



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

**Independent Audit of
EXIM's Information
Security Program
Effectiveness for Fiscal
Year 2019**

January 13, 2020

OIG-AR-20-04

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

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

The Office of Inspector General (OIG), an independent office within EXIM, was statutorily created in 2002 and organized in 2007. The mission of EXIM OIG 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.



Office of Inspector General

To: Howard Spira
Senior Vice President and Chief Information Officer

From: Jennifer Fain
Acting Inspector General 

Subject: Independent Audit of EXIM's Information Security Program Effectiveness for Fiscal Year 2019

Date: January 13, 2020

This memorandum transmits the audit report on the effectiveness of the Export-Import Bank of the United States' (EXIM or the Bank) information security program for fiscal year (FY) 2019. Under a contract monitored by this office, we engaged the independent public accounting firm of KPMG LLP (KPMG) to perform the audit. The objective was to determine whether EXIM developed and implemented an effective information security program and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA).

KPMG determined that EXIM's information security program and practices were effective overall as a result of a majority of the FY 2019 Inspector General FISMA Reporting Functions scored a Level 4: Managed and Measurable (Identify, Protect, Detect, and Respond) as described by the DHS criteria. However, deficiencies were found within four Cybersecurity Functions (Identify, Protect, Detect, and Recover) and four FISMA Metric Domains (Risk Management, Data Protection and Privacy, Information Security and Continuous Monitoring, and Contingency Planning) that need improvement, but were not pervasive to affect the overall effectiveness and assessment of the program. The report contains seven new recommendations. Management concurred with the recommendations and we consider management's proposed actions to be responsive. The recommendations will be closed upon completion and verification of the proposed actions.

We appreciate the cooperation and courtesies provided to KPMG and this office during the audit. If you have questions, please contact me, Jennifer Fain at (202) 565-3439 or jennifer.fain@exim.gov or Courtney Potter at (202) 565-3976 or courtney.potter@exim.gov. You can obtain additional information about EXIM OIG and the Inspector General Act of 1978 at www.exim.gov/about/oig.



KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

January 10, 2020

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

Re: Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices Report – Fiscal Year 2019

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 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.3, dated April 9, 2019 (FY 2019 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 requirements¹ 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.

¹ Contract No. GS-00F-275CA, Task Order 83310118F0016, dated March 22, 2019

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.



Jennifer Fain
Acting Inspector General
Export Import Bank of the United States
January 10, 2020
Page 2 of 3

The objective for this independent audit was to determine whether EXIM developed and implemented an effective information security program and practices as required by FISMA. To determine whether EXIM developed and implemented an effective information security program and practices for the period of October 1, 2018 to September 30, 2019, 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 Standards and Technology (NIST).

We based our work on a selection of EXIM-wide security controls and a selection of system-specific security controls across one EXIM information system and one EXIM contractor information system. As part of our audit, we responded to the DHS FY 2019 IG FISMA Reporting Metrics and assessed the maturity levels on behalf of the 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 Functions³ and eight FISMA Metric Domains.⁴ During the past year, EXIM implemented corrective actions to remediate prior-year deficiencies over risk management policies and procedures, information security continuous monitoring program policies and strategies, incident handling policies and procedures, and many improvements to the contingency planning program. When we assessed EXIM's information security program against the DHS FY 2019 IG FISMA Reporting Metrics, we found that the Cybersecurity Functions' Identify, Protect, Detect, and Respond scored at Level 4: Managed and Measureable; and Recover scored at Level 3: Consistently Implemented.

Since the majority of EXIM's Cybersecurity Functions scored at a Level 4: Managed and Measureable, the information security program was considered effective according to the

³ OMB, DHS, and CIGIE developed the FY 2019 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. In FY 2019, 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 2019 IG FISMA Reporting Metrics, Version 1.3, April 9, 2019, 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.



Jennifer Fain
Acting Inspector General
Export Import Bank of the United States
January 10, 2020
Page 3 of 3

instructions detailed within the DHS FY 2019 IG FISMA Reporting Metrics. However, we did identify deficiencies within the Cybersecurity Functions for FISMA program areas. Specifically, we noted the following:

Cybersecurity Function: Identify

1. Policies and procedures to define, analyze, and implement risk management requirements set by the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act) need improvement (Risk Management)

Cybersecurity Function: Detect

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

Cybersecurity Function: Protect

3. Safeguards around data protection and privacy need improvement. (Data Protection and Privacy)

Cybersecurity Function: Recover

4. Contingency planning program needs improvement. (Contingency Planning)

We considered these deficiencies when we assessed the maturity levels for the FY 2019 IG FISMA Reporting Metrics. We provided 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.

Very truly yours,

KPMG LLP

January 10, 2020

EXECUTIVE SUMMARY

Independent Audit of EXIM's Information Security
Program Effectiveness for FY 2019
OIG-AR-20-04, January 13, 2020

Why We Did This Audit

The Federal Information Security Modernization Act of 2014 (FISMA of the Act) requires agencies 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. The Act provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over information technology that support operations and assets. It 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 the U.S. Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), which is accomplished through DHS' CyberScope tool. In addition, FISMA requires Offices of Inspectors General to provide an independent assessment of the effectiveness of an agency's information security program.

To fulfill its FISMA responsibilities the Office of Inspector General (OIG) contracted with KPMG LLP for an annual independent audit of the effectiveness of the Export-Import Bank of the United States' (EXIM or the Bank) information security program. The objective of this performance audit was to determine whether EXIM developed and implemented an effective information security program and practices as required by FISMA. In addition, we followed up on the status of prior-year FISMA findings.

What We Recommend

We made seven recommendations to improve the effectiveness of EXIM's information security program.

What We Found

EXIM's information security program and practices were effective overall as a result of a majority of the FY 2019 Inspector General FISMA Reporting Functions scored a Level 4: Managed and Measurable (Identify, Protect, Detect, and Respond) as described by the DHS criteria. Consistent with applicable FISMA requirements, OMB's policy and guidance, the National Institute of Standards and Technology (NIST) standards and guidelines, and Federal Information Processing Standards (FIPS), EXIM's information security program and practices for its systems were established and have been maintained for the five Cybersecurity Functions and eight FISMA Metric Domains. However, we found deficiencies within four Cybersecurity Functions (Identify, Protect, Detect, and Recover) and four FISMA Metric Domains (Risk Management, Data Protection and Privacy, Information Security and Continuous Monitoring, and Contingency Planning) that need improvement, but were not pervasive to affect the overall effectiveness and assessment of the program.

Additionally, we determined that EXIM remediated many of the deficiencies reported in the FY 2018 FISMA performance audit and effectively designed and implemented the 13 NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, controls that we tested for a randomly selected system. The Bank implemented corrective actions to remediate many of the prior-year deficiencies over risk management policies and procedures, information security continuous monitoring program policies and strategies, incident handling policies and procedures, and many improvements to the contingency planning program.

However, for Cybersecurity Function Recover and FISMA Metric Domain Contingency Planning, EXIM should continue to develop and implement controls and practices that are Level 4: Management and Measurable to consistently evaluate and improve the effectiveness of its information security program. Furthermore, the Bank should implement corrective actions to strengthen its Risk Management policies and procedures, Information Security Continuous Monitoring program, Data Protection and Privacy program safeguards, and Contingency Planning program to include formal business impact analyses.

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
TABLE OF CONTENTS	ii
LIST OF TABLES.....	iii
ABBREVIATIONS AND GLOSSARY	iv
INTRODUCTION.....	6
OBJECTIVE, SCOPE, AND METHODOLOGY	6
BACKGROUND.....	6
AUDIT RESULTS	10
FINDINGS.....	10
Finding 1: Policies and procedures to define, analyze, and implement risk management requirements set by the SECURE Technology Act need improvement.....	10
Finding 2: Information Security Continuous Monitoring (ISCM) program was not fully established.....	11
Finding 3: Safeguards around Data Protection and Privacy need improvement. (Protect Function – DP).....	13
Finding 4: Contingency planning program needs improvement.....	15
CONCLUSION.....	18
APPENDIXES	19
Appendix A: Scope and Methodology	19
Appendix B: Federal Laws, Regulations, and Guidance.....	22
Appendix C: Status of Prior Year Recommendations	23
Appendix D: Management’s Response.....	27
Appendix E: Security Controls Section.....	31
Appendix F: DHS FY 2019 IG FISMA Metric Results	32
Appendix G: System Selection Approach.....	40
Appendix H: Distribution List	41

LIST OF TABLES

Table 1: Alignment of the NIST Framework for	9
Table 2: Inspector General Assessed Maturity Levels	9
Table 3: Prior-Year Findings – 2018 Evaluation	23
Table 4: Selected Security Controls and Testing Results	31
Table 5: EXIM FY 2019 IG FISMA Metric Results.....	35

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

INTRODUCTION

This report is intended solely for the information and use of the Export-Import Bank of the United States and the Office of 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) 2019. The objective was to determine whether EXIM developed and implemented an 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 developed and implemented an effective information security program and practices as required by FISMA for the fiscal year ending September 30, 2019. 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 the Financial Management System – Next Generation (FMS-NG) and ^{(b) (4)} and performed the detailed steps prescribed in the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2019 IG FISMA Reporting Metrics), version 1.3, dated April 9, 2019, 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-financing 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) (4) GSS

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) (4) and (b) (4). 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, Revision 4.

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

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.

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 2019 IG FISMA Reporting Metrics. DHS revised the FY 2018 IG FISMA Reporting Metrics and issued the FY 2019 IG FISMA Reporting Metrics, Version 1.3 on April 9, 2019. 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 Functions⁶ outlined in the NIST Cybersecurity Framework⁷ 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. In FY 2019, CIGIE did not include additional FISMA Metric Domains but for most metrics, referenced additional criteria to the overarching questions and revised specific sub questions. See **Table 1** below for a description of the NIST Cybersecurity Framework Security Functions and the associated FY 2019 IG FISMA Metric Domains.

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: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2019 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2019 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: Ad-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 2019 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.
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 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 many of the prior-year deficiencies over risk management policies and procedures, information security continuous monitoring program policies and strategies, incident handling policies and procedures, and many improvements to the contingency planning program. We found the program was effective as a result of a majority of FY 2019 IG FISMA Reporting Metrics for the five Cybersecurity Functions scored a Level 4: Managed and Measurable, as prescribed by the DHS criteria.

However, we found deficiencies within four of the five Cybersecurity Functions and four of the eight FISMA Metric Domains that need improvement, but were not pervasive to affect the overall effectiveness and assessment of the program. The deficiencies are described in the *Findings* section below. 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.

A summary of the results for the DHS FY 2019 IG FISMA Reporting Metric assessment is in **Appendix F**.

As noted above, we evaluated the open prior-year findings from the FY 2018 FISMA performance audit and noted management took sufficient action to close most deficiency conditions identified. 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: Policies and procedures to define, analyze, and implement risk management requirements set by the SECURE Technology Act need improvement.

During FY 2019, we noted that EXIM's existing information security risk management policies and procedures did not fully define and implement action plan(s) for implementing processes to comply with the SECURE Technology Act (or the Act). Per Bank policy, EXIM purchases information technology products and (b) (4)

(b) (4) . However, EXIM management did not formally analyze the impact of (b) (4) threats to the organization from the Bank's perspective

and document the policies and procedures in place to help mitigate against the risks posed by those threats.

The Act was issued into law in FY 2019. Due to competing priorities, EXIM did not have the resources in place to define and implement processes to comply with the Act across the organization.

Without an effective program to identify and define the Act, the Bank cannot fully protect its information systems, exposing the organization to potential vulnerabilities and threats.

The following guidance is relevant to this deficiency:

Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act), *specifically 1326. Requirements for executive agencies*, states:

(a) IN GENERAL—The head of each executive agency shall be responsible for—

(1) assessing the supply chain risk posed by the acquisition and use of covered articles and avoiding, mitigating, accepting, or transferring that risk, as appropriate and consistent with the standards, guidelines, and practices identified by the Council under section 1323(a)(1); and

(2) prioritizing supply chain risk assessments conducted under paragraph (1) based on the criticality of the mission, system, component, service, or asset.

We recommend that the Office of the Chief Information Officer:

1. Formally develop an action plan and implement processes to assess the (b) (4) risks at the Bank and address procedural requirements of the SECURE Technology Act.

Management’s Response:

EXIM will formally develop an action plan and implement processes to address procedural requirements of the SECURE Technology Act.

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 program that addresses the risks and requirements of the SECURE Technology Act.

Finding 2: Information Security Continuous Monitoring (ISCM) program was not fully established.

In the FY 2018 FISMA performance audit, we noted that EXIM had not fully established its ISCM program to effectively and efficiently collect, monitor, analyze, report and resolve if

appropriate ISCM data. We reported that the Bank did not fully implement a (b) (4)

. The Bank used a (b) (4)

however, this (b) (4) did not meet the minimum requirements for a DHS Continuous Diagnostics and Mitigation (CDM) Program.

As of June 2019, to address this deficiency, the Bank installed a DHS CDM (b) (4), however; for the reporting period, the software was not (b) (4)

Additionally, for the full reporting period, the Bank had not (b) (4) .

Due to the United States government shutdown from December 22, 2018, until January 25, 2019, the Bank was not in complete operation and this had an adverse impact on the procurement time and implementation of the (b) (4) capability.

Without full implementation of a (b) (4), EXIM may not have full capabilities in place to (b) (4)

on an ongoing basis.

The following guidance is relevant to this deficiency:

- 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]:

.... 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 the Office of the Chief Information Officer:

2. Fully implement and configure its (b) (4) across all of the Bank's information systems.
3. Configure the (b) (4)
4. Perform and document evidence of a periodic review of the reported activity and perform research and resolution, as appropriate.

Management's Response:

EXIM is following a project plan with milestones that includes fully implementing (b) (4) to log activity across all of the Bank's information systems, (b) (4), and to perform and document evidence of a periodic review of the reported activity and perform research and resolution, as appropriate.

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: Safeguards around Data Protection and Privacy need improvement. (Protect Function – DP)

During FY 2019, we noted that EXIM did not have sufficient safeguards implemented to monitor and prevent unauthorized exfiltration of information from the Bank's information systems. Specifically, (b) (4)

It was noted that the Bank does receive an automated email from (b) (4)

Due to competing priorities and limited resources, EXIM was unable to implement controls to monitor and determine if there was any exfiltration of data in FY 2019 for (b) (4)

EXIM may not have full capabilities in place to limit the transfer of the Bank's personally identifiable information (PII) and other agency sensitive data. Additionally, (b) (4)

The following guidance is relevant to this deficiency:

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

Section: SC-7 (10) Boundary Protection | Prevent Unauthorized Exfiltration:

The organization prevents the unauthorized exfiltration of information across managed interfaces.

Supplemental Guidance: Safeguards implemented by organizations to prevent unauthorized exfiltration of information from information systems include, for example: (i) strict adherence to protocol formats; (ii) monitoring for beaconing from information systems; (iii) monitoring for steganography; (iv) disconnecting external network interfaces except when explicitly needed; (v) disassembling and reassembling packet headers; and (vi) employing traffic profile analysis to detect deviations from the volume/types of traffic expected within organizations or call backs to command and control centers. Devices enforcing strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to protocol formats and specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layers. This control enhancement is closely associated with cross-domain solutions and system guards enforcing information flow requirements.

SC-7 (12) Boundary Protection | Host-Based Protection:

The organization implements [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined information system components].

Supplemental Guidance: Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.

We recommend that the Office of the Chief Information Officer:

5. Implement controls to review employees periodically who have an organizational exception for (b) (4) and (b) (4)

(b) (4)

6. Fully implement an appropriately configured hardware and/or software solution, (b) (4) to limit the transfer of the Bank's PII (e.g., SSNs, credit card numbers, and Bank ABA routing and account numbers) and other Bank sensitive data (b) (4) ensuring all resolution activities taken based on the analyses are documented and retained as evidence.

Management's Response:

Management concurred with the recommendation. EXIM has implemented controls to periodically review if users are still required to have an exception to (b) (4)

*and (b) (4)
EXIM has already implemented an appropriately configured software solution to limit the transfer of the Bank's PII and other Bank sensitive data for all systems (b) (4) EXIM will be implementing (b) (4) that will monitor and track all types of sensitive data ensuring all resolution activities taken are documented and retained as evidence.*

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

Finding 4: Contingency planning program needs improvement.

During FY 2019, we noted that EXIM management did not complete a formally documented analysis to determine mission/business processes and (b) (4)

Additionally, the Bank did not (b) (4)

However, the Bank did perform informal organizational and system-level business impact analyses (BIAs) for (b) (4), and system security plans as appropriate were updated to reflect the Recovery Time Objective, the Recovery Point Objective, and the Maximum Tolerable Downtime.

Due to a misunderstanding of the requirements associated with defining and conducting periodic BIAs, the Bank performed BIAs for the relevant systems but did not formally document (b) (4) and update the respective contingency plans.

By not performing and documenting (b) (4) in a systematic manner across the organization, the (b) (4)

(b) (4)

The following guidance is relevant to this deficiency:

U.S. Department of Homeland Security Federal Emergency Management Agency, *Federal Continuity Directive 1 (FCD-1)*, states:

Organizations conduct and document a risk assessment of all MEFs [mission essential functions] by completing a Business Impact Analysis (BIA) for all threats and hazards, and all capabilities associated with the continuance of essential functions at least every two years.

NIST SP 800-53, Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations*, security control CP-2 Contingency Plan, states:

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];

NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, 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 the Office of the Chief Information Officer:

7. At a minimum (b) (4) perform BIAs and formally document the analysis performed in a manner that adheres to NIST guidance and incorporates (b) (4) and incorporate the results within the organizational and in-scope systems continuity plans.

Management’s Response:

EXIM resourced and began completion of a formally documented analysis to determine mission/business processes and (b) (4)

Bank (b) (4) Additionally, the

At a minimum (b) (4) EXIM will perform BIAs and formally document the analysis performed in a manner that adheres to NIST guidance and incorporates the (b) (4) and will incorporate the results within the organizational and all reportable system continuity plans.

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 the FY 2018 FISMA performance audit (see appendix C for details) and effectively designed and implemented the 13 NIST SP 800-53, Rev. 4 controls that we tested for the FMS-NG. The Bank's information security program and practices are effective overall despite the findings discussed within this report. The majority of the FY 2019 IG FISMA Reporting Metrics for the five Cybersecurity Functions and eight FISMA Metric Domains were scored at a Level 4: Managed and Measurable. EXIM should continue to 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. Furthermore, EXIM should implement corrective actions to strengthen its RM policies and procedures, ISCM program, data protection and privacy program safeguards, and CP program to include formal BIAs.

APPENDIXES

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).⁸ 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 selected one EXIM-hosted system, FMS-NG, one contractor-hosted information system, (b) (4), and tested FMS-NG for additional National Institute of Standards and Technology (NIST) security controls. See **Appendix G**, *System Selection Approach*.

To assess EXIM's maturity levels for *FY 2019 Inspector General Information Security Modernization Act of 2014 Reporting Metrics* (FY 2019 IG FISMA Reporting Metrics), 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 2019 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 FMS-NG and (b) (4) (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.

⁸ *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 FMS-NG and ^{(b) (4)} (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 FMS-NG and ^{(b) (4)} (where applicable) for the maturity level 5 questions within the eight FISMA Metric Domains. The test procedures evaluated the design of the controls.

As prescribed in the FY 2019 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 2019 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 2019 IG FISMA Reporting Metrics and developed and executed test procedures for these control for APS.⁹ 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 in Washington, D.C., during the period of May 20, 2019, through October 15, 2019. During the course of our audit, we met with EXIM management to provide a status of the engagement and discuss our preliminary conclusions.

⁹ In addition to evaluating EXIM's maturity levels for the FY 2019 IG FISMA Reporting Metrics, Contract No. GS-00F-275CA, Task Order 83310118F0016, effective March 22, 2019, required us to test additional NIST 800-53 controls for a selected information system.

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 19-02 – Fiscal Year 2018-2019 Guidance on Federal Information Security Privacy Management Requirements (or newer version)
- FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 1.3, dated April 9, 2019
- 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.¹⁰ 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 have noted that status within the table below.

Table 3: Prior-Year Findings – 2018 Evaluation

Finding	Recommendation	FY Identified	FY 2018 Status
Finding 1: Risk management policies and procedures need improvement. (Identify Function – RM)	We recommend that EXIM management: <ol style="list-style-type: none"> 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 (b) (7)(E) including policies, procedures, and plans and/or strategies to (b) (7)(E) 	2018	Closed – Recommendations 1 - 3

¹⁰ See the Independent Audit of the Export-Import Bank’s Information Security Program Effectiveness for Fiscal Year 2018 at [https://www.exim.gov/sites/default/files/oig/audit/Independent Audit of Export-Import Banks Information Security Program Effectiveness for Fiscal Year 2018 OIG-AR-19-03 - Redacted FINAL.pdf](https://www.exim.gov/sites/default/files/oig/audit/Independent%20Audit%20of%20Export-Import%20Banks%20Information%20Security%20Program%20Effectiveness%20for%20Fiscal%20Year%202018%20OIG-AR-19-03%20-%20Redacted%20FINAL.pdf).

Finding	Recommendation	FY Identified	FY 2018 Status
	<p>3. Address mission and business process considerations for information security in (b) (7)(E)</p>		
<p>Finding 2: Information security continuous monitoring program was not fully established. (Detect Function - ISCM)</p>	<p>We recommend that EXIM management:</p> <p>4. Update the ISCM policies, procedures, and strategy to include the following: (b) (7)(E)</p> <p>5. Update the ISCM procedures, and strategy to include and (b) (7)(E)</p> <p>6. Establish (b) (7)(E) to measure the effectiveness of the ISCM program.</p> <p>7. Complete the (b) (7)(E) in real time for (b) (7)(E) to analyze event data</p>	<p>2018</p>	<p>Closed – Recommendations 4 - 6</p> <p>Recommendation number 7 has not been fully remediated. Refer to Finding #2 in the Findings section for the FY 2019 audit results.</p>

Finding	Recommendation	FY Identified	FY 2018 Status
<p>Finding 3: Incident handling policies and procedures were not completely documented. (Respond Function - IR)</p>	<p>We recommend that EXIM management:</p> <p>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)</p> <p>9. (b) (7)(E) especially to include aspects documented within the lessons learned from training and testing.</p>	<p>2018</p>	<p>Closed - Recommendations 8 - 9</p>
<p>Finding 4: Contingency planning program needs improvement. (Recover Function - CP)</p>	<p>We recommend that EXIM management:</p> <p>10. Fully document, finalize, and approve (b) (7)(E) to address business and mission requirements.</p> <p>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.</p> <p>12. Complete the (b) (7)(E) for the Bank and its systems, including (b) (7)(E) and incorporate the (b) (7)(E) test results into the</p>	<p>2018</p>	<p>Closed - Recommendations 10, 13, and 14 Recommendations 11 and 12 were not fully remediated related to BIA's. Refer to Finding #4 in the Findings section for the FY 2019 audit results.</p>

Finding	Recommendation	FY Identified	FY 2018 Status
	<p>analysis and strategy development efforts for the Bank and in-scope systems continuity plans.</p> <p>13. Fully document and perform (b) (7)(E) for its systems, including (b) (7)(E) on an annual basis and retain the test results.</p> <p>14. Develop and include a business continuity plan within (b) (7)(E)</p>		

Appendix D: Management’s Response



Reducing Risk. Unleashing Opportunity.

January 10, 2020

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

Dear Ms. Fain,

Thank you for providing the Export-Import Bank of the United States (“EXIM” or “EXIM 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 2019” dated December 18, 2019 (the “Report”). Management continues to support the OIG’s work which complements EXIM’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 EXIM’s information security program and practices. EXIM appreciates KPMG recognizing that “consistent with applicable FISMA requirements, OMB’s policy and guidance, the National Institute of Standards and Technology (“NIST”) standards and guidelines, and Federal Information Processing Standards (“FIPS”), EXIM’s information security program and practices for its systems were established and have been maintained for the five Cybersecurity Functions and eight FISMA Metric Domains”. Further, EXIM appreciates KPMG recognizing that “during the past year, EXIM implemented corrective actions to remediate prior-year deficiencies over risk management policies and procedures, information security continuous monitoring program policies and strategies, incident handling policies and procedures, and many improvements to contingency planning program.” EXIM also appreciates that KPMG found that EXIM’s “program was effective as a result on a majority of FY 2019 IG FISMA Reporting Metrics for five Cybersecurity Functions scored a Level 4: Managed and Measurable, as prescribed by the DHS criteria”.

The OIG, through KPMG, has identified four findings that resulted in seven new recommendations to improve the effectiveness of EXIM’s information security program. EXIM concurs with all seven recommendations and is moving forward with implementing them.

1



Reducing Risk. Unleashing Opportunity.

Recommendation 1: Formally develop an action plan and implement processes to assess the (b) (4) risks at EXIM and address procedural requirements of the SECURE Technology Act.

Management Response: EXIM concurs with this recommendation.

EXIM will formally develop an action plan and implement processes to address procedural requirements of the SECURE Technology Act.

Recommendation 2: Fully implement and configure its (b) (4) to (b) (4) across all of EXIM's information systems.

Management Response: EXIM concurs with this recommendation.

EXIM will follow a project plan with milestones that includes fully implementing (b) (4) across all of the Bank's information systems. (4)

Recommendation 3: Configure the (b) (4) to (b) (4)

Management Response: EXIM concurs with this recommendation.

EXIM will follow a project plan with milestones that includes (b) (4)

Recommendation 4: Perform and document evidence of a periodic review of the reported activity and perform research and resolution, as appropriate.

Management Response: EXIM concurs with this recommendation.

EXIM will follow a project plan with milestones that includes performing and documenting evidence of a periodic review of the reported activity and performing research and resolution, as appropriate.

Recommendation 5: Implement controls to review employees periodically who have an organizational exception for (b) (4) and (b) (4) (b) (4)



Reducing Risk. Unleashing Opportunity.

Management Response: EXIM concurs with this recommendation.

EXIM will implement controls to periodically review if (b) (4)

Recommendation 6: Fully implement an appropriately configured hardware and/or software solution, (b) (4) to limit the transfer of EXIM's PII (e.g., SSNs, credit card numbers, and Bank ABA routing and account numbers) and other Bank sensitive data (b) (4) ensuring all resolution activities taken based on the analyses are documented and retained as evidence.

Management Response: EXIM concurs with this recommendation.

EXIM has already implemented an appropriately configured software solution to limit the transfer of the bank's PII and other EXIM sensitive data for all systems (b) (4) EXIM will implement (b) (4) that will monitor and track all types of sensitive data ensuring all resolution activities taken are documented and retained as evidence.

Recommendation 7: At a minimum (b) (4) perform BIAs and formally document the analysis performed in a manner that adheres to NIST guidance and incorporates (b) (4) and incorporate the results within the organizational and in-scope systems continuity plans.

Management Response: EXIM concurs with this recommendation.

At a minimum (b) (4) EXIM will perform BIAs and formally document the analysis performed in a manner that adheres to NIST guidance and incorporates the (b) (4) and incorporate the results within the organizational and in-scope systems continuity plans.

EXIM has resourced and began completion of a formally documented analysis to determine mission/business processes and (b) (4)



Reducing Risk. Unleashing Opportunity.

Additionally, EXIM began (b) (4)

We thank the OIG for your efforts to ensure EXIM'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,

A handwritten signature in black ink, appearing to read "Adam Martinez".

Adam Martinez
Chief Management Officer
Export-Import Bank of the United States

Appendix E: Security Controls Section

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 FY 2019 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.¹¹ To do so, we performed an analysis and determined that the FY 2019 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 Financial Management System – Next Generation (FMS-NG).

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	FMS-NG	No exceptions noted
2	SC-4	Information in Shared Resources	FMS-NG	No exceptions noted
3	RA-5	Vulnerability Scanning	FMS-NG	No exceptions noted
4	CM-4	Security Impact Analysis	FMS-NG	No exceptions noted
5	IA-8	Identification and Authorization	FMS-NG	No exceptions noted
6	CM-5	Access Restrictions for Change	FMS-NG	No exceptions noted
7	AC-5	Separation of Duties	FMS-NG	No exceptions noted
8	SA-11	Developer Security Testing and Evaluation	FMS-NG	No exceptions noted
9	SA-12	Supply Chain Protections	FMS-NG	No exceptions noted
10	PM-4	Plans of Actions and Milestones Process	FMS-NG	No exceptions noted
11	SA-5	External Information Systems Services	FMS-NG	No exceptions noted
12	CP-10	Information System Recovery and Reconstitution	FMS-NG	No exceptions noted
13	SC-24	Fail In Known State	FMS-NG	No exceptions noted

¹¹Supra note 11.

Appendix F: DHS FY 2019 IG FISMA Metric Results

On October 23, 2019, 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 2019 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY IG 2019 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 2019 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 2019 IG FISMA Reporting Metrics guidance, a security program is considered effective if the majority of the FY 2019 IG FISMA Reporting Metrics are at Level 4: Management and Measurable.

For each of the FY 2019 IG FISMA Reporting Metrics, EXIM management generally assessed the maturity level of its information security program as a Level 4: Managed and Measurable using DHS’ scoring methodology (a five-level maturity model scale). When we assessed EXIM’s information security program for each of the FY 2019 IG FISMA Reporting Metrics, we found that the Identify, Protect, Detect, and Respond Cybersecurity Functions scored at Level 4: Managed and Measurable, and Recover scored at Level 3: Consistently Implemented. Therefore, EXIM’s information security program is considered effective, as stipulated by DHS’ scoring methodology.

However, there were still areas that we evaluated and found would improve the effectiveness of its information security program, EXIM should address the following:

- Areas for improvement in the Identify Domain – Risk Management (RM):
 - Bank should ensure the risk-based allocation of resources for the protection of high value assets through collaboration and data-driven prioritization.
 - EXIM’s existing information security risk management policies and procedures did not fully define and implement action plan(s) for implementing processes to comply with the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act). Additionally, Supporting documentation was unavailable to evidence an analysis of (b) (4) risks was performed and appropriate controls are in place to mitigate those risks (see **Finding 1** in the Findings section above).
 - The Bank management did implement automated solutions to provide (b) (4) across the organization, including (b) (4)

- Areas for improvement in the Protect Domain – Configuration Management (CM)
 - Not applicable – No CM metric was assessed below a Level 4: Management and Measurable.

- Areas for improvement in the Protect Domain – Identity and Access Management (IA):
 - EXIM should employ automation to (b) (4) with necessary parties.
 - EXIM should use automation to (b) (4) To the extent practical, this process should be centralized.
 - EXIM should employ automated mechanisms (e.g. machine-based, or user based enforcement) to support the management of (b) (4)

- Areas for improvement in the Protect Domain – Data Protection and Privacy (DP):
 - EXIM should implemented safeguards to monitor and prevent unauthorized exfiltration of information from the Bank’s information systems. Specifically, (b) (4)

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

 - EXIM should measure the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting (b) (4) Additionally, the organization make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.

- Areas for improvement in the Protect Domain – Security Training (ST):
 - Not applicable – No ST metric was assessed below a Level 4: Management and Measurable.

- Areas for improvement in the Detect Domain – Information Security Continuous Monitoring (ISCM):
 - The Bank should implement processes to (b) (4) and make updates on lessons learned.

- The Bank management did not fully implement (b) (4)
(see Finding 2 in the **Findings** section above).
- Areas for improvement in the Respond Domain – Incident Response (IR):
 - EXIM should fully implement solutions to detect, analyze, and if necessary remediate internal and external incidents and threats in a timely manner.
 - The Bank should sufficiently maintain evidence for the consistent use of performance metrics for (b) (4)
- Areas for improvement in the Recover Domain – Contingency Planning (CP):
 - EXIM management did not manage the Bank’s (b) (4) related to contingency planning activities. Management did not integrate (b) (4) into the Bank’s contingency planning policies and procedures, define and implement a contingency plan for the Bank’s (b) (4) apply appropriate (b) (4) controls to alternate (b) (4) and consider alternate (b) (4) for the Bank’s (b) (4) and to support critical information systems (Level 4: Managed and Measurable metrics not met).
 - EXIM should formally conduct and document the analysis and results for entity-level and system-level business impact analysis’ (see Finding 4 in the **Findings** section above).
 - EXIM should integrate metrics on the effectiveness of its information system contingency plans with (b) (4) such as (b) (4)
 - EXIM should employ automated mechanisms to (b) (4) more thoroughly and effectively. In addition, EXIM should (b) (4) as appropriate.
 - EXIM should monitor effectiveness of recovery activities are communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

The following tables summarizes of our assessed maturity levels for the FY 2019 IG FISMA Metric Results.

Table 5: EXIM FY 2019 IG FISMA Metric Results

Function 1: Identify - Risk Management

Function	Count
Ad-hoc	0
Defined	3
Consistently Implemented	1
Managed and Measurable	7
Optimized	1
Function Rating:	Managed and Measurable (Level 4)

Function 2A: Protect - Configuration Management

Function	Count
Ad-hoc	0
Defined	0
Consistently Implemented	1
Managed and Measurable	7
Optimized	0
Function Rating:	Managed and Measurable (Level 4)

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-hoc	0
Defined	0
Consistently Implemented	3
Managed and Measurable	6
Optimized	0
Function Rating:	Managed and Measureable (Level 4)

Function 2C: Protect – Data Protection and Privacy

Function	Count
Ad-hoc	0
Defined	2
Consistently Implemented	1
Managed and Measurable	2
Optimized	0
Function Rating:	Managed and Measureable (Level 4)

Function 2D: Protect – Security Training

Function	Count
Ad-hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	4
Optimized	2
Function Rating:	Managed and Measureable (Level 4)

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

Function	Count
Ad-hoc	0
Defined	2
Consistently Implemented	2
Managed and Measurable	3
Optimized	0
Function Rating:	Managed and Measureable (Level 4)

Function 5: Recover - Contingency Planning

Function	Count
Ad-hoc	0
Defined	1
Consistently Implemented	5
Managed and Measurable	1
Optimized	0
Function Rating:	Consistently Implemented (Level 3)

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Managed and Measureable (Level 4)	Managed and Measureable (Level 4)	We determined that EXIM's information security program and practices for Risk Management at the Managed and Measurable maturity level 4.
Function 2A: Protect – Configuration Management	Managed and Measureable (Level 4)	Managed and Measureable (Level 4)	We determined that EXIM's information security program and practices for Configuration Management at the Managed and Measurable maturity level 4.

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 2B: Protect – Identity and Access Management	Managed and Measureable (Level 4)	Managed and Measureable (Level 4)	We assessed EXIM’s information security program and practices for Identity and Access Management at the Managed and Measurable maturity level 4.
Function 2C: Protect – Data Protection and Privacy	Managed and Measureable (Level 4)	Managed and Measureable (Level 4)	We assessed EXIM’s information security program and practices for Data Protection and Privacy at the Managed and Measurable maturity level 4.
Function 2D: Protect – Security Training	Managed and Measureable (Level 4)	Managed and Measureable (Level 4)	We assessed EXIM’s information security program and practices for Security Training at the Managed and Measurable maturity level 4.
Function 3: Detect - ISCM	Managed and Measureable (Level 4)	Managed and Measureable (Level 4)	We assessed EXIM’s information security program and practices for ISCM at the Managed and Measurable maturity level 4.
Function 4: Respond - Incident Response	Managed and Measureable (Level 4)	Managed and Measureable (Level 4)	We determined that EXIM’s information security program and practices for Incident Response at the Managed and Measurable maturity level 4.
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	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 Consistently Implemented maturity level.
Overall	Effective	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.

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
			<p>Although we noted deficiencies affecting specific questions within the RM, DP, ISCM, IR, and CP metric domains, we determined its information security program was effective as we evaluated the majority of the FY 2019 IG FISMA Reporting Metrics at the Managed and Measurable (Level 4) or high maturity levels.</p>

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 EXIM-Online (EOL) as it was selected for testing in the 2018 FISMA performance audit. We randomly selected Financial Management System – Next Generation (FMS-NG) to use for system-level testing for the FY 2019 Inspector General Federal Information Modernization Act of 2014 Reporting Metrics (FY 2019 IG FISMA Reporting Metrics). Additionally, for FMS-NG, 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) (4) to be used for performing system-level test work over FY 2019 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 2019 EXIM FISMA performance audit:

- FMS-NG was tested for system-level procedures in support of the FY 2019 IG FISMA Reporting Metrics.
- FMS-NG was tested for 13 additional selected NIST SP 800-53 controls.
- (b) (4) was tested for contractor and cloud specific test procedures in support of the FY 2019 IG FISMA Reporting Metrics.

Appendix H: Distribution List

Kimberly Reed, President and Chairman
David Fogel, Senior Vice President and Chief of Staff
Adam Martinez, Chief Management Officer
Lauren Fuller, Senior Advisor to the President and Chairman
Stephen Renna, Chief Banking Officer
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Mary Jean Buhler, Chief Financial Officer
David Slade, Senior Vice President and General Counsel
David Sena, Senior Vice President of Board Authorized Finance
Inci Tonguch-Murray, Deputy Chief Financial Officer
Patricia Wolf, Vice President and Controller
Cristopolis Dieguez, Director, Internal Controls and Compliance
James DeVaul, Partner, KPMG LLP
Courtney Potter, Deputy AIG for Audits and Evaluations, OIG
Amanda Myers, Counsel, OIG

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

