EXIM
EXPORT-IMPORT BANK
OF THE UNITED STATES

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

Independent Audit of the Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2018

March 13, 2019
OIG-AR-19-03

Information about specific vulnerabilities in IT systems has been redacted from the publicly released version of this report. The information withheld was compiled in connection with OIG law enforcement responsibilities and consists of information that, if released publicly, could lead to the circumvention of the law.

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

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

This audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives.

To: Howard Spira, Senior Vice President and Chief Information Officer

From: Jennifer Fain, Acting Assistant Inspector General for Audits and Evaluations

Subject: Independent Audit of Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2018 (OIG-AR-19-03)

Date: March 13, 2019

This memorandum transmits KPMG LLP's (KPMG) audit report on the Export-Import Bank's (EXIM Bank) Information Security Program for Fiscal Year 2018. Under a contract monitored by this office, we engaged the independent public accounting firm of KPMG to perform the audit. The contract required the audit to be performed in accordance with generally accepted government auditing standards.

We appreciate the cooperation and courtesies provided to KPMG and this office during the audit. If you have questions, please contact me at (202) 565-3439 or jennifer.fain@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.

March 6, 2019

Jennifer Fain
Acting Inspector General for Audits and Evaluations
Export Import Bank of the United States
811 Vermont Avenue, NW
Washington, DC 20571

Re: Independent Audit on the Effectiveness of the Export-Import Bank of the United States' Information Security Program and Practices Report – Fiscal Year 2018

Dear Ms. Fain,

We are pleased to submit this report, which presents the results of our independent audit of the Export Import Bank of the United States (EXIM or the Bank) information security program and practices and compliance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires federal agencies, including EXIM, to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility for the collection of annual FISMA responses to the Department of Homeland Security (DHS). DHS, in conjunction with OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), developed the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* Version 1.0.1, dated May 24, 2018 (FY 2018 IG FISMA Reporting Metrics). The EXIM Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct this independent audit. The OIG monitored our work to ensure generally accepted government auditing standards (GAGAS) and contractual requirements[1] were met.

We conducted this performance audit in accordance with GAGAS.[2] 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.

The objective for this independent audit was to determine whether EXIM developed and implemented an effective information security program and practices as required by

[1] Contract No. GS-00F-275CA, Task Order 83310118F0016, dated March 22, 2018

[2] In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

FISMA. To determine whether EXIM developed and implemented an effective information security program and practices for the period of October 1, 2017 to September 30, 2018, we evaluated the Bank's security plans, policies, and procedures in place for effectiveness as required by applicable federal laws and regulations, and guidance issued by OMB and the National Institute of Standard and Technology (NIST).

We based our work on a selection of EXIM-wide security controls and a selection of system-specific security controls across two selected EXIM information systems and one EXIM contractor information system. As part of our audit, we responded to the DHS FY 2018 IG FISMA Reporting Metrics and assessed the maturity levels on behalf of EXIM OIG. Additional details regarding the scope of our independent audit are included in the **Objective, Scope, and Methodology** section and **Appendix A,** *Scope and Methodology.* **Appendix B**, *Status of Prior-Year Recommendations,* summarizes EXIM's progress in addressing prior-year recommendations.

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, EXIM established and maintained its information security program and practices for its information systems for the five Cybersecurity Functions[3] and eight FISMA Metric Domains.[4] During the past year, EXIM implemented corrective actions to remediate prior-year deficiencies over vulnerability management, baseline configurations, information assurance monitoring, and firewall capabilities. Additionally, the Bank effectively designed and implemented 12 of 13 controls from NIST Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, that we tested for a selected information system and contractor information system. When we assessed EXIM's information security program against the DHS FY 2018 IG FISMA Reporting Metrics, we found that the Cybersecurity Functions' Identify, Protect, and Detect scored at Level 3: Consistently Implemented, and Respond and Recover scored at Level 2: Defined. As stipulated by the FY 2018 IG FISMA Reporting Metrics, an information security program is effective when a majority of the five Cybersecurity Functions score Level 4: Managed and Measurable. Since the majority of EXIM's Cybersecurity Functions scored at a Level 3: Consistently Implemented, the information security program was considered not effective. Further, we identified deficiencies within four of the five Cybersecurity Functions for four of the eight FISMA program areas. Specifically, we noted the following:

---

[3] OMB, DHS, and CIGIE developed the FY 2018 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. In FY 2018, the eight IG FISMA Metric Domains were aligned with the five Cybersecurity Functions of Identify, Protect, Detect, Respond, and Recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[4] As described in the FY 2018 IG FISMA Reporting Metrics, Version 1.0.1, May 24, 2018, the eight FISMA Metric Domains are: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

Cybersecurity Function: Identify
1. Risk management policies and procedures need improvement. (Risk Management)

Cybersecurity Function: Detect
2. Information security continuous monitoring program was not fully established. (Information Security Continuous Monitoring)

Cybersecurity Function: Respond
3. Incident handling policies and procedures were not completely documented. (Incident Response)

Cybersecurity Function: Recover
4. Contingency planning program needs improvement. (Contingency Planning)

We considered these finding when we assessed the maturity levels for the FY 2018 IG FISMA Reporting Metrics. We provided 14 recommendations related to these four control deficiencies that, if effectively addressed by management, should strengthen the respective information systems and EXIM's information security program.

KPMG did not render an opinion on EXIM's internal controls over financial reporting or over financial management systems as part of this performance audit. We caution that projecting the results of our performance audit to future periods or other EXIM information systems not included in our selection is subject to the risk that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate. This report is intended solely for the information and use of the EXIM and the OIG, and is not intended to be, and should not be used by anyone other than these specified parties.

Sincerely,

KPMG LLP

March 6, 2019

TABLE OF CONTENTS

TABLE OF CONTENTS 4
LIST OF FIGURES AND TABLES 5
ABBREVIATIONS AND GLOSSARY 6
INTRODUCTION 8
OBJECTIVE, SCOPE, AND METHODOLOGY 8
BACKGROUND 8
AUDIT RESULTS 12
FINDINGS 13
Finding 1: Risk management policies and procedures need improvement. (Identify Function – RM) 13
Finding 2: Information security continuous monitoring program was not fully established (Detect Function – ISCM) 17
Finding 3: Incident handling policies and procedures were not completely documented. (Respond Function – IR) 20
Finding 4: Contingency planning program needs improvement. (Recover Function – CP) 22
CONCLUSION 25
APPENDICES 27
Appendix A: Scope and Methodology 27
Appendix B: Federal Laws, Regulations, and Guidance 30
Appendix C: Status of Prior-Year Recommendations 31
Appendix D: Management's Response 34
Appendix E: Security Controls Selection 39
Appendix F: DHS FY 2018 IG FISMA Metric Results 40
Appendix G: System Selection Approach 50
Appendix H: Distribution List 51

LIST OF FIGURES AND TABLES

Table 1. Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2018 IG FISMA Metric Domains

Table 2. Inspector General Assessed Maturity Levels

Table 3. Prior Year Findings – 2017 Evaluation

Table 4. Selected Security Controls and Testing Results

Table 5. EXIM FY 2018 IG FISMA Reporting Metric Results

ABBREVIATIONS AND GLOSSARY

ATO	Authority to Operate
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CIO	Chief Information Officer
CIGIE	Council of Inspectors General on Integrity and Efficiency
CRO	Chief Risk Officer
DHS	Department of Homeland Security
DRP	Disaster Recovery Plan
EOL	EXIM Online
EXIM	Export-Import Bank of the United States
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
ICT	Information and Communications Technology
IG	Inspector General
ISCP	Information System Contingency Plan
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
PII	Personally Identifiable Information

PIV	Personal Identity Verification
ROB	Rules of Behavior
SA&A	Security Authorization and Accreditation
SAR	Security Assessment Report
SP	Special Publication
SSP	System Security Plan
TTE	Training, Testing, and Exercises

INTRODUCTION

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

This report presents the results of the independent audit conducted by KPMG, LLP (KPMG) on the effectiveness of the information security program and practices of the Export-Import Bank (EXIM or the Bank) for fiscal year (FY) 2018. The objective was to determine whether EXIM Bank developed and implemented effective information security program and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA).

OBJECTIVE, SCOPE, AND METHODOLOGY

As stated, the objective of the audit was to determine whether EXIM Bank developed and implemented an effective information security program and practices as required by FISMA for the fiscal year ending September 30, 2018. To address our objective, we evaluated the Bank's security program, plans, policies, and procedures in place for effectiveness as required by applicable federal laws and regulations, guidance issued by the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). We tested security controls for (b) (7)(E) and performed the detailed steps prescribed in the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2018 IG FISMA Reporting Metrics), version 1.0.1, dated May 24, 2018, to evaluate EXIM's policies, procedures, and practices for Identify – Risk Management (RM); Protect – Configuration Management (CM), Identity and Access Management (IA), Data Protection and Privacy (DP), and Security Training (ST); Detect – Information Security Continuous Monitoring (ISCM); Respond – Incident Response (IR); and Recover – Contingency Planning (CP). Finally, we followed up on the status of prior-year FISMA findings. See **Appendix A** for more details on the scope and methodology.

BACKGROUND

EXIM is an independent, self-sustaining executive agency and a wholly-owned United States government corporation. EXIM'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 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's network infrastructure consists largely of networking devices with various servers running different operating system platforms. Standard desktop personal computers and laptops run (b) (7)(E) The networks are protected from external threats by a range of information technology security devices, including data loss prevention tools, firewalls, intrusion detection and prevention systems, antivirus, and spam-filtering systems.

Federal Laws, Roles, and Responsibilities. On December 17, 2002, the President signed into law the E-Government Act (Public Law 107-347), which included the Federal Information Security Management Act of 2002. FISMA, as amended,[5] permanently reauthorized the framework established in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA continues the annual review and reporting requirements introduced in GISRA. In addition, FISMA includes new provisions aimed at further strengthening the security of the federal government's information and information systems, such as the development of minimum standards for agency systems. NIST has been tasked to work with federal agencies in the development of those standards. NIST issues these standards and guidelines as Federal Information Processing Standards (FIPS) and Special Publications. FIPS provide the minimum information security requirements that are necessary to improve the security of federal information and information systems, and the Special Publication (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.

[5] The Federal Information 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) sets forth authority for the Secretary of the DHS to administer the implementation of such policies and procedures for information systems.

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 Chief Information Officers and Senior Agency Information Security Officers, to report the security status of their information systems to DHS and OMB, which is accomplished through DHS' CyberScope tool. CyberScope, operated by DHS on behalf of OMB, replaces the legacy paper-based submission process and automates agency reporting. In addition, OIGs provide an independent assessment of effectiveness of an agency's information security program. OIGs must also report their results to DHS and OMB annually through CyberScope.

FY 2018 IG FISMA Reporting Metrics. DHS revised the FY 2017 IG FISMA Reporting Metrics and issued the FY 2018 IG FISMA Reporting Metrics, Version 1.0.1. on May 24, 2018. DHS created the metrics for 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 Cybersecurity Functions[6] outlined in the NIST Cybersecurity Framework[7] and are intended to provide agencies with a common structure for identifying and managing cybersecurity risks across the enterprise, as well as to provide IGs with guidance for assessing the maturity of controls to address those risks. In addition, CIGIE implemented maturity models for Risk Management, Configuration Management, Identity and Access Management, Security Training, and Contingency Planning, which were similar to the Information Security Continuous Monitoring and Incident Response maturity models that were instituted in FY 2015 and FY 2016, respectively. In FY 2018, CIGIE added the Data Protection and Privacy FISMA Metric Domain, which included five additional questions. See

[6] In *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.0, NIST created Functions to organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

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

Table 1 below for a description of the NIST Cybersecurity Framework Security Functions and the associated FY 2018 IG FISMA Metric Domains.

Table 1: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2018 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2018 IG FISMA Metric Domains
Identify	Risk Management (RM)
Protect	Configuration Management (CM) Identity and Access Management (IA) Data Protection and Privacy (DP) Security Training (ST)
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response (IR)
Recover	Contingency Planning (CP)

The maturity models have five levels: Level 1: Ah-Hoc, Level 2: Defined, Level 3: Consistently Implemented, Level 4: Managed and Measurable, and Level 5: Optimized. The maturity level for a domain is determined by a simple majority, with the most frequently assessed level across the questions serving as the domain rating. A security program is considered effective if the majority of the FY 2018 IG FISMA Reporting Metrics are at Level 4: Management and Measurable. **Table 2** provides the descriptions for each maturity level.

Table 2: Inspector General Assessed Maturity Levels

Maturity level	Maturity Level Description
Level: 1 Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level: 2 Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.

Maturity level	Maturity Level Description
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

AUDIT RESULTS

Consistent with applicable FISMA requirements, OMB's policy and guidance, the NIST standards and guidelines, and FIPS, EXIM's information security program and practices for its unclassified systems were established and have been maintained for the five Cybersecurity Functions and eight FISMA Metric Domains. During the past year, EXIM implemented corrective actions to remediate prior-year deficiencies over vulnerability management, baseline configurations, information assurance monitoring, and firewall capabilities. However, we found the program was not effective as a result of a majority of FY 2018 IG FISMA Reporting Metrics for the five Cybersecurity Functions did not score Level 4: Managed and Measurable, as prescribed by DHS criteria. Furthermore, we found deficiencies within four of the five Cybersecurity Functions and four of eight FISMA Metric Domains that need improvement. The deficiencies over RM policies and procedures, the ISCM program, incident handling policies and procedures, and CP program are described in the *Findings* section below.

For each of the FY 2018 IG FISMA Reporting Metrics, EXIM management generally assessed the maturity level of its information security program as a Level 3: Consistently Implemented using DHS' scoring methodology (a five-level maturity model scale). When we assessed EXIM's information security program for each of the FY 2018 IG FISMA Reporting Metrics, we found that the Identify, Protect,[8] Detect, Cybersecurity Functions scored at Level 3: Consistently Implemented, and Respond and Recover scored at Level 2: Defined. Therefore, EXIM's information security program is considered not effective, as stipulated by DHS' scoring methodology (i.e., EXIM did not score Level 4: Managed and Measurable for a majority of the FY 2018 IG FISMA Reporting Metrics). To achieve an effective information security program as stipulated by DHS guidance, EXIM should develop and implement practices that address Level 4: Managed and Measurable metrics. A summary of the results for the DHS FY 2018 IG FISMA Reporting Metric assessment is in **Appendix F.**

By not having a mature and effective information security program, EXIM 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.

[8] We assessed three of nine Identify and Access Management metrics and two of six Security Training metrics as Level 4: Managed and Measurable. See **Appendix E.**

Additionally, the Bank effectively designed and implemented 12 of 13 NIST Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* controls that we tested for (b) (7)(E).

We provided recommendations related to the identified control deficiencies that, if effectively addressed by management, should strengthen the respective information systems and EXIM's information security program.

As noted above, we evaluated the open prior-year findings from the FY 2016 and FY 2017 FISMA performance audits and noted management took sufficient action to close all four recommendations. See **Appendix C***, Status of Prior-Year Findings*, for additional details.

In a written response to this report, the EXIM Chief Information Officer (CIO) concurred with our findings and recommendations (see **Appendix D**, *Management Response)*.

FINDINGS

Finding 1: Risk management policies and procedures need improvement. (Identify Function – RM)

During FY 2018, we noted that the controls and processes were effective for the following RM areas: information security architecture, Plans of Action and Milestones (POA&Ms), developer security testing and evaluation, supply chain protections, risk management roles and responsibilities, system level risk assessments, communication of information about risks, and monitoring of contractor system security controls. However, NIST SP 800-53 requires organizations to develop security policies, procedures, and plans for the information system that (1) address NIST's security control requirements, (2) are consistent with the organization's enterprise structure, and (3) are updated to address changes to the information system/environment of operation. EXIM's RM policies and procedures did not consistently address the following NIST SP 800-53, Rev. 4, security controls:

- Risk Assessment Policy and Procedures (RA-1),
- Configuration Management Policy and Procedures (CM-1),
- Information System Component Inventory (CM-8),
- Continuous Monitoring (CA-7), and
- Information System Documentation (SA-5).

The configuration management process inherently affects the hardware and software assets within the Bank. Consequently, management not having a properly documented inventory of their current assets affects the completeness and effectiveness of change management policies and procedures. Without a complete listing of assets used at the Bank, proper policies and procedures cannot be established for continuous monitoring to ensure that all assets are monitored. An essential component of a RM program is monitoring of current assets.

Specifically, EXIM management did not:

- Document the (b) (7)(E) , including policies, procedures, and plans and/or strategies to identify (b) (7)(E) within the Bank's infrastructure.

- Define mission and business process considerations for information security within (b) (7)(E) and ensuring that they fully align with the requirements noted within SA-5.

During FY 2018, management was (b) (7)(E) therefore, (b) (7)(E) for the entire fiscal period, a deficiency was noted.

Due to competing priorities, including the remediation of prior-year deficiencies, updating of legacy controls, and transitioning of essential staff, management was not able to adequately (b) (7)(E) across the organization for the full fiscal year.

Without a fully documented (b) (7)(E) for the majority of the fiscal year that aligns to (b) (7)(E) , the Bank may not be able to assess and address (b) (7)(E) . Additionally, without an effective program to identify and define (b) (7)(E) , the Bank may not adequately protect its (b) (7)(E) , exposing the organization to potential vulnerabilities and threats.

The following guidance is relevant to this deficiency:

- NIST SP 800-53, Rev. 4, includes the following RM controls:

  RA-1: Risk Assessment Policy and Procedures
  The organization:
  a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
  b. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency].

  CM-1: Configuration Management Policy and Procedures
  The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
b. Reviews and updates the current: 1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency].

CA-7: Continuous Monitoring
The organization:
a. Establishment of [Assignment: organization-defined metrics] to be monitored;
b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
c. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
d. Correlation and analysis of security-related information generated by assessments and monitoring;
e. Response actions to address results of the analysis of security-related information; and
f. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

CM-8: Information System Component Inventory
The organization:
a. Develops and documents an inventory of information system components that: 1. accurately reflects the current information system; 2. includes all components within the authorization boundary of the information system; 3. is at the level of granularity deemed necessary for tracking and reporting; and 4. includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

SA-5: Information System Documentation
The organization:
a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3.

Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service;
c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response;
d. Protects documentation as required, in accordance with the risk management strategy; and
e. Distributes documentation to [Assignment: organization-defined personnel or roles].

We recommend that EXIM management:

1. Formally document (b) (7)(E) that address the NIST SP 800-53, Revision 4, RA-1, CM-1, CM-8, CA-7, and SA-5 security controls.

2. Document the current (b) (7)(E) , including policies, procedures, and plans and/or strategies to (b) (7)(E)

3. Address mission and business process considerations for information security in (b) (7)(E) .

Management's Response:

EXIM finalized a Risk Management Program during the fiscal year. EXIM has updated the documentation (b) (7)(E) *to include policies and procedures to identify* (b) (7)(E) *infrastructure. EXIM fully established and implemented a hardware and software asset management* (b) (7)(E) *inventory for EXIM Bank.* (b) (7)(E)

.

Evaluation of Management's Response: If implemented properly, we believe that process management as defined above for remediating this issue will improve the Bank's RM program.

Finding 2: Information security continuous monitoring program was not fully established (Detect Function – ISCM)

During FY 2018, we noted that controls and processes were effective over the following ISCM areas: roles and responsibilities, (b) (7)(E) . Although EXIM management developed the FY 2018 ISCM Strategy in July 2018, it was not in place for the majority of the fiscal year (nine of 12 months), and management had not (b) (7)(E) Therefore, for the majority of FY 2018, EXIM's ISCM did not have formal policy and practices in place to consistently address the following areas: ongoing (b) (7)(E) , which are required as part of FY 2018 IG FISMA Reporting Metric 47.

Additionally, EXIM had not fully established its ISCM program. Specifically, we noted:

- The Bank's ISCM strategy did not define ISCM requirements and activities at each organizational tier to facilitate an organization-wide approach, as stipulated within FY 2018 IG FISMA Reporting Metric 46. Additionally, (b) (7)(E)

- The Bank did not fully implement a security information and event management (SIEM) software product. Currently, the Bank uses (b) (7)(E)

Due to competing priorities, including the remediation of prior-year deficiencies, updating of legacy controls, and transitioning of essential staff, management was not able to adequately define and implement policies and procedures related to continuous monitoring at the Bank. In addition, the DHS CM program was delayed; although, EXIM has been pro-active by participating in the pilot program.

Without establishing a fully comprehensive information system continuous monitoring program, EXIM may not have full capabilities in place to assess critical information

(b) (7)(E)

contained in security reports or plans (i.e., security incident and event management plans, compliance reporting, and POA&Ms) on an ongoing basis.

The following guidance is relevant to this deficiency:

- NIST SP 800-53, Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations,* includes the following security control requirements:

  CA-7: Continuous Monitoring Security Control
  The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
  a. Establishment of [Assignment: organization-defined metrics] to be monitored;
  b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
  c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
  d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
  e. Correlation and analysis of security-related information generated by assessments and monitoring;
  f. Response actions to address results of the analysis of security-related information; and
  g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

  SI-4: Information System Monitoring Security Control
  The organization:
  a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections;
  b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
  c. Deploys monitoring devices: 1. strategically within the information system to collect organization-determined essential information; and 2. at ad hoc locations within the system to track specific types of transactions of interest to the organization;
  d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
  e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

AU-6: Audit Review, Analysis, and Reporting Security Control
The organization:
a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
b. Reports findings to [Assignment: organization-defined personnel or roles].

NIST SP 800-53, Rev. 4 also states, "The organization tracks and documents information system security incidents."

- NIST SP 800-137, Rev. 1, *Information Security Continuous Monitoring for Federal Information Systems and Organizations, Section 2.3,* states:
  Consideration is given to ISCM tools that:
  - Pull information from a variety of sources
  - Use open specifications such as the Security Content Automation Protocol (SCAP);
  - Offer interoperability with other products such as help desk, inventory management, configuration management, and incident response solutions;
  - Support compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines;
  - Provide reporting with the ability to tailor output and drill down from high-level, aggregate metrics to system-level metrics; and
  - Allow for data consolidation into Security Information and Event Management (SIEM) tools and dashboard products.

- OMB-14-03, *Enhancing the Security of Federal Information and Information Systems*, states on [page 6]:

  The ISCM strategies shall address all security controls selected and implemented by agencies, including the frequency of and degree of rigor associated with the monitoring process. ISCM strategies, which must be approved by the appropriate agency authorizing official, shall also include all common controls inherited by organizational information systems. Additionally, all strategies must address the agencies' plans for transitioning to and maintaining consistency with Federal information security policies, standards, and guidelines. Agency officials shall monitor the security state of their information systems and the environments in which those systems operate on an ongoing basis with a frequency sufficient to

make ongoing risk-based decisions on whether to continue to operate the systems within their organizations.

We recommend that EXIM management:

4. Update the ISCM policies, procedures, and strategy to include the following: (b) (7)(E)

5. Update the ISCM procedures, and strategy to include and (b) (7)(E)

6. Establish (b) (7)(E) to measure the effectiveness of the ISCM program.

7. Complete the (b) (7)(E) and (b) (7)(E) to analyze event data in real time for the (b) (7)(E) compliance.

Management's Response:

EXIM updated the ISCM related policies and procedures during the fiscal year to align with the applicable NIST and DHS guidelines. (b) (7)(E)

EXIM has established (b) (7)(E) *the effectiveness of the ISCM program.*

Evaluation of Management's Response: If implemented properly, we believe that process management as defined above for remediating this issue will assist in establishing a complete ISCM program.

Finding 3: Incident handling policies and procedures were not completely documented. (Respond Function – IR)

During FY 2018, we noted that controls and processes were effective over IR roles and responsibilities and the collaboration with external stakeholders to ensure on-site technical assistance/surge capabilities for quick response to incidents. NIST SP 800-53, Rev. 4 requires that organizations develop incident response policies and procedures that are reviewed and approved. EXIM's Incident Handling Policies and Procedures did not fully (b) (7)(E)

(b) (7)(E) , as outlined in NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*.

In addition, during FY 2018, EXIM management was still (b) (7)(E)

As this implementation was still in progress during FY 2018 and was not in place for the entirety of the fiscal year, a deficiency was noted.

Due to competing priorities, including the remediation of prior-year deficiencies, updating of legacy controls, and transitioning of essential staff, management (b) (7)(E)

However, KPMG noted that the new Chief Information Security Officer (CISO) and Information System Security Manager (ISSM) are in the process of developing or updating policies and procedures to be (b) (7)(E)

Without fully documented (b) (7)(E)

The following guidance is relevant to this deficiency:

- NIST SP 800-53, Rev. 4, states:

  IR-4: Incident Handling:
  The organization:
  a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

- NIST SP 800-61, Rev. 2, states:

  Establishing an incident response capability should include the following actions: Creating an incident response policy and plan; Developing procedures for performing incident handling and reporting; setting guidelines for communicating with outside parties regarding incidents; selecting a team structure and staffing

model; establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies); determining what services the incident response team should provide; staffing and training the incident response team.

We recommend that EXIM management:

8. Implement (b) (7)(E) NIST SP 800-53, Rev. 4, security control requirement IR-4 and NIST 800-61, Rev. 2, guidance and include detailed steps for responding to an incident. (b) (7)(E)

9. (b) (7)(E) , especially to include aspects documented within the lessons learned from training and testing.

Management's Response:

Management concurred with the recommendation. The EXIM Security Incident Handling Policy was updated with all recommendations included and staff were trained this fiscal year after the assessment period had ended.

Evaluation of Management's Response: Management's response meets the intent of our recommendation.

Finding 4: Contingency planning program needs improvement. (Recover Function – CP)

During FY 2018, (b) (7)(E) . However, EXIM's contingency planning program did not fully adhere to requirements and guidance from FIPS 200, NIST SP 800-53, Rev. 4, and NIST SP 800-34. Specifically, we identified the following:

- EXIM did not document an organizational and/or system level Information System Contingency Plan (ISCP).

- EXIM did not document (b) (7)(E) .

- EXIM was not able to provide evidence of the functional training, testing, and exercises (TT&Es) for (b) (7)(E) , which are required of moderate-level systems.

- The (b) (7)(E) did not include a (b) (7)(E)

Due to competing priorities and transitioning staff, management was not able to adequately define and implement policies and procedures related to contingency planning across the organization.

Without establishing an effective contingency planning process, EXIM may not be able to determine the true impact to the business or fully recover its operations in the event of a disaster or emergency. (b) (7)(E)

The following guidance is relevant to this deficiency:

- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, states:

  > Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

- NIST SP 800-53, Rev. 4, includes the following security control requirement:

  > CP-2 Contingency Plan:
  > The organization:
  > a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
  > b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
  > c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
g. Protects the contingency plan from unauthorized disclosure and modification.

- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, refer to NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* [refer to Section 5, pages 27 – 34], which identifies the following types of exercises widely used in information system TT&E programs by single organizations. NIST states:

> Functional Exercises. Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.
>
> TT&E activities appropriate to their respective impact level: For moderate-impact systems, a functional exercise at an organization-defined frequency should be conducted. The functional exercise should include all ISCP points of contact and be facilitated by the system owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from backup media.

NIST SP 800-34 further states:

> In order to develop and maintain an effective information system contingency plan, there must be 7 steps, present in the process:
>
> - Develop the contingency planning policy;
> - Conduct the business impact analysis;
> - Identify preventive controls;
> - Create contingency strategies;
> - Develop an information system contingency plan;
> - Ensure plan testing, training, and exercises; and
> - Ensure plan maintenance

These steps represent key elements in a comprehensive information system contingency planning capability.

We recommend that EXIM management:

10. Fully document, finalize, and approve (b) (7)(E) to address business and mission requirements.

11. Fully document policies, procedures, and/or strategies for (b) (7)(E) that adheres to NIST SP 800-53 security control requirement CP-2 and NIST SP 800-34 guidance.

12. Complete the (b) (7)(E) for the Bank and its systems, including (b) (7)(E) , and incorporate the (b) (7)(E) results into the analysis and strategy development efforts for the Bank and in-scope systems continuity plans.

13. Fully document and perform (b) (7)(E) for its systems, including (b) (7)(E) , on an annual basis and retain the test results.

14. Develop and include a business continuity plan within (b) (7)(E) .

Management's Response:

Management concurs and has taken the initiative to correct the findings. The ISCP documentation is in the process of being updated, finalized, and approved. The Director, Security Services, (b) (7)(E)

EXIM conducted functional training, testing, and exercises (TT&E) in FY18 after the assessment period, the results were documented, (b) (7)(E)

Evaluation of Management's Response: If implemented properly, we believe that process management as defined above for remediating this issue will assist in strengthening the Bank's CP program.

CONCLUSION

We determined that EXIM remediated many of the deficiencies reported in prior FISMA performance audits and effectively designed and implemented 12 of the 13 NIST SP 800-53, Rev. 4, controls that we tested for (b) (7)(E) However, the Bank's information security program and practices are not effective overall, as a result of a majority of FY 2018 IG FISMA Reporting Metrics for the five Cybersecurity Functions and eight FISMA Metric Domains did not score Level 4: Managed and Measurable, as prescribed by DHS criteria.

Furthermore, we found deficiencies with EXIM's RM policies and procedures, ISCM program, incident handling policies and procedures, and CP program. EXIM should develop and implement controls and practices that are Level 4: Management and Measurable for the five Cybersecurity Functions and eight FISMA Metric Domains to consistently evaluate and improve the effectiveness of its information security program. Additionally, EXIM should implement corrective actions to strength its RM policies and procedures, ISCM program, incident handling policies and procedures, and CP program to address fully NIST SP 800-53 security control requirements and applicable NIST SPs 800-34, 800-61, and 800-137 guidance. By not having a mature and effective information security program, EXIM management is at an increased risk of operating without a full understanding of its risk posture, including potential vulnerabilities to which its information system may be susceptible.

APPENDICES

Appendix A: Scope and Methodology

To evaluate the effectiveness of the Export Import Bank of the United States' (EXIM or the Bank) information security program and its compliance with Federal Information Security Modernization Act of 2014 (FISMA), we conducted a performance audit that was focused on the information security controls, program, and practices at the Bank level (entity level) and for a selection of information systems.

We conducted the performance audit in accordance with generally accepted government auditing standards (GAGAS).[10] 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.

To assess EXIM's information security controls and practices at the system level, we made a selection of one EXIM-hosted system, (b) (7)(E) , one contractor-hosted information system, (b) (7)(E) , and one additional system to test specific National Institute of Standards and Technology (NIST) security controls, (b) (7)(E) . See **Appendix G**, *System Selection Approach*.

To assess EXIM's maturity levels for *FY 2018 Inspector General Information Security Modernization Act of 2014 Reporting Metrics* (FY 2018 IG FISMA Reporting Metrics), Version 1.0.1, May 24, 2014, we performed test procedures at the Bank level (entity level) and for the selection of information systems. Our methodology for determining the maturity levels for each of the five Cybersecurity Functions and eight FISMA Metric Domains from the FY 2018 IG FISMA Reporting Metrics was:

1. We requested that EXIM management communicate its self-assessed maturity levels, where applicable, to confirm our understanding of the FISMA-related policies and procedures, guidance, structures, and processes established by the Bank. This helped us to understand specific artifacts to evaluate as part of the FISMA audit.

2. We performed test procedures for maturity level 3 (Consistently Implemented) at the Bank and (b) (7)(E) (where applicable) for the maturity level 3 questions within the eight FISMA Metric Domains. The test procedures evaluated the design and operating effectiveness of the security controls from NIST Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* referenced in the metric questions. If we determined that maturity level 3 controls were ineffective, we assessed, based on test results and evidence obtained, the maturity at level 1 (Ad Hoc) or 2 (Defined) for the questions that failed testing.

[10] *Supra* note 2.

3. For maturity level 3 controls determined to be effective, we performed level 4 (Managed and Measurable) test procedures for the Bank and (b) (7)(E) (where applicable) for the maturity level 4 questions within the eight FISMA Metric Domains. The test procedures evaluated the design and operating effectiveness of the controls.

4. For maturity level 4 controls determined to be effective, we performed level 5 (Optimized) test procedures for the Bank and (b) (7)(E) (where applicable) for the maturity level 5 questions within the eight FISMA Metric Domains. The test procedures evaluated the design of the controls. For the FY 2018 FISMA performance audit, we did not assess any controls at the Level 5, Optimized. Thus, no testing was necessary to evaluate the Bank's controls at that level.

As prescribed in the FY 2018 IG FISMA Reporting Metrics, a FISMA Metric Domain is considered effective if it is at Level 4: Managed and Measurable or at Level 5: Optimized. See **Appendix F**, *DHS FY 2018 IG FISMA Metric Results.*

In addition to the procedures above, we selected 13 additional NIST SP 800-53, Rev. 4, security controls that were not referenced in the FY 2018 IG FISMA Reporting Metrics and developed and executed test procedures for these control for (b) (7)(E).[11] See **Appendix E**, *Security Controls Selection*.

To assess the effectiveness of the information security program and practices of EXIM, our scope included the following:

- Inquiries of information system owners, information system security managers, system administrators, and other relevant individuals to walk through each control process.

- An inspection of the information security practices and policies established by the Office of Management and Technology.

- An inspection of the information security practices, policies, and procedures in use across EXIM.

- An inspection of IT artifacts to determine the implementation and operating effectiveness of security controls.

We performed our fieldwork at EXIM's headquarters office in Washington, D.C., during the period of May 20, 2018, through January 9, 2019. During the course of our audit, we met

[11] In addition to evaluating EXIM's maturity levels for the FY 2018 IG FISMA Reporting Metrics, Contract No. GS-00F-275CA, Task Order 83310118F0016, dated March 22, 2018, required us to test 25-35 additional NIST 800-53 controls for a selected information system.

with EXIM management to provide a status of the engagement and discuss our preliminary conclusions.

See **Appendix B** for details on the federal laws, regulations, and guidance used as criteria for the performance audit and **Appendix C** for a status of prior-year recommendations.

Appendix B: Federal Laws, Regulations, and Guidance

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

- Federal Information Security Modernization Act of 2014 (Public Law 113-283, §2, 128 Stat. 3073, 3075-3078 [2014])
- Office of Management and Budget (OMB) Memo 17-05 –Fiscal Year 2016-2017 Guidance on Federal Information Security Privacy Management Requirements (or newer version)
- FY 2018 IG Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 1.0.1, dated May 24, 2018
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, Rev. 1, *Guide for Assessing Security Controls for Federal Information Systems and Organizations*
- NIST SP 800-30, *Managing Information Security Risk*
- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*
- NIST SP800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
- NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*
- NIST SP 800-137, Rev. 1, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
- Federal Information Processing Standards (FIPS) 199: *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*.

Appendix C: Status of Prior-Year Recommendations

As part of this year's Federal Information Security Modernization Act of 2014 (FISMA) performance audit, we followed up on the status of open prior-year findings reported by the predecessor auditor. We inquired of Export-Import Bank of the United States (EXIM) personnel and inspected evidence related to current-year test work to determine the status of the findings. If recommendations were implemented, we closed the findings. If recommendations were partially implemented, not implemented at all, or we identified findings during our testing, we closed the predecessor auditor's recommendation and re-issued a similar recommendation in FY 2018.

Table 3. Prior Year Findings – 2017 Evaluation

Finding	Recommendation	FY Identified	FY 2018 Status
EXIM Bank should improve the maturity of its information security program.	In FY 2016, we recommended that the EXIM Bank CIO: a. Perform an assessment of EXIM Bank's current information security program to identify the cost-effective security measures required to achieve a fully mature program. b. Implement appropriate processes and procedures to improve the information security program and align it with Level 4: Managed and Measurable IG metrics. As we noted further issues during the FY 2017 audit, the recommendations will remain open, and we are therefore not issuing any new recommendations related to this finding.	2016	Closed – Issued Recommendations Specific to the Deficiencies found - See the **Audit Results** section.
EXIM Bank should improve controls over its vulnerability management program	In FY 2016, we recommended that the EXIM Bank CIO:	2016	Closed

Finding	Recommendation	FY Identified	FY 2018 Status
	a. Continue with their efforts to decommission all unsupported software to reduce their exposure to vulnerabilities that cannot be remediated. b. Implement available (b) (7)(E) that exist across all operating platforms in the Bank's network environment. During the FY 2017 audit, we noted that the Bank adequately addressed recommendation A. However, we noted further issues related to recommendation B. As a result, recommendation B will remain open, and we are therefore not issuing any new recommendations related to this finding.		
EXIM Bank Should Improve Controls over Baseline Configuration Implementation	In FY 2016, we recommended that the EXIM Bank CIO: a. Document and implement baseline configuration settings for all information technology products deployed within the Bank. b. Document justifications or compensating controls for any deviations from established baseline configuration settings for each of the information technology products deployed within the Bank. As we noted further issues during the FY 2017 audit, the recommendations will remain open, and we are therefore not issuing any new recommendations related to this finding.	2016	Closed

Finding	Recommendation	FY Identified	FY 2018 Status
EXIM Bank Should Improve Controls over Information Assurance Monitoring	We recommend that the EXIM Bank CIO develop and implement a monitoring and auditing process that identifies and remediates gaps in the Bank's information assurance control implementation and that validates compliance with the Bank's privacy and awareness training program.	2017	Closed
EXIM Bank Should Improve Controls over Firewall Capabilities Implementation	As this weakness was remediated during the audit, we are not issuing a recommendation.	2017	Closed

Appendix D: Management's Response

EXIM
EXPORT-IMPORT BANK OF THE UNITED STATES

Reducing Risk. Unleashing Opportunity.

February 27, 2019

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

Dear Ms. Salehi,

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 2018" dated February 13, 2019 (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 KPMG, LLP ("KPMG") to conduct a performance audit of the Bank's information security program and practices. The Bank appreciates KPMG recognizing that "consistent with applicable FISMA requirements, OMB's policy and guidance, the NIST standards and guidelines, and FIPS, EXIM's information security program and practices for its unclassified systems were established and have been maintained for the five Cybersecurity Functions and eight FISMA Metric Domains" and that "during the past year, EXIM implemented corrective actions to remediate prior-year deficiencies over vulnerability management, baseline configurations, information assurance monitoring, and firewall capabilities." The Bank also appreciates the assurance that while the overall score for its information security program was at a Level 3 based on the DHS FY 2018 IG FISMA Reporting Metrics, the Bank has effectively designed and implemented 12 of the 13 NIST Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations controls.

The OIG, through KPMG, has identified four findings that resulted in fourteen new recommendations to improve the Bank's information security program and practices, and its policies and procedures. The Bank concurs with all fourteen recommendations and will move forward with implementing the recommendations.

Recommendation 1: Formally document (b) (7)(E) that address the NIST SP 800-53, Revision 4, RA-1, CM-1, CM-8, CA-7, and SA-5 security controls.

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

1

EXIM EXPORT-IMPORT BANK OF THE UNITED STATES

Reducing Risk. Unleashing Opportunity.

Recommendation 2: Document the current (b) (7)(E) including (b) (7)(E)

Management Response: The Bank concurs with this recommendation.

During FY 2018, the Bank fully established and implemented a hardware and software asset management process to maintain a complete hardware and software asset inventory for the Bank. The (b) (7)(E)

Recommendation 3: Address mission and business process considerations for information security in the (b) (7)(E)

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

Recommendation 4: Update the ISCM policies, procedures, and strategy to include the following: (b) (7)(E)

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

Recommendation 5: Update the ISCM procedures, and strategy to include and (b) (7)(E) (b) (7)(E)

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

Recommendation 6: Establish (b) (7)(E) to measure the effectiveness of the ISCM program.

Management Response: The Bank concurs with this recommendation.

2

EXIM EXPORT-IMPORT BANK OF THE UNITED STATES

Reducing Risk. Unleashing Opportunity.

The Bank has established qualitative and quantitative performance metrics to measure the effectiveness of the ISCM program.

Recommendation 7: Complete the (b) (7)(E) to (b) (7)(E) (b) (7)(E) compliance.

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

Recommendation 8: Implement (b) (7)(E) NIST SP 800-53, Rev. 4, security control requirement IR-4 and NIST 800-61, Rev. 2, guidance and include detailed steps for responding to an incident. (b) (7)(E) (b) (7)(E)

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

Recommendation 9: (b) (7)(E) (b) (7)(E) especially to include aspects documented within the lessons learned from training and testing.

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

Recommendation 10: Fully document, finalize, and approve (b) (7)(E) to address business and mission requirements.

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

3

EXIM EXPORT-IMPORT BANK OF THE UNITED STATES

Reducing Risk. Unleashing Opportunity.

Recommendation 11: Fully document policies, procedures, and/or strategies for (b) (7)(E) (b) (7)(E) that adheres to NIST SP 800-53 security control requirement CP-2 and NIST SP 800-34 guidance.

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

Recommendation 12: Complete the (b) (7)(E) for the Bank and its systems, including (b) (7)(E) (b) (7)(E) and incorporate the (b) (7)(E) results into the analysis and strategy development efforts for the Bank and in-scope systems continuity plans.

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

Recommendation 13: Fully document and perform functional TT&Es for its systems, including (b) (7)(E) (b) (7)(E) on an annual basis and retain the test results.

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

Recommendation 14: Develop and include a business continuity plan within (b) (7)(E)

Management Response: The Bank concurs with this recommendation.

(b) (7)(E)

4

EXIM
EXPORT-IMPORT BANK
OF THE UNITED STATES

Reducing Risk. Unleashing Opportunity.

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

Sincerely,

JEFFREY GOETTMAN Digitally signed by JEFFREY GOETTMAN Date: 2019.02.27 16:37:41 -05'00'

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

5

Appendix E: Security Controls Selection

During planning, we identified the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, controls referenced in the F*Y 2018 Inspector General (IG) Federal Information Security Modernization Act 2014 (FISMA) Reporting Metrics* (FY 2018 IG FISMA Reporting Metrics), and we judgmentally selected additional NIST SP 800-53 controls to obtain a total population of 25-35 controls.[12] To do so, we performed an analysis and determined that the FY 2018 DHS IG FISMA Reporting Metric had 22 unique NIST 800-53 security controls that were to be tested at the system level. Therefore, we judgmentally identified the following 13 additional NIST SP 800-53 controls to test for the Automated Processing System (APS).

Table 4. Selected Security Controls and Testing Results

No.	NIST SP 800-53 Security Control	Control Name	System	Results
1	SA-10	Developer Configuration Management	(b) (7)(E)	No exceptions noted
2	SC-4	Information in Shared Resources	(b) (7)(E)	No exceptions noted
3	RA-5	Vulnerability Scanning	(b) (7)(E)	No exceptions noted
4	CM-4	Security Impact Analysis	(b) (7)(E)	No exceptions noted
5	IA-8	Identification and Authorization	(b) (7)(E)	No exceptions noted
6	CM-5	Access Restrictions for Change	(b) (7)(E)	No exceptions noted
7	AC-5	Separation of Duties	(b) (7)(E)	No exceptions noted
8	SA-11	Developer Security Testing and Evaluation	(b) (7)(E)	No exceptions noted
9	SA-12	Supply Chain Protections	(b) (7)(E)	No exceptions noted
10	PM-4	Plans of Actions and Milestones Process	(b) (7)(E)	No exceptions noted
11	SA-5	External Information Systems Services	(b) (7)(E)	Exception Noted. See Finding 1 in the **Findings** section.
12	CP-10	Information System Recovery and Reconstitution	(b) (7)(E)	No exceptions noted
13	SC-24	Fail In Known State	(b) (7)(E)	No exceptions noted

[12] *Supra* note 11.

Appendix F: DHS FY 2018 IG FISMA Metric Results

On October 31, 2018, we provided the Export-Import Bank of the United States (EXIM or the Bank) Office of Inspector General (OIG) with the assessed maturity levels for each of the 67 questions outlined in the *FY 2018 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY IG 2018 FISMA Reporting Metrics). The following tables represent each of the NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond, and Recover) that we assessed to respond to the FY 2018 IG FISMA Reporting Metrics. Each of the five functions had specific evaluation questions that we assessed, for 67 questions, and each question was associated with a maturity level. The tables below represent the number of objectives that we evaluated for each Cybersecurity Framework function and the maturity model rating that each respective FISMA Metric domain question "met." Per DHS' FY 2018 IG FISMA Reporting Metrics guidance, a security program is considered effective if the majority of the FY 2018 IG FISMA Reporting Metrics are at Level 4: Management and Measurable.

Furthermore, ratings throughout the eight FISMA Metric Domains are determined by a simple majority, in which the most frequent level across the questions serve as the domain rating.

For each of the FY 2018 IG FISMA Reporting Metrics, EXIM management generally assessed the maturity level of its information security program as a Level 3: Consistently Implemented using DHS' scoring methodology (a five-level maturity model scale). When we assessed EXIM's information security program for each of the FY 2018 IG FISMA Reporting Metrics, we found that the Identify, Protect,[13] and Detect Cybersecurity Functions scored at Level 3: Consistently Implemented, and Respond and Recover scored at Level 2: Defined. Therefore, EXIM's information security program is considered not effective, as stipulated by DHS' scoring methodology (i.e., EXIM did not score Level 4: Managed and Measurable for a majority of the FY 2018 IG FISMA Reporting Metrics). To achieve an effective information security program as stipulated by DHS guidance, EXIM should develop and implement practices that address Level 4: Managed and Measurable metrics. Specifically, to evaluate and improve the effectiveness of its information security program, EXIM should address the following:

- Areas for improvement in the Identify Domain – Risk Management (RM):
    - Because the Bank did not have (b) (7)(E) fully in place during the FISMA performance audit period (see Finding 2 in the **Findings** section above), we noted that Bank management did not consistently subject the information systems included in its inventory to its monitoring processes.

[13] *Supra* note 8.

- During FY 2018, the Bank's Enterprise Risk Committee had not approved EXIM's (b) (7)(E) (see Finding 1 in the **Findings** section above); therefore, formal operation of these procedures were not in place.

- EXIM management did not consistently ensure that (b) (7)(E) tracking and reporting (see Finding 1 in the **Findings** section above).

- EXIM management did not fully define its mission and business processes with consideration of information security (b) (7)(E) (Level 4: Managed and Measurable metric not met).

- EXIM's risk management policies and procedures did not fully address all of the NIST SP 800-53, Rev. 4, control requirements (see Finding 1 in the **Findings** section above).

- EXIM management did not integrate the Bank's information security architecture with its (b) (7)(E) and define and implement security methods, mechanisms, and capabilities for both the (b) (7)(E) (Level 4: Managed and Measurable metric not met).

- EXIM management did not (1) consistently monitor and analyze a defined qualitative and quantitative performance measures on the effectiveness of the Bank's (b) (7)(E) activities, and (2) collect, analyze, and report information of the effectiveness of its (b) (7)(E) activities to make appropriate adjustments, as needed, to ensure the Bank's risk posture is maintained (Level 4: Managed and Measurable metrics not met).

- The Bank management did not consistently monitor the effectiveness of risk responses (b) (7)(E) (Level 4: Managed and Measurable metric not met).

- EXIM's daily dashboard of critical applications and services did not include the (b) (7)(E) In addition, management did always not use qualitative and quantitative performance metrics (e.g., those defined within service level agreements (SLAs)) to measure, report on, and (b) (7)(E) (Level 4: Managed and Measurable metrics not met).

- Areas for improvement in the Protect Domain – Configuration Management (CM)

  - The Bank did not implement (b) (7)(E) (see Finding 2 in the **Findings** section above).

- EXIM management did not monitor, analyze, and report on qualitative and quantitative performance measures to gauge the effectiveness of the (b) (7)(E) (Level 4: Managed and Measurable metrics not met).

- EXIM accepted the risk associated with not (b) (7)(E)

  however, management did not document and test compensating controls to minimize this risk (Level 4: Managed and Measurable metric not met).

- Areas for improvement in the Protect Domain – Identity and Access Management (IA):

  - EXIM management did not always employ automated mechanisms to (b) (7)(E)

    (Level 4: Managed and Measurable metrics not met).

  - EXIM management did not consistently provision and manage (b) (7)(E) in accordance with the principles of (b) (7)(E) . As part of testing of the general information technology controls for the FY 2018 EXIM financial statements audit, it was noted that (b) (7)(E) on the servers and databases and that all share (b) (7)(E) Furthermore, for (b) (7)(E) tested, developers had access to production servers and were (b) (7)(E) (refer to the FY 2018 Financial Statements Audit Management Letter).

- Areas for improvement in the Protect Domain – Data Protection and Privacy (DP):

  - EXIM management did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of (b) (7)(E)

    (Level 4: Managed and Measurable metrics not met).

  - EXIM management accepted the risk that its policies and procedures did not fully address (i) use of (b) (7)(E)

    However, management did not implement and test compensating controls to minimize risks (Level 4: Managed and Measurable metric not met).

- Areas for improvement in the Protect Domain – Security Training (ST):

- EXIM management did not always address the Bank's identified knowledge, skills, and abilities gaps through training or hiring of additional resources/contractors (Level 4: Managed and Measurable metric not met).

- EXIM management did not fully measure the effectiveness of its awareness training program by, for example, (b) (7)(E) and following up with additional awareness or training, and/or disciplinary action, as appropriate (Level 4: Managed and Measurable metric not met).

- Areas for improvement in the Detect Domain – Information Security Continuous Monitoring (ISCM):

  - The FY 2018 ISCM strategy that had been recently developed was not in place for the majority of the fiscal year (nine of 12 months) and (b) (7)(E) within the Bank (see Finding 2 in the **Findings** section above).

  - The Bank management did not fully implement a security incident and event management (SIEM) software product. Currently, the Bank uses the Kiwi system log; however, (b) (7)(E) (see Finding 2 in the **Findings** section above).

  - EXIM management did not always monitor and analyze (b) (7)(E) on the effectiveness of the Bank's (b) (7)(E) and procedures and overall program and make updates as appropriate (see Finding 4 in the **Findings** section above).

  - EXIM management did not always utilize the results of (b) (7)(E) to maintain (b) (7)(E) of its information systems (Level 4: Managed and Measurable metric not met).

  - EXIM management did not integrate metrics on the effectiveness of the (b) (7)(E) program to deliver persistent situational awareness across the organization, explain the environment for both a threat/vulnerability and risk/impact perspective, and cover business areas of operation and security (Level 4: Managed and Measurable metric not met).

- Areas for improvement in the Respond Domain – Incident Response (IR):

  - During the 2018 FISMA performance audit period, EXIM management did not approve incident handling policies and procedures and fully (b) (7)(E)

    (see Finding 3 in the **Findings** section above).

- During FY 2018, EXIM management did not formally assign responsibility for monitoring and tracking the effectiveness of IR activities. Furthermore, EXIM staff did not consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of IR activities (Level 4: Managed and Measurable metrics not met). Since completion of our fieldwork, (b) (7)(E)

- Areas for improvement in the Recover Domain – Contingency Planning (CP):

  - EXIM management did not fully document its organizational and/or system level Information Security Continuous Monitoring Plans (ISCP) in a manner that adhered to NIST SP 800-53, Rev. 4, contingency plan control (CP-2) and NIST 800-34, Rev.1, *Contingency Planning Guide for Federal Information Systems* (See Finding 4 in the **Findings** section above).

  - EXIM management did not manage the (b) (7)(E) related to contingency planning activities. Management did not integrate (b) (7)(E) concerns into the Bank's contingency planning policies and procedures, define and implement a contingency plan for the (b) (7)(E) , apply appropriate (b) (7)(E) , and consider alternate telecommunication service providers for the (b) (7)(E) (Level 4: Managed and Measurable metrics not met).

  - EXIM management did not fully document (b) (7)(E) (see Finding 4 in the **Findings** section above).

  - The Security Assessment and Authorization (SA&A)[14] package for one selected system did not include the required (b) (7)(E) (see Finding 4 in the **Findings** section above).

  - The Bank management was unable to provide evidence for the functional training, testing, and exercises (TT&E) for (b) (7)(E) (see Finding 4 in the **Findings** section above).

[14] SA&A is the process by which federal organizations examine their information technology infrastructure and develop supporting evidence necessary for security assurance accreditation. SA&A packages should include system security plans, business continuity plans, security assessment reports (SARs), POA&Ms, and Authorities to Operate (ATOs).

The following tables summarizes of our assessed maturity levels for the FY 2018 IG FISMA Metric Results.

Table 5. EXIM FY 2018 IG FISMA Metric Results

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	11
Managed and Measurable	1
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	8
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	6

Managed and Measurable	3
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 2C: Protect – Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	4
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 2D: Protect – Security Training

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	4
Managed and Measurable	2
Optimized	0
Function Rating: Consistently Implemented (Level3)	

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	4
Managed and Measurable	0
Optimized	0

Function Rating: Consistently Implemented (Level 3)	

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that EXIM's information security program and practices for Risk Management did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 2A: Protect – Configuration Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that EXIM's information security program and practices for Configuration Management did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
			Implemented maturity level.
Function 2B: Protect – Identity and Access Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that EXIM's information security program and practices for Identity and Access Management did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 2C: Protect – Data Protection and Privacy	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that EXIM's information security program and practices for Data Protection and Privacy did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 2D: Protect – Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that EXIM's information security program and practices for Security Training did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that EXIM's information security program and practices for ISCM did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 4: Respond - Incident Response	Defined (Level 2)	Defined (Level 2)	We determined that EXIM's information security program and practices for Incident Response did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Defined maturity level.
Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	We determined that EXIM's information security program and practices for Contingency Planning did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Defined maturity level.
Overall	Not Effective	Not Effective	Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, EXIM has established and maintained its information security program and practices for the five Cybersecurity Functions and eight FISMA program areas. However, the program was not fully effective as reflected deficiencies that we identified in risk management, information continuous monitoring, incident response, and contingency planning. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). The FY 2018 IG FISMA Reporting

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
			Metrics define an effective information security program as Managed and Measurable (Level 4).

Appendix G: System Selection Approach

We obtained a listing of all systems from the Export-Import Bank of the United States (EXIM or the Bank) Federal Information Security Modernization Act of 2014 (FISMA) system inventory. We sorted the FISMA inventory to identify systems managed and hosted by EXIM and removed Infrastructure General Support System (GSS) as it was selected for testing additional National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* security controls in the 2017 FISMA performance audit. We randomly selected EXIM Online (EOL) to use for system-level testing for the *FY 2018 Inspector General Federal Information Modernization Act of 2014 Reporting Metrics* (FY 2018 IG FISMA Reporting Metrics). We then judgmentally selected the Application Processing System (APS) as it has not been assessed in many years, and it manages the application and underwriting of long-term guarantees and direct loans, which is essential to the EXIM. For APS, we tested the 13 additional NIST 800-53 controls detailed in **Appendix E**, *Security Controls Selection.*

We then sorted the FISMA inventory to identify contractor systems hosted on the cloud or by third parties that had a Federal Information Processing Standards (FIPS) 199 Moderate impact and contained Personally Identifiable Information (PII). We judgmentally selected (b) (7)(E) to be used for performing system-level test work over FY 2018 IG FISMA Metric Metrics related to contractor systems and cloud service providers.

In summary, we selected the following systems as the representative subset of systems to test for the FY 2018 EXIM FISMA performance audit:

- (b) (7)(E) in support of the FY 2018 IG FISMA Reporting Metrics.
- (b) (7)(E) was tested for 13 additional selected NIST SP 800-53 controls.
- (b) (7)(E) in support of the FY 2018 IG FISMA Reporting Metrics.

Appendix H: Distribution List

Jeffrey Gerrish, Acting President and Chairman
Jeffrey Goettman, Executive Vice President and Chief Operating Officer
Doug Adler, Acting Senior Vice President and General Counsel
Margaux Matter, Senior Vice President and Chief of Staff
David Sena, Senior Vice President of Board Authorized Finance
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Nicole Valtos, Vice President and Deputy Chief Operating Officer
Inci Tonguch-Murray, Acting Senior Vice President and Chief Financial Officer
Stacy Dawn, Chief Information Security Officer and Chief Privacy Officer
Cristopolis Dieguez, Director, Internal Controls and Compliance
James DeVaul, Partner, KPMG LLP
Parisa Salehi, Acting Inspector General, OIG
Elizabeth Sweetland, Detailed Counsel, OIG
Erica Wardley, Deputy Assistant Inspector General for Audits and Evaluations, OIG

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