank's privacy and awareness training program.

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380
exim.gov

Management Response: The Bank concurs with this recommendation.

The Bank's Office of Chief Information Officer (OCIO) will review its existing information assurance policy, procedures, and practices and will consult with appropriate personnel in other Federal Agencies to identify best practices to ensure compliance in an efficient and low-cost manner. The OCIO envisions the following activities to reach compliance in this area:

1. Periodic reminders to the EXIM staff of their obligations and responsibilities under the Bank's information assurance policy (e.g., bank wide messages from the OCIO);

2. Review and update to content presented in the annual IT security awareness training with a specific focus on information assurance; and

3. Conduct of periodic spot checks and inspections of EXIM office spaces for compliance with information assurance policy, including provision of reports to senior management of individuals who violate information assurance policy. This work will be completed by September 30, 2018.

In addition to the newly issued recommendation, Cotton re-issued the following three recommendations from prior year audits:

Recommendation: In FY2016 OIG recommended that the OCIO:

a. Perform an assessment of EXIM Bank's current information security program to identify the cost-effective security measures required to achieve a fully mature program; and

b. Implement appropriate processes and procedures to improve the information security program and align it with Level 4: Managed and Measureable, IG metrics.

Management Response: The Bank concurs with this recommendation.

OCIO completed a gap analysis to achieve 'Level 4, Managed and Measurable' in September 2017, and a copy was provided to the OIG. (b) (7)(E)

(b) (7)(E)

2

Recommendation: In FY2016 OIG recommended that the OCIO:

a. Continue with their efforts to decommission all unsupported software to reduce their exposure to vulnerabilities that cannot be remediated; and

b. Implement available (b) (7)(E) that exist across all operating platforms in the Bank's network environment.

Management Response: The Bank concurs with this recommendation.

This recommendation involves a two phased effort. (b) (7)(E)

(b) (7)(E)

(b) (7)(E) . This will be completed by August 1, 2018.

Recommendation: In FY2016 OIG recommended that the OCIO:

a. Document and implement baseline configuration settings for all information technology products deployed within the Bank;

b. Document justifications or compensating controls for any deviations from established baseline configuration settings for each of the information technology products deployed within the Bank.

Management Response: The Bank concurs with this recommendation.

OCIO agrees with this recommendation, (b) (7)(E)

(b) (7)(E)

3

(b) (7)(E)

(b) (7)(E) This will be completed by August 1, 2018.

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,

Jeffrey Goettman
Executive Vice President and Chief Operating Officer
Export-Import Bank of the United States

4

Appendix D: Selected Security Controls and Testing Results

Table 4. Selected Security Controls and Testing Results

No.	800-53 Control	Control Title	System	Results
1.	AC-8	System Usage Notification	GSS	Controls are effective
2.	AC-12	Session Termination	GSS	Controls are effective
3.	AC-17	Remote Access	GSS	Controls are effective
4.	AC-18	Wireless Access	GSS	Controls are effective
5.	AC-19	Access Control for Mobile Devices	GSS	Controls are effective
6.	AU-2	Auditable Events	GSS	Controls are effective
7.	AU-6	Audit Review, Analysis, and Reporting	GSS	Controls are effective
8.	CM-2	Baseline Configuration	GSS	Controls are not effective
9.	CM-3	Configuration Change Control	GSS	Controls are effective
10.	CM-6	Configuration Settings	GSS	Controls are not effective
11.	MP-5	Media Transport	GSS	Controls are effective
12.	MP-6	Media Sanitation	GSS	Controls are effective
13.	PE-2	Physical Access Authorizations	GSS	Controls are effective
14.	PE-3	Physical Access Control	GSS	Controls are not effective
15.	PE-6	Monitoring Physical Access	GSS	Controls are effective
16.	PL-4	Rules of Behavior	GSS	Controls are effective
17.	RA-5	Vulnerability Scanning	GSS	Controls are not effective
18.	SA-9	External Information System Services	GSS	Controls are effective

Appendix E: DHS FY 2017 IG FISMA Metric Results

The following tables represent each of the NIST Cybersecurity Framework domains that we reviewed to respond to the FY 2017 IG FISMA Metrics. Each of the five domain areas (Identify, Protect, Detect, Respond, and Recover) had specific evaluation questions that we assessed, for a total of 54 questions, and each question was associated with a maturity level. The tables below represent the number of objectives that we evaluated for each Cybersecurity Framework, as well as the maturity model rating that each of the respective domain questions "met." Per DHS's FY 2017 IG FISMA metrics, only agency programs that score at or above Level 4: Managed and Measureable for a NIST Framework Function have effective programs within that area.

Furthermore, ratings throughout the five domains are determined by a simple majority, in which the most frequent level across the questions (i.e., the mode) serves as the domain rating. For example, if there are seven questions in a domain and the agency receives "Defined" ratings for three questions and "Managed and Measurable" ratings for four questions, then the domain rating is "Managed and Measurable." If two or more levels are equally frequently rated, the agency is rated at the higher level.

Table 5. EXIM Bank FY 2017 IG FISMA Metric Results

Identify	
Level	**# Met**
Level 1: Ad-hoc	1
Level 2: Defined	3
Level 3: Consistently Implemented	4
Level 4: Managed and Measureable	**4**
Level 5: Optimized	0

Protect	
Level	**# Met**
Level 1: Ad-hoc	0
Level 2: Defined	4
Level 3: Consistently Implemented	**13**
Level 4: Managed and Measureable	6
Level 5: Optimized	0

Detect	
Level	**# Met**
Level 1: Ad-hoc	2
Level 2: Defined	**2**
Level 3: Consistently Implemented	1
Level 4: Managed and Measureable	0
Level 5: Optimized	0

Respond	
Level	**# Met**
Level 1: Ad-hoc	0
Level 2: Defined	2
Level 3: Consistently Implemented	**3**
Level 4: Managed and Measureable	2
Level 5: Optimized	0

Recover	
Level	**# Met**
Level 1: Ad-hoc	0
Level 2: Defined	0
Level 3: Consistently Implemented	**5**
Level 4: Managed and Measureable	2
Level 5: Optimized	0

Overall		
Area	**Level**	**Effective**
Identify	Level 4: Managed and Measurable	**Yes**
Protect	Level 3: Consistently Implemented	**No**
Detect	Level 2: Defined	**No**
Respond	Level 3: Consistently Implemented	**No**
Recover	Level 3: Consistently Implemented	**No**
Overall:	**Level 3: Consistently Implemented**	**No**

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