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

Independent Audit of Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2016

March 15, 2017
OIG-AR-17-04

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, Chief Information Officer

From: Terry Settle, Assistant Inspector General for Audits TLS

Subject: Independent Audit of Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2016 (OIG-AR-17-04)

Date: March 15, 2017

This memorandum transmits Cotton & Company LLP's (Cotton & Company) audit report on Export-Import Bank's (EXIM Bank) Information Security Program for Fiscal Year 2016. 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 nine new recommendations and two partially 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/about/oig.

cc: C.J. Hall, Acting President and Chairman, Executive Vice President and Chief Operating Officer
Angela Freyre, General Counsel
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
David Sena, Senior Vice President and Chief Financial Officer
Inci Tonguch-Murray, Deputy Chief Financial Officer
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

March 3, 2017

Terry Settle
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 2016

Dear Ms. Settle:

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 Export-Import Bank of the United States' (EXIM Bank's) information security program and practices for the fiscal year ending September 30, 2016. Cotton & Company performed the work from May through December 2016.

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.

ACRONYMS

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
IR	Incident Response
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
SSP	System Security Plan

Executive Summary

OIG-AR-17-04

Independent Audit of the EXIM Bank's Information Security Program Effectiveness for Fiscal Year 2016

March 3, 2017

Why We Did This Audit

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

What We Recommended

We partially reissued two recommendations and made nine new recommendations 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) update agreements with third-party service providers, (3) improve vulnerability management, (4) adequately document and implement baseline configuration settings for IT products, (5) implement appropriate access management prior to granting users access to systems, (6) update and implement effective role-based security training, (7) improve controls around shared system accounts, (8) implement appropriate account management controls for the Application Processing System (APS) application, and (9) improve procedures for managing software licenses.

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. EXIM Bank has addressed several of the challenges identified during previous FISMA audits. During the past year, EXIM Bank fully implemented Personal Identity Verification (PIV) card usage for logical system access. Additionally, EXIM Bank improved the controls around the account management process for the Infrastructure General Support System (GSS); improved remote access timeout configurations; and adequately documented and updated its configuration management plans for the Infrastructure GSS and (b) (7)(E). However, under DHS metrics, EXIM Bank has not effectively implemented a mature information security program. Specifically, the Bank's current Information Security Continuous Monitoring (ISCM) and Incident Response (IR) policies, plans, procedures, and strategies are not consistently implemented organization-wide, impacting the maturity and effectiveness of its overall information security program.

The DHS significantly revised the Inspector General (IG) reporting metrics for agencies in fiscal year (FY) 2016, 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 2016 IG FISMA metrics, which use a five-level maturity model scale, we found that only one of the five National Institute of Standards and Technology (NIST) Cybersecurity Framework areas, the Recover domain, was effectively implemented consistent with FISMA requirements and applicable DHS and NIST guidelines (i.e., was at Level 4 or higher). The remaining framework areas – Identify, Protect, Detect, and Respond – were not effectively implemented (i.e., were at Level 3 or below). Per DHS' FY 2016 IG FISMA metrics, only agency programs that scored at or above the Managed and Measureable level (Level 4) for a NIST Framework Function have effective programs within that area. EXIM Bank's overall score for its information security program was Level 2: Defined, which does not represent an effective program. A summary of the results for the DHS FY 2016 IG FISMA Metrics is in Appendix D.

We noted, however, a number of new challenges identified in this year's FISMA audit. While the Bank effectively implemented 11 of the 14 NIST SP 800-53, Rev. 4 controls that we tested for the Application Processing System (APS) and the Infrastructure GSS, we identified several significant areas for improvement. Specifically, Bank management:

- Has not implemented appropriate security controls over (b) (7)(E) used to access EXIM Bank data. (*2014 prior-year finding*)
- Did not effectively remediate Plan of Action and Milestones (POA&M) items in a timely manner. *(2015 prior-year finding)*
- Has not effectively documented security agreements with third-party service providers.
- Has not effectively implemented a vulnerability management program.
- Has not effectively implemented baseline configurations and documented deviations for information technology (IT) products.
- Has not effectively implemented Access Management controls.
- Has not effectively implemented a role-based training program.
- Has not effectively implemented controls around the use of shared system accounts.
- Has not effectively implemented Account Management controls for the APS application.
- Has not effectively implemented software license management controls.

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

TABLE OF CONTENTS

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.

Objective

This report presents the results of the independent performance audit of the information security program of the Export-Import Bank (EXIM Bank or the Bank) for fiscal year (FY) 2016, conducted by Cotton & Company LLP. The objective was to determine whether EXIM Bank developed and implemented effective information security programs and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA).

Scope and Methodology

To determine whether EXIM Bank developed and implemented effective information security programs and practices as required by FISMA, we evaluated its security program, plans, policies, and procedures in place throughout FY 2016 for effectiveness 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 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.1.3*, to evaluate EXIM Bank's policies, procedures, and practices 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 Application Processing System (APS) and 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 APS and the Infrastructure GSS were judgmentally chosen from selected security control families through a collaborative effort between the EXIM Bank OIG and Cotton & Company. See Appendix C for 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 2016. 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 11, 2017, and included their comments where appropriate.

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

Background

The Export-Import Bank of the United States is an independent, self-sustaining executive agency and a wholly-owned United States government corporation. 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 such as 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. The standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) and SPs. FIPS provide the minimum information security requirements that are necessary to improve the security of federal information and information systems, and the SP 800 and selected 500 series provide computer security guidelines and recommendations. For instance, FIPS Publication 200, *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 through CyberScope. CyberScope, operated by DHS on behalf of OMB, replaces the legacy paper-based submission process and automates agency reporting. In addition, Offices of Inspectors General (OIGs) provide an independent assessment of whether the agency is applying a risk-based approach to its information security programs and information systems. OIGs must also report their results to OMB annually through CyberScope.

[1] The Federal Information Security Modernization Act of 2014 amends 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.

FY 2016 OIG FISMA Metrics. On July 29, 2016, DHS issued *FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.1* (the metrics).[2] DHS created the metrics for Inspectors General (IGs) to use in conducting their annual independent evaluations to determine the effectiveness of the information security program and practices of their respective agency. The metrics are organized around the five information security functions outlined in the NIST Cybersecurity Framework and are intended to provide agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and 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 2016 IG FISMA Metric Domains.

Table 1. Aligning the Cybersecurity Framework Security Functions to the FY 2016 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2016 IG FISMA Metric Domains
Identify – The organization's ability to manage and understand cybersecurity risk to systems, assets, data, and capabilities.	Risk Management and Contractor Systems
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 and Privacy 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 program. 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) 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

[2] DHS released the final version of the *FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics*, version 1.1.3, on September 26, 2016.

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 Information Security Continuous Monitoring maturity model introduced in 2015, which maps to the Detect function of the Cybersecurity Framework. DHS has not yet developed maturity models for the remaining three functions of the Cybersecurity Framework (i.e., Identify, Protect, and Recover); however, it has developed Maturity Model Indicators (Level 1-5 assessments) for those domains. These indicators act as a stepping stone, allowing IGs to reach preliminary conclusions similar to those achievable with a fully developed model.

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. Capability Maturity Model Continuum

Maturity Level	Description
Level 1: Ad-hoc	The functional program (identify, protect, detect, respond, or recover) is not formalized and the organization performs function activities in a reactive manner, resulting in an ad hoc program that does not meet Level 2 requirements for a defined program.
Level 2: Defined	The organization has formalized its functional program through the development of comprehensive function policies, procedures, and strategies consistent with NIST guidance and other regulatory guidance; however, it has not consistently implemented the function policies, procedures, and strategies organization-wide.
Level 3: Consistently Implemented	In addition to formalizing and defining its functional program (Level 2), the organization consistently implements the functional program across the agency; however, it does not capture qualitative and quantitative measures and data on the effectiveness of the functional program across the organization, or use these measures and data to make risk-based decisions.
Level 4: Managed and Measurable	In addition to being consistently implemented (Level 3), functional activities are repeatable, and the organization uses metrics to measure and manage the implementation of the functional program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.

Maturity Level	Description
Level 5: Optimized	In addition to being managed and measurable (Level 4), the organization's functional program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.

Information about specific vulnerabilities in IT systems has been redacted from the publicly released version of this report. The redacted information is sensitive and its disclosure in a widely distributed report might cause loss to Export-Import Bank of the United States. We have provided that information in a separate report intended solely for the information and use of the Export-Import Bank of the United States.

RESULTS

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

- Fully implemented the use of personal identity verification (PIV) cards for logical system access.

- Improved controls around the account management processes for the Infrastructure GSS by ensuring that accounts do not remain active for individuals who have not logged in within 90 days; accounts for separated individuals do not remain active; and EXIM Bank periodically reviews accounts for appropriateness.

- Improved remote access controls to ensure that remote users are timed out or disconnected from the EXIM Bank network after a period of inactivity, in accordance with EXIM Bank policy.

- Adequately documented and updated its configuration management plans for its Infrastructure GSS and (b) (7)(E) systems.

Nevertheless, we found that EXIM Bank's information security program and practices are not effective overall.

EXIM Bank has not effectively implemented a mature information security program. Specifically, the Bank's current Information Security Continuous Monitoring (ISCM) and Incident Response (IR) policies, plans, procedures, and strategies are not consistently implemented organization-wide, impacting the maturity and effectiveness of its overall information security program.

DHS significantly revised the IG reporting metrics for agencies in FY 2016, which resulted in more rigorous evaluation criteria and assessments than in previous years. When evaluating EXIM Bank's information security measurement program against the DHS FY 2016 IG FISMA metrics, a five-level maturity model scale, we found that only one of the five NIST Cybersecurity Framework areas, the Recover domain, was effectively implemented consistent with FISMA requirements and applicable DHS and NIST guidelines (i.e., was at Level 4 or higher). The remaining framework areas – Identify, Protect, Detect, and Respond – were not effectively implemented (i.e., were at Level 3 or below). Per DHS' FY 2016 IG FISMA metrics guidelines, only agency programs that scored at or above the Managed and Measureable level (Level 4) for a NIST Framework Function have effective programs within that area. EXIM Bank's overall score for its information security program

was Level 2: Defined, which does not represent an effective program. A summary of the results for the DHS FY 2016 IG FISMA Metrics is in Appendix D.

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. Additionally, management has not performed an assessment of the maturity of its information security program to determine what improvements are necessary to achieve a fully measurable 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.

We noted a number of new challenges identified in this year's FISMA audit. While the Bank effectively implemented 11 of the 14 NIST SP 800-53, Rev. 4 controls that we tested for the APS and the Infrastructure GSS, we identified several significant areas for improvement. Specifically, Bank management:

- Has not implemented appropriate security controls over (b) (7)(E) used to access EXIM Bank data. (*2014 prior-year finding*)
- Did not effectively remediate Plan of Action and Milestones (POA&M) items in a timely manner. *(2015 prior-year finding)*
- Has not effectively documented security agreements with third-party service providers.
- Has not effectively implemented a vulnerability management program.
- Has not effectively implemented baseline configurations and documented deviations for information technology (IT) products.
- Has not effectively implemented access management controls.
- Has not effectively implemented a role-based training program.
- Has not effectively implemented controls around the use of shared system accounts.
- Has not effectively implemented account management controls for the APS application.
- Has not effectively implemented software license management controls.

We partially reissued two prior-year recommendations and made nine new recommendations 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 B.

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

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.

DHS significantly revised the IG reporting metrics for agencies in FY 2016, which resulted in more rigorous evaluation criteria and requirements than previous years. When evaluating EXIM Bank's information security program against the DHS FY 2016 IG FISMA metrics, a five-level maturity model scale, we found that only one of the five NIST Cybersecurity Framework areas, the Recover 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 – Identify, Protect, Detect, and Respond – were not effectively implemented (i.e., were at Level 3 or below).

EXIM Bank's overall maturity level for its information security program scored at Level 2: Defined. We noted several areas for improvement in the maturity of the Detect (ISCM) and Respond (IR) domains, as described below. Additionally, while we identified weaknesses with security controls within the Identify (Risk Management and Contractor Systems) and Protect (Configuration Management, Identity and Access Management, and Security and Privacy Training) domains, these were security weaknesses that individually impacted the effectiveness of the Bank's information security program and required specific recommendations. As a result, those weaknesses are addressed in the remaining findings and recommendations of this report, and not as part of this finding.

- Areas for improvement in the Detect domain include the following:
    - The Bank is currently in the process of filling two IT Security positions to improve the management and effectiveness of the ISCM program. These positions have yet to be filled, limiting the resources (people, processes, and technology) to effectively implement ISCM activities. This also applies to the IR process discussed below in the Respond domain areas for improvement.
    - The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements.
    - ISCM processes are not consistently performed across the organization.
    - EXIM Bank's qualitative and quantitative performance measures used to evaluate the effectiveness of its ISCM program are not consistently captured, analyzed, and used across the organization in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.
    - EXIM Bank does not have formalized or defined processes for collecting and considering lessons learned to improve ISCM processes.

- EXIM Bank has not fully implemented technology in automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools are not interoperable.

- Areas for improvement in the Respond domain include the following:

  - The Bank has not defined how it will integrate IR activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate.

  - The Bank has not defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents.

  - The Bank has not identified or defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of the IR program, perform trend analysis, achieve situational awareness, and control ongoing risk.

  - The Bank has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and IR processes.

  - The Bank has not fully implemented automation technologies to support its IR processes and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some IR activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures.

  - (b) (7)(E)

  - The Bank has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems.

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. Additionally, management has not performed an assessment of the maturity of its information security program to determine what improvements are necessary to achieve a fully measurable 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 1:

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.

Management's Response:

The Bank concurs with this recommendation.

The Bank's Office of Chief Information Officer (OCIO) will 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.

OCIO will conduct a gap analysis and once these gaps are identified, they will be triaged on those gaps that are at a higher level of priority than others and will then estimate the cost and level of effort required to close these gaps. The implementation will be a multi-year effort. The Bank's OCIO anticipates having a prepared assessment and initial plan by September 1, 2017.

Regarding the second part of the recommendation, OCIO will develop processes and procedures required to enhance the Bank's IT security program in order to achieve level 4 in the Maturity Model across the board.

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 Security Controls over (b) (7)(E) (b) (7)(E)

The FY 2014 FISMA audit identified the following weaknesses related to the security of (b) (7)(E) :

- EXIM Bank employees were able to use (b) (7)(E) to access their EXIM Bank email, (b) (7)(E)

- While (b) (7)(E) were generally prohibited from accessing the Bank's internal resources, there were special instances in which (b) (7)(E) had been configured to do so. We noted that EXIM Bank did not have in place policy, procedures, or configuration guidance to ensure that these special instances were approved and that (b) (7)(E) secured before connecting.

- The Bank did not have controls in place to enforce (b) (7)(E)

FY 2016 testing noted that the Bank acquired (b) (7)(E) (b) (7)(E) management software to allow the CIO to monitor and enforce security controls on (b) (7)(E) (b) (7)(E)

Additionally, EXIM implemented security controls to prevent (b) (7)(E) from accessing the Bank's internal resources. The testing therefore confirmed that the first two weaknesses identified in 2014 were successfully remediated.

However, the 2016 audit found that the weakness originally identified in FY 2014 related to (b) (7)(E) has not yet been completely remediated. FY 2016 testing found that the (b) (7)(E) (b) (7)(E) management software deployed by the Bank is able (b) (7)(E)

[3] (b) (7)(E)

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

The following guidance is relevant to this control activity:

NIST SP (b) (7)(E) **,** states:

(b) (7)(E)

NIST SP (b) (7)(E) :

(b) (7)(E)

NIST SP (b) (7)(E) states:

(b) (7)(E)

FIPS (b) states:

(b) (7)(E)

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

Recommendation:

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

a. (b) (7)(E)

b. Restrict the installation of unapproved or malicious software.

c. Prevent unauthorized (b) (7)(E) from connecting to internal EXIM Bank resources.

As of FY 2016, Recommendation A remains open; we are therefore not issuing any new recommendations related to this finding. See Appendix A for a complete listing of the status of prior-year FISMA audit findings.

Management's Response:

The Bank concurs with this recommendation.

OCIO will address #1 of the remaining open recommendation to (b) (7)(E)

he Bank expects to have this effort completed by April 1, 2017.

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 (b) (7)(E)

Finding: EXIM Bank Should Improve Controls over Its Plan of Action & Milestones Process

As initially identified in our FY 2015 FISMA audit report, we found during our FY 2016 testing that controls remained inadequate to ensure that appropriate POA&M management controls are in place. Specifically, we noted the following:

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

Management stated that they were aware that the POA&Ms had passed their scheduled completion dates but did not want to change the original scheduled completion dates until the Bank had determined new remediation plans. Per EXIM policy, notations for any modifications to the original POA&M entry or milestones are to be made separately and identified as "changes to milestones"; however, testing noted that these modifications were not being documented as required. Without adequate POA&M management, the Bank may remain exposed to known vulnerabilities that could be exploited by internal and external threats.

The following guidance is relevant to this control activity:

EXIM POA&M Policy, version 04, effective March 10, 2016 states:

> *6.11 Reporting on remediation progress must be accomplished not less frequently than quarterly.*
>
> *6.12 Once the POA&M has been reported, changes are not to be made to the original description of the weakness, key milestones and scheduled completion dates, or source. Notations for any modifications to the original entry are to be made separately and identified as "Changes to Milestones."*

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

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

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

> *Control: The organization:*
> *a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:*
> *1. Are developed and maintained;*
> *2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and*
> *3. Are reported in accordance with OMB FISMA reporting requirements.*
> *b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.*

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

Recommendation:

In our FY 2015 FISMA audit report, we recommended that the EXIM Bank CIO implement a process to ensure that the Bank reviews all system POA&Ms at an organization-defined frequency, and that it updates milestones to reflect actions taken to remediate POA&M items.

As of FY 2016, the recommendation noted remains open; we are therefore not issuing any new recommendations related to this finding. See Appendix A for a complete listing of the status of prior-year FISMA audit findings.

Management's Response:

The Bank concurs with this recommendation.

The Bank's OCIO will implement a process to review and update system POA&Ms by adding a new column to our POA&M tracking spreadsheet to provide up-to-date information regarding open POA&Ms which are at risk of not meeting their scheduled completion dates and for which an approved remediation plan does not yet exist. This will permit management to make the POA&M process consistent, while making it transparent when a remediation is not completed when planned. The new information column in the POA&M spreadsheet will be added and in use by March 15, 2017.

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 reviews all system POA&Ms at an organization-defined frequency, and that it updates milestones to reflect actions taken to remediate POA&M items.

Finding: EXIM Bank Should Improve Controls over Agreements with Third-Party Service Providers

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.

EXIM management stated that GSA is one of a limited number of agencies that provide these services, which EXIM Bank is required to use, and that the Bank has limited leverage regarding the information documented in the agreement. EXIM management also stated that it periodically reviews the GSA system security plan for the system to gain assurance that GSA is appropriately implementing a security program consistent with FISMA requirements; however, the Bank does not perform this review in accordance with a defined frequency. Without documenting requirements related to security performance measurement, reporting, and monitoring within the established agreement, there is an increased risk that EXIM Bank may be unaware of the security risks over its data.

The following guidance is relevant to this control activity:

EXIM Infrastructure GSS SSP, *SA-9, External Information System Services,* states:

> *The Bank:*
> a. *Requires that providers of external information system services (Exchange Online) comply with organizational information security requirements and employs applicable FedRAMP and 800-53 rev 4 Moderate level controls in accordance with applicable FISMA, OMB Executive Orders, directives, Ex-Im Bank policies, regulations, CIS and USGCB standards, and NIST guidance;*
> b. *incorporates security requirements into contracts, interagency service agreements (ISA), and memorandums of understanding (MOU), and documents in the service agreement, the government oversight and user roles and responsibilities with regard to external information system services;*
> c. *Employs organization-defined Continuous Monitoring processes methods, and techniques defined in the CM Policy to monitor security control compliance by external service providers on an ongoing basis. 3rd Party Service Providers are required to permit Ex-Im Bank the ability to monitor the contractor's security compliance, including access required to audit and perform vulnerability testing within contractor facilities employed under the contract and any subcontracts. Ex-Im Bank monitors security controls in accordance with requirement defined in this SSP. Security control compliance is monitored as part of the Bank's continuous monitoring activities.*

NIST SP 800-35, *Guide to Information Technology Security Services,* section 4.5.1, *Monitor Service Provider Performance*, states:

> *The targets set forth in the service agreement should be compared with the metrics gathered. Although metrics will provide service-level targets, the organization may also want to use end user evaluations or customer satisfaction level surveys to evaluate performance. The IT security managers will have to work with other operational managers (such as customer service managers) to ensure that the service provider is meeting service targets. The IT security managers also need to ensure service providers are complying with IT security policy and processes, as well as applicable laws and regulations. IT security managers must ensure during the operations phase that the service provider does not compromise private, confidential, personal, or mission-sensitive data. Compliance reports will help with this effort. The service agreement should have included clauses that specify penalties and/or remedies for noncompliance and management should employ these when the service provider does not perform as the contract dictates.*

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

Recommendation 2:

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.

Management's Response:

> *The Bank concurs with this recommendation.*
>
> *The Bank's OCIO has reviewed the agreements with all third-party service providers and has found the Human Resources and Payroll Processing agreement with the General Services Administration is the only such agreement missing the language requested within the OIG's recommendation. Further, the Bank is in the process of reviewing the documentation and draft agreements with the Interior Business Center which will replace the agreement with the GSA. The Bank's OCIO will ensure that the new agreement will specify how information security performance will be measured, reported, and monitored. This effort will be completed by the date of changeover to the IBC HR and payroll processing system, anticipated to be June 2017.*

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 updates all agreements with third-party service providers to ensure that they specify how information security performance is measured, reported, and monitored.

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

Controls are not adequate to ensure that EXIM Bank remediates known configuration-related vulnerabilities in a timely manner. (b) (7)(E)

(b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) . As a result, EXIM Bank's operation of the (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) EXIM Bank management stated that the Bank intends to decommission all (b) (7)(E) (b) (7)(E) by the end of 2016, but were required to continue operating them until then due to current business needs. Bank management also informed us that it was not prioritizing remediation of (b) (7)(E) (b) (7)(E) due to an upcoming FY 2017 migration to (b) (7)(E) as the (b) (7)(E) (b) (7)(E) would be remediated by the upcoming upgrade.

Operating an environment in which (b) (7)(E) In particular, running (b) (7)(E) (b) (7)(E) presents risk from both a security and an operational perspective.

The following guidance is relevant to this control activity:

EXIM Bank Vulnerability Management Program, dated July 8, 2016, states:

> *I. Vulnerability Scanning*
> *We currently use* (b) (7)(E) *for vulnerability scanning.*
> (b) (7)(E)
>
> *II. Identification and prioritization of Vulnerabilities*
> *Identification and prioritization of potential vulnerabilities identified in the scanning reports is a time and labor intensive manual process. IT security specialists review each report for critical, high and moderate vulnerabilities; verify that they are not false positives; and select confirmed vulnerabilities for remediation and/or risk acceptance. We have refined this process so that we can at least avoid analyzing recurring vulnerabilities found by subsequent scans by recording recurrent findings as either "False Positive" or "authorized exceptions" (which applies to potential vulnerabilities for which a remediation does not exist or for which the recommended remediation cannot be deployed for some business or performance reason). Authorized exceptions are authorized for a period of time (up to one year), so that they cannot become permanently authorized.*
>
> *III. Remediation*
> (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 3:

We recommend that the EXIM Bank CIO:

a. Continue with their efforts to (b) (7)(E) 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.

Management's Response:

The Bank concurs with this recommendation.

In October 2016, the Bank's OCIO completed their (b) (7)(E) *by removing the* (b) (7)(E) *. Additionally, the Bank's OCIO will* (b) (7)(E) *on the Bank's network.*

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 (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 identifies and documents deviations from configuration settings. Specifically, we identified (b) (7)(E) that each had (b) (7)(E) deviations from the documented configuration settings. EXIM management was unable to justify these deviations. In addition, EXIM Bank still uses (b) (7)(E) (b) (7)(E)

EXIM management stated that it is in the process of upgrading all (b) (7)(E) (b) (7)(E) and all (b) (7)(E) (b) (7)(E) and that it will (b) (7)(E) Bank management stated that the Bank had a business need for each baseline deviation; however, it had not completely documented these deviations for the (b) (7)(E) (b) (7)(E) because the Bank was in the process of migrating to (b) (7)(E) in FY 2017, which will fully re-baseline the systems.

Without implementing appropriate baseline configuration settings or appropriate management approval where deviations are necessary, EXIM is at increased risk of having insecure settings, which could lead to exploits of known vulnerabilities.

The following guidance is relevant to this control activity:

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 4:

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.

Management's Response:

The Bank concurs with this recommendation.

In FY2016, the Bank's OCIO developed and implemented policy and procedures for change and configuration management for all IT systems. In FY2017, the Bank's OCIO will develop and implement an independent verification process to ensure that baseline configurations with approved deviations are complied with. Any new deviations will proceed through a review and approval process. The Bank expects to have this effort completed by August 1, 2017.

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 Access Management

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.

This weakness exists because EXIM Bank incorporates signing the RoB into their security awareness training, and the Bank's policy states that employees have a 10-day grace period to complete this training. This policy is not in compliance with FISMA and DHS requirements, which state that individuals must provide a signed acknowledgement of their understanding and agreement to abide by the RoB prior to gaining access to federal

information. In addition, EXIM Bank does not follow up on or enforce its internal 10-day grace period, and users can continue to access the network after this period without completing the training or signing the RoB.

Without appropriate controls in place for ensuring that employees sign a RoB prior to obtaining access to the Bank's networks, there is an increased risk of individuals performing inappropriate or unauthorized activities, which could lead to unintentional use, access, and exposure of sensitive data.

The following guidance is relevant for this control activity:

NIST SP 800-53, Rev. 4, *PL-4, Rules of Behavior*, states:

> *Control: The organization:*
> *a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;*
> *b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;*

NIST SP 800-53, Rev. 4, *PS-6, Access Agreements,* states:

> *Control: The organization:*
> *a. Develops and documents access agreements for organizational information systems;*
> *b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and*
> *c. Ensures that individuals requiring access to organizational information and information systems:*
> *1. Sign appropriate access agreements prior to being granted access; and*
> *2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].*

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

Recommendation 5:

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.

Management's Response:

The Bank concurs with this recommendation.

The Bank's OCIO will develop and implement an on-boarding process which requires all users (employees, contractors, temps, and interns) to execute a signed Rules of Behavior Agreement with the Bank prior to being granted any network or system access. The Bank expects to have this effort completed by Apri1 2017.

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 requires all personnel to sign the Bank's RoB agreement before obtaining access to the Bank's data.

Finding: EXIM Bank Should Improve Controls over Role-Based Training

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. Specifically, we noted that the Bank has identified only four roles that have specialized security responsibilities and are required to take role-based security training, including:

- CIO
- Director, IT Security and System Assurance
- Director, Infrastructure Operations
- Information System Security Officer

NIST SP 800-53, Rev. 4 states, "Organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties." We noted that EXIM Bank has not identified the majority of the recommended roles as requiring specialized security training and has not required employees in these roles to take such training.

This weakness exists because management has focused on management-level roles, given the time and cost associated with tracking training for a significantly larger cohort of personnel. Without appropriate security-related training for those involved in security activities, the likelihood that employees will incorrectly configure or manage systems is increased, which in turn increases the overall vulnerability risk to the Bank's systems and data.

The following guidance is relevant to this control activity:

NIST SP 800-53, Rev. 4, *AT-3, Role-Based Security Training*, states:

> *Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:*
> *a. Before authorizing access to the information system or performing assigned duties;*
> *b. When required by information system changes; and*
> *c. [Assignment: organization-defined frequency] thereafter.*
>
> *Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/ procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role- based security training also applies to contractors providing services to federal agencies.*

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

Recommendation 6:

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.

Management's Response:

The Bank concurs with this recommendation.

The Bank's OCIO will define those roles which possess specialized security responsibilities and identify all staff that fit to these roles. The OCIO will develop procedures to ensure that all personnel with specialized security responsibilities revised role based training annually. Implementation of these procedures will be documented with training materials, attendance rosters, and completion dates. The Bank expects to have this effort completed by July 1, 2017.

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 identifies a comprehensive list of all roles requiring specialized security training, and that these individuals receive role-based training annually.

Finding: EXIM Bank Should Improve Controls over the Use of (b) (7)(E)

EXIM Bank has not implemented appropriate controls over the frequency of reviews and updates to (b) (7)(E) . Specifically, we noted that EXIM uses a (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) This frequency does not comply with the documented policy and increases the risk that individuals no longer with the agency could still have knowledge and use of (b) (7)(E) (b) (7)(E) . Additionally, while Bank

(b) (7)(E)

Upon receiving notification of this finding, EXIM management acknowledged the error and stated that the Bank would consider establishing a new policy to change the password more frequently.

The following guidance is relevant to this control activity:

(b) (7)(E)

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

> *Control: The organization:*
> *…*
> *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;*
> *…*
> *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 7:

We recommend that the EXIM Bank CIO implement a review and update of (b) (7)(E) on a frequency that is compliant with EXIM Bank's documented policies and procedures. (b) (7)(E)

Management's Response:

The Bank concurs with this recommendation.

The Bank's OCIO will review their procedures for (b) (7)(E) *for all* (b) (7)(E) *and revise our policy or procedures as needed to ensure that* (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 reviews and (b) (7)(E) in accordance with established Bank policy.

Finding: EXIM Bank Should Improve Controls over APS Account Management

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.

EXIM Bank management stated that the APS application relies on the Infrastructure GSS for single sign-on authentication and therefore relies on the disabling of network accounts to satisfy this control requirement. However, by relying on the GSS rather than implementing application-level controls, there is increased risk that individuals that have an active network account but that no longer require access to the APS application could have unnecessary or excessive privileges within APS.

The following guidance is relevant to this control activity:

APS SSP, *AC-2, Account Management,* states:

Control is Partially Inherited as a Common Control. See Infrastructure SSP/SCM for control implementation descriptions.

The Infrastructure GSS SSP/SCM, AC-2 (1), *Account Management*, states:

For Network access, the Bank, employs automated mechanisms to support the management of network accounts by deactivating dormant accounts after 90 days of inactivity.

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

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

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

Recommendation 8:

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.

Management's Response:

> *The Bank concurs with this recommendation.*
>
> *The Bank's OCIO currently conducts monthly application account reviews and will amend their APS user account management procedures to disable all APS user accounts after 90 days of not being accessed. The Bank expects to have this effort completed by June 1, 2017.*

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 disables all APS accounts after 90 days of inactivity.

Finding: EXIM Bank Should Improve Controls over Software License Management

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 using 33 (b) (7)(E) and (b) (7)(E) licenses in excess of its purchased license amounts.

Bank management stated the Bank's software needs fluctuate, and the Bank routinely exceeds its purchased license amounts in order to meet stakeholder needs. (b) (7)(E) (b) (7)(E) agreement allows the Bank to exceed the purchased license amounts. According to this agreement, at the end of the fiscal year, the Bank is required to "true-up" its licenses by reconciling the active licenses and either purchasing any excess licenses required, or removing them. While Bank management reconciled its software licenses at the end of FY 2016, it did not follow through with purchasing or removing the excess licenses that existed as of September 30, 2016. As a result, the Bank entered FY 2017 with excess licenses.

By not purchasing or removing the excess licenses, the Bank is at increased risk of non-compliance with established vendor agreements.

The following guidance is relevant to this control activity:

OMB M-16-12, *Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing*, dated June 2, 2016, states:

> *FITARA provides new authorities and responsibilities that Chief Information Officers (CIOs) can use to improve their agencies' IT management policies and practices. To improve covered agencies' software management practices, CIOs, in coordination with Chief Acquisition Officers (CAOs) and Chief Financial Officers (CFOs), must take the following steps:*
> *…*
>
> *2) Maintain a continual agency-wide inventory of software licenses, including all licenses purchased, deployed, and in use, as well as spending on subscription services (to include provisional (i.e. cloud) software as a service agreement (SaaS)). Agencies must better understand the true usage of certain types of software.*
>
> *3) Analyze inventory data to ensure compliance with software license agreements, consolidate redundant applications, and identify other cost-saving opportunities.*

NIST SP 800-53, Rev. 4, *CM-10, Software Usage Restrictions,* states:

> *Control: The organization:*
> *a. Uses software and associated documentation in accordance with contract agreements and copyright laws;*
> *b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and*
> *c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.*

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

Recommendation 9:

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.

Management's Response:

The Bank concurs with this recommendation.

The Bank is now in full compliance with the quantities of (b) (7)(E) *software currently owned by the Bank. Further, the OCIO will develop written procedures to implement the process currently used to review compliance with our software license quantities. The Bank expects to have this effort completed by April 1, 2017.*

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 removes all instances of software that have not been properly licensed, and that it implements documented procedures for periodically reviewing and reconciling license quantities.

Federal Laws, Regulations, Policies, and Guidance

As part of our tests of internal controls, we reviewed EXIM Bank's information security program to determine its effectiveness, as prescribed by applicable federal laws and regulations related to information security, including but not limited to:

- Federal Information Security Modernization Act of 2014
- FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.1.3
- NIST SPs and FIPS, particularly:
    - SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
    - SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
    - 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*

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.

Finding	Recommendation	FY Identified	FY 2016 Status
During our FY 2011 testing, we found that EXIM 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, EXIM Bank was not employing PIV multifactor authentication mechanisms for users connecting to the Bank's networks internally. The CIO stated that action had not been taken to implement PIV access to EXIM 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 EXIM Bank had developed a plan for the implementation and use of PIV cards to achieve multifactor authentication for access to the EXIM Bank network and had rolled out a pilot program to begin the implementation. However, this program was still in the testing phase and had not been deployed throughout the agency. For FY 2015, we found that the Bank had completed PIV implementation for logical access for Bank employees; however, this was not fully rolled out until the end of the fiscal year, in September 2015. We also found that the Bank had not yet fully implemented PIV access for all contractors accessing the Bank's	We recommend that the CIO fully implement the use of PIV cards to achieve multifactor authentication to the EXIM Bank network for all access, as required by OMB M-11-11.	2012	Closed

Finding	Recommendation	FY Identified	FY 2016 Status
networks. Until EXIM 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 EXIM Bank has implemented effective account management processes for the Infrastructure GSS.	We recommend that the EXIM 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	Closed
In our FY 2014 FISMA audit report, we found that controls were not adequate to ensure that remote users are timed out or disconnected from the EXIM Bank network in accordance with EXIM Bank policy. Specifically, we found: • Remote connections through the virtual private network (VPN) did not time out. EXIM Bank policy requires remote connections to time out after 30 minutes of inactivity. • Remote connections disconnected after 8 hours. EXIM Bank policy	We recommend that the EXIM 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.	2014	Closed

Finding	Recommendation	FY Identified	FY 2016 Status
requires remote connections to disconnect after 6 hours. • Remote desktop connection settings were set to time out after 1 hour rather than the required 30 minutes. During our FY 2015 testing, we noted that, while the above weaknesses were remediated, controls over remote access still need improvement. Specifically, we noted that remote users are required to use two-factor authentication to log into EXIM Bank's network. After logging on to the VPN (b) (7)(E), users not using an EXIM Bank machine must then remote desktop (RDP) into a Bank machine in order to access Bank resources. However, we found that the system does not force users to log on to RDP to access the network. Non-Bank machines can be configured to skip over the RDP step after successfully connecting to the VPN, instead directly accessing EXIM resources, which violates Bank policy.			
Controls are not adequate to ensure that EXIM Bank data accessible from (b) (7)(E) is adequately protected. In FY 2015, we noted that the Bank has acquired software that will enable it to enforce security controls on (b) (7)(E). This software has been configured and implemented for (b) (7)(E).	We recommend that the EXIM Bank CIO deploy (b) (7)(E) security controls that: 1. (b) (7)(E) 2. Restrict the installation of unapproved or malicious software. 3. Prevent (b) (7)(E) from connecting to internal EXIM Bank resources.	2014	Reissued Numbers 2 and 3 closed; Number 1 remains open

Finding	Recommendation	FY Identified	FY 2016 Status
Controls are not adequate to ensure that all EXIM Bank system security plans (SSPs) are appropriately documented to address all applicable NIST 800-53, Rev. 4 controls. Specifically, we noted that the FMS-NG SSP did not address NIST 800-53, Rev. 4 privacy controls.	We recommend that the EXIM Bank CIO update the FMS-NG SSP to identify and document all applicable NIST SP 800-53, Rev. 4 controls.	2015	Closed
Controls are not adequate to ensure that EXIM Bank has documented configuration management plans that address configuration management requirements for all of its systems. Specifically, we noted that EXIM Bank did not provide configuration management plans for the Infrastructure GSS and (b) (7)(E) systems. The Bank stated that plans did exist; however, the plans were not consistently updated or were outdated. As a result, the Bank would not provide the plans to the auditors. Without appropriate configuration management plans that address how to move changes through change management processes; how to update configuration settings and baselines; how to maintain information system component inventories; how to control development, test, and operational environments; and how to develop, release, and update key documents, the Bank may be susceptible to unauthorized and malicious system changes.	We recommend that the EXIM Bank CIO document configuration management plans for the Infrastructure GSS and (b) (7)(E) systems that: a. Address roles, responsibilities, and configuration management processes and procedures. b. Establish a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items. c. Define the configuration items for the information system and place the configuration items under configuration management. d. Protect the configuration management plan from unauthorized disclosure and modification.	2015	Closed
Controls are not adequate to ensure that the Bank performed appropriate	We recommend that the EXIM Bank CIO ensure that testing of	2015	Closed

Finding	Recommendation	FY Identified	FY 2016 Status
contingency planning activities in FY 2015. Specifically, we found that in FY 2015, the Bank did not perform its annual continuity of operations plan (COOP) exercise that validates the Bank's ability to continue operations in the event of a disaster. The Bank stated that due to a lapse in its authority, resource constraints and re-prioritization prevented it from coordinating and executing the plan. Without validation of COOP capabilities, the Bank may not be aware of the plan's effectiveness or potential weaknesses that require remediation. In addition, there is an increased risk that the Bank will be unable to perform its mission in the event that systems are unavailable for extended periods of time.	the COOP plan is performed on an annual basis to ensure that the Bank is prepared to continue operations and appropriately respond to potential disasters.		
Controls are not adequate to ensure that appropriate POA&M management controls are in place. Specifically, we noted the following: • For the (b) (7)(E) , the Bank had not started addressing POA&Ms (b) (7)(E) nd the scheduled completion dates passed with no milestone updates. • For the (b) (7)(E), the Bank had not started addressing POA&M (b) (7)(E), and the scheduled completion date passed with no milestone updates.	We 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	Reissued

Management Comments

EXIM
EXPORT-IMPORT BANK OF THE UNITED STATES

Reducing Risk. Unleashing Opportunity.

February 24, 2017

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 Mr. McCarthy,

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 2016" dated February 6, 2017 (the "Report"). Management continues to support the OIG's work which complements the Bank's efforts to continually improve its processes. EXIM Bank is proud of the strong and cooperative relationship it has with the OIG.

The OIG contracted with Cotton & Company, LLP ("Cotton") to conduct a performance audit of the Bank's security programs and practices. The Bank appreciates Cotton recognizing that "the Bank has addressed several of the challenges identified during previous fiscal year FISMA audits" and that the "Bank improved the controls around the account management process for the Infrastructure General Support System (GSS); improved remote access timeout configurations; and adequately documented and updated its configuration management plans for the Infrastructure GSS and (b) (7)(E) The Bank also appreciates the assurance that while the overall score for its information security program begins at a Level 2 based on the newly implemented DHS FY2016 IG FISMA Metrics, the Bank has effectively implemented 11 of the 14 NIST SP 800-53, Rev. 4 controls.

The OIG, through Cotton, has made nine new recommendations to further enhance current policies to protect and improve the information and information systems, increase its effectiveness, and to fulfill the responsibilities as outlined in FISMA. The Bank concurs with all nine recommendations and will move forward with implementing the recommendations.

Recommendation 1: 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.

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

Management Response: The Bank concurs with this recommendation.

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

The Bank's Office of Chief Information Officer (OCIO) will 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.

OCIO will conduct a gap analysis and once these gaps are identified, they will be triaged on those gaps that are at a higher level of priority than others and will then estimate the cost and level of effort required to close these gaps. The implementation will be a multi-year effort. The Bank's OCIO anticipates having a prepared assessment and initial plan by September 1, 2017.

Regarding the second part of the recommendation, OCIO will develop processes and procedures required to enhance the Bank's IT security program in order to achieve level 4 in the Maturity Model across the board.

Recommendation 2: 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.

Management Response: The Bank concurs with this recommendation.

The Bank's OCIO has reviewed the agreements with all third-party service providers and has found the Human Resources and Payroll Processing agreement with the General Services Administration is the only such agreement missing the language requested within the OIG's recommendation. Further, the Bank is in the process of reviewing the documentation and draft agreements with the Interior Business Center which will replace the agreement with the GSA. The Bank's OCIO will ensure that the new agreement will specify how information security performance will be measured, reported, and monitored. This effort will be completed by the date of changeover to the IBC HR and payroll processing system, anticipated to be June 2017.

Recommendation 3: We recommend that the EXIM Bank CIO:

1. Continue with their efforts to (b) (7)(E) to reduce their exposure to vulnerabilities that cannot be remediated.
2. (b) (7)(E) that exist across all operating platforms in the Bank's network environment.

Management Response: The Bank concurs with this recommendation.

In October 2016, the Bank's OCIO completed (b) (7)(E)

(b) (7)(E)

Recommendation 4: We recommend that the EXIM Bank CIO:

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

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

Management Response: The Bank concurs with this recommendation.

In FY2016, the Bank's OCIO developed and implemented policy and procedures for change and configuration management for all IT systems. In FY2017, the Bank's OCIO will develop and implement an independent verification process to ensure that baseline configurations with approved deviations are complied with. Any new deviations will proceed through a review and approval process. The Bank expects to have this effort completed by August 1, 2017.

Recommendation 5: We recommend that the EXIM Bank CIO:

1. Update their on-boarding process to separate the acknowledgement of the RoB from 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.

2. Implement procedures to formally track compliance with the updated process.

Management Response: The Bank concurs with this recommendation.

The Bank's OCIO will develop and implement an on-boarding process which requires all users (employees, contractors, temps, and interns) to execute a signed Rules of Behavior Agreement with the Bank prior to being granted any network or system access. The Bank expects to have this effort completed by April 2017.

Recommendation 6: We recommend that the EXIM Bank CIO:

1. Identify and document a comprehensive list of all roles with information security responsibilities.

2. Document and implement procedures to ensure that all of the identified roles receive annual role-based security training.

Management Response: The Bank concurs with this recommendation.

The Bank's OCIO will define those roles which possess specialized security responsibilities and identify all staff that fit to these roles. The OCIO will develop procedures to ensure that all personnel with specialized security responsibilities revised role based training annually. Implementation of these procedures will be documented with training materials, attendance rosters, and completion dates. The Bank expects to have this effort completed by July 1, 2017.

Recommendation 7: We recommend that the EXIM Bank CIO implement a review and update of (b) (7)(E) 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 (b) (7)(E)

Management Response: The Bank concurs with this recommendation.

The Bank's OCIO will review their procedures for changing (b) (7)(E) (b) (7)(E) vise our policy or procedures as needed to ensure (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E)

Recommendation 8: 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.

Management Response: The Bank concurs with this recommendation.

The Bank's OCIO currently conducts monthly application account reviews and will amend their APS user account management procedures to disable all APS user accounts after 90 days of not being accessed. The Bank expects to have this effort completed by June 1, 2017.

Recommendation 9: We recommend that the EXIM Bank CIO:

1. 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.

2. 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.

Management Response: The Bank concurs with this recommendation.

The Bank is now in full compliance with the quantities of (b) (7)(E) software currently owned by the Bank. Further, the OCIO will develop written procedures to implement the process currently used to review compliance with our software license quantities. The Bank expects to have this effort completed by April 1, 2017.

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

Recommendation: In our FY 2014 FISMA audit report, we recommended that the EXIM Bank CIO deploy (b) (7)(E)

1. (b) (7)(E)

2. Restrict the installation of unapproved or malicious software.

3. Prevent unauthorized (b) (7)(E) from connecting to internal EXIM Bank resources.

As of FY 2016, Recommendation 1 still remains open; we are therefore not issuing any new recommendations related to this finding. See Appendix A for a complete listing of the status of prior-year FISMA audit findings.

Management Response: The Bank concurs with this recommendation.

OCIO will address #1 of the remaining open recommendation to (b) (7)(E)
(b) (7)(E) (b) (7)(E)
(b) (7)(E)
(b) (7)(E) The Bank expects to have this effort completed by April 1, 2017.

Recommendation: In our FY 2015 FISMA audit report, we recommended that the EXIM Bank CIO implement a process to ensure that the Bank reviews all system POA&Ms at an organization-defined frequency, and that it updates milestones to reflect actions taken to remediate POA&M items.

As of FY 2016, the recommendation noted remains open; we are therefore not issuing any new recommendations related to this finding. See Appendix A for a complete listing of the status of prior-year FISMA audit findings.

Management Response: The Bank concurs with this recommendation.

The Bank's OCIO will implement a process to review and update system POA&Ms by adding a new column to our POA&M tracking spreadsheet to provide up-to-date information regarding open POA&Ms which are at risk of not meeting their scheduled completion dates and for which an approved remediation plan does not yet exist. This will permit management to make the POA&M process consistent, while making it transparent when a remediation is not completed when planned. The new information column in the POA&M spreadsheet will be added and in use by March 15, 2017.

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

Sincerely,

Charles J. Hall
Chairman of the Board of Directors and President (Acting)
Export-Import Bank of the United States

APPENDIX C

Selected Security Controls and Testing Results

800-53 Control	Control Title	System	Results
AC-2	Account Management	APS	Controls are not effective
AU-2	Audit Events	APS	Controls are effective
AU-6	Audit Review, Analysis, and Reporting	APS	Controls are effective
CM-2	Baseline Configuration	APS	Controls are effective
CM-3	Configuration Change Control	APS	Controls are effective
CM-6	Configuration Settings	APS	Controls are not effective
IA-2	Identification and Authentication	APS	Controls are effective
CM-8	Information System Component Inventory	GSS	Controls are effective
CM-10	Software Usage Restrictions	GSS	Controls are not effective
CM-11	User-Installed Software	GSS	Controls are effective
MP-1	Media Protection Policy and Procedures	GSS	Controls are effective
MP-2	Media Access	GSS	Controls are effective
MP-4	Media Storage	GSS	Controls are effective
MP-5	Media Transport	GSS	Controls are effective

DHS FY 2016 IG FISMA Metrics Results

The following tables represent each of the NIST Cybersecurity Framework domains that we reviewed to respond to the FY 2016 IG FISMA Metrics. Each of the five domain areas (Identify, Protect, Detect, Respond, and Recover) had specific control objectives that we evaluated, and each objective was associated with a maturity level. The tables below represent the number of objectives that we evaluated for each Cybersecurity Framework, their associated maturity level, and whether the control objective was "met" or "not met." The number of control objectives "met" for each level within the respective domains determined the overall score for that domain. Per DHS' FY 2016 IG FISMA metrics, only agency programs that score at or above Level 4: Managed and Measureable (13 points) for a NIST Framework Function have effective programs within that area.

Furthermore, the point allotment for each level of maturity is determined by meeting all of the requirements in the previous level(s), and half or more of the level currently under assessment. For example, an agency is considered to be at level 3 if it has met all of the level 1 and level 2 requirements and half or more of the level 3 requirements.

Identify

Level	Met	Not Met	%	Points	Possible
Level 1: Ad-hoc	0	0	100%	3	3
Level 2: Defined	2	2	50%	4	4
Level 3: Consistently Implemented	9	2	82%		6
Level 4: Managed and Measureable	5	1	83%		5
Level 5: Optimized	Achieve 100% of Level 4 Capabilities				2
Level 2: Defined		**Effective**	No	**7**	20

Protect

Level	Met	Not Met	%	Points	Possible
Level 1: Ad-hoc	0	0	100%	3	3
Level 2: Defined	2	3	40%		4
Level 3: Consistently Implemented	12	6	67%		6
Level 4: Managed and Measureable	6	2	75%		5
Level 5: Optimized	Achieve 100% of Level 4 Capabilities				2
Level 1: Ad-hoc		**Effective**	No	**3**	20

Detect

Level	Met	Not Met	%	Points	Possible
Level 1: Ad-hoc	10	0	100%	3	3
Level 2: Defined	8	2	80%	4	4
Level 3: Consistently Implemented	1	9	10%		6

Level 4: Managed and Measureable	0	12	0%		5
Level 5: Optimized	0	7	0%		2
Level 2: Defined		**Effective**	No	**7**	20

Respond

Level	Met	Not Met	%	Points	Possible
Level 1: Ad-hoc	12	0	100%	3	3
Level 2: Defined	8	4	67%	4	4
Level 3: Consistently Implemented	3	10	23%		6
Level 4: Managed and Measureable	0	9	0%		5
Level 5: Optimized	0	8	0%		2
Level 2: Defined		**Effective**	No	**7**	20

Recover

Level	Met	Not Met	%	Points	Possible
Level 1: Ad-hoc	0	0	100%	3	3
Level 2: Defined	2	0	100%	4	4
Level 3: Consistently Implemented	6	0	100%	6	6
Level 4: Managed and Measureable	3	0	100%	5	5
Level 5: Optimized	Achieve 100% of Level 4 Capabilities			2	2
Level 5: Optimized		**Effective**	Yes	**20**	20

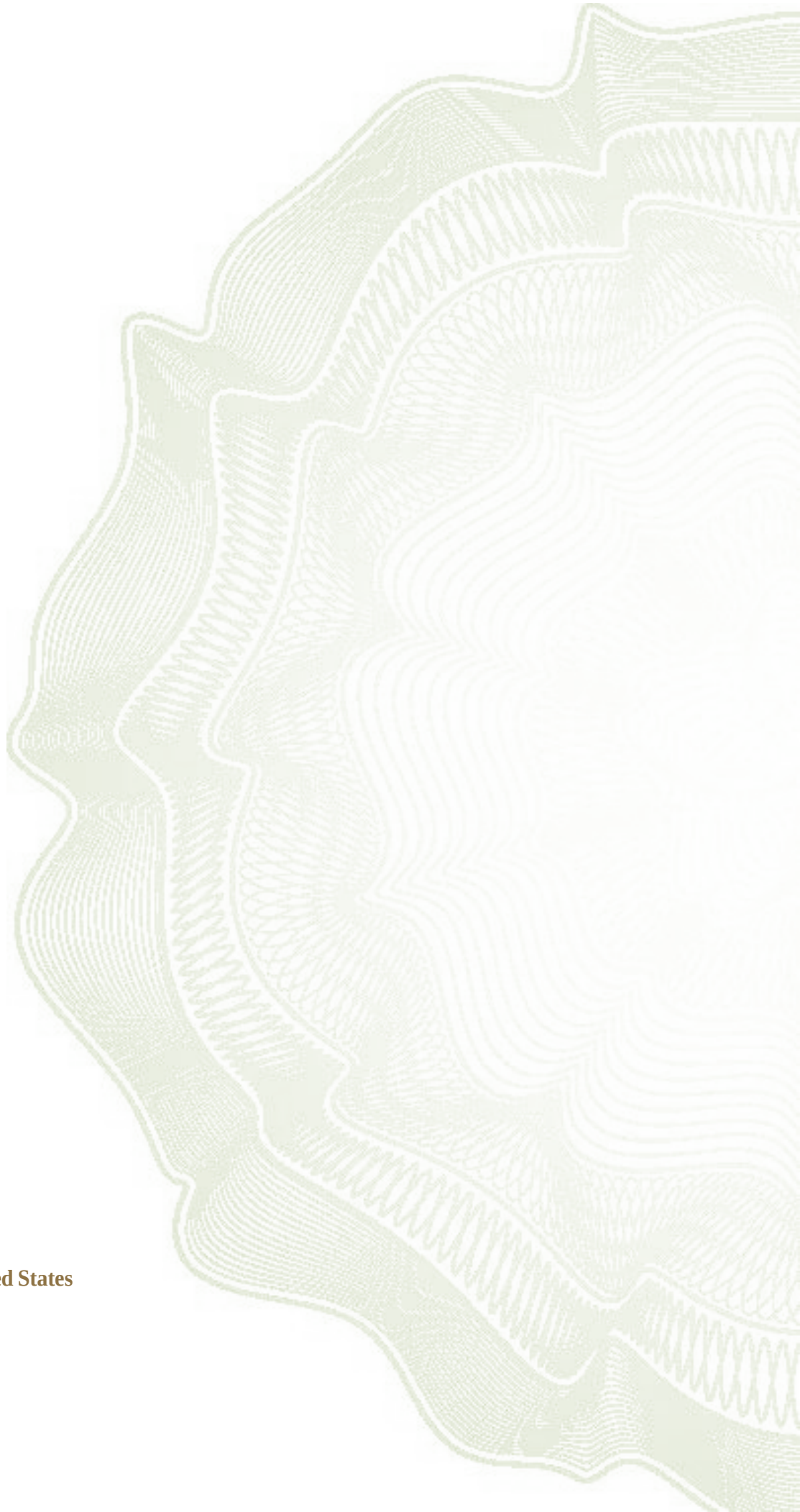
Area	Level	Points	Possible	Effective
Identify	Level 2: Defined	7	20	No
Protect	Level 1: Ad-hoc	3	20	No
Detect	Level 2: Defined	7	20	No
Respond	Level 2: Defined	7	20	No
Recover	Level 5: Optimized	20	20	Yes
Total		**44**	100	
	Effective	No		

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

Email:	IGhotline@exim.gov
Telephone:	1-888-OIG-EXIM (1-888-644-3946)
Fax:	(202) 565-3988
Address:	Office of Inspector General Export-Import Bank of the United States 811 Vermont Avenue, NW Suite 138 Washington, DC 20571

Comments and Suggestions

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



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