



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

Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices Report – Fiscal Year 2020

February 4, 2021

OIG-AR-21-03

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 or the Agency) is the official export credit agency of the United States (U.S.). EXIM is an independent, self-financing executive agency and a wholly owned U.S. government corporation. EXIM'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 the Agency's 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 on the Effectiveness of EXIM's Information Security Program and Practices Report – Fiscal Year 2020

Date: February 4, 2021

This memorandum transmits the independent audit report on the effectiveness of the Export-Import Bank of the United States (EXIM or the Agency) information security program and practices for fiscal year (FY) 2020. 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). In addition, we requested that KPMG perform an independent vulnerability assessment over select EXIM information systems. The objectives of the vulnerability assessment were to determine whether the Agency's information systems are properly managed and configured to prevent unauthorized users from gaining access and whether significant security vulnerabilities and weaknesses exist.

KPMG determined that EXIM's information security program and practices were effective overall as a result of a majority of the FY 2020 Inspector General FISMA Reporting Functions scored a Level 4: Managed and Measurable (Identify, Protect, Detect, and Respond). However, deficiencies were found within the Cybersecurity Functions areas of Identify, Detect and Protect and three FISMA metric domains that need improvement, but were not pervasive to affect the overall effectiveness and assessment of the program. Management concurred with all six recommendations contained in the report. We consider management's proposed actions to be responsive. Therefore, the recommendations will be closed upon completion and verification of the implementation 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 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.



February 4, 2021

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 2020

Dear Ms. Fain,

We are pleased to submit this report, which presents the results of our independent performance audit of the Export-Import Bank of the United States (EXIM or the Agency) 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 evaluation 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 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 4.0, dated April 17, 2020 (FY 2020 IG FISMA Reporting Metrics). The EXIM Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct this independent performance 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.

The objective for this independent performance audit was to determine whether EXIM developed and implemented an effective information security program and practices for fiscal year 2020 in accordance with the criteria set forth by FY2020 IG FISMA Reporting Metrics. KPMG evaluated EXIM'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).

¹ Contract No. GS-00F-275CA, Task Order 83310118F0016, dated March 22, 2020

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.

In addition, the OIG requested that KPMG perform an independent vulnerability assessment³ over select EXIM information systems. The objectives of the vulnerability assessment were to determine whether EXIM's information systems are properly managed and configured to prevent unauthorized users from gaining access and whether significant security vulnerabilities and weaknesses exist. Detailed results of the vulnerability assessment were transmitted in a restricted disclosure report to EXIM and EXIM OIG. The related findings and recommendations are incorporated in **Finding 3** below.

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 2020 IG FISMA Reporting Metrics and assessed the maturity levels on behalf of the EXIM OIG. Additional details regarding the scope of our independent performance audit are included in the **Objective, Scope, and Methodology** section and **Appendix A, Scope and Methodology**. **Appendix C, 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 Functions⁴ and eight FISMA Metric Domains.⁵ 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. KPMG assessed EXIM's information security program against the DHS FY 2020 IG FISMA Reporting Metrics, we found that the Cybersecurity Functions' Identify, Protect, Detect, and Respond scored at Level 4: Managed and Measurable; and Recover scored at Level 3: Consistently Implemented.

Based on the results of our performance audit procedures, the majority of EXIM's Cybersecurity Functions scored at a Level 4: Managed and Measurable, therefore, the information security program was considered effective according to the instructions detailed within **Appendix F, DHS' FY 2020 IG FISMA Reporting Metrics**.

However, we did identify deficiencies within the Cybersecurity Functions areas of Identify, Detect and Protect and FISMA program areas of Risk Management and Information Security Continuous Monitoring. Specifically, we noted the following:

Cybersecurity Function: Identify

³ A vulnerability assessment is a technical review of security weaknesses, flaws, and misconfigurations in an information system.

⁴ OMB, DHS, and CIGIE developed the FY 2020 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. In FY 2020, 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*.

⁵ As described in the FY 2020 IG FISMA Reporting Metrics, Version 4.0, April 17, 2020, 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.

EXPORT-IMPORT BANK – OFFICE OF INSPECTOR GENERAL

1. EXIM has not implemented (b) (4)

(FISMA domain:

(b) (4))

Cybersecurity Function: Detect

2. EXIM has not fully implemented policies and procedures for (b) (4)

(FISMA domain: (b) (4))

Cybersecurity Function: Protect

3. (b) (4) vulnerabilities and weaknesses (b) (4) were identified.

(FISMA domain: (b) (4))

KPMG considered these deficiencies when we assessed the maturity levels for the FY 2020 IG FISMA Reporting Metrics. We provided recommendations related to these three 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 EXIM and OIG, and is not intended to be, and should not be used by anyone other than these specified parties.

Sincerely,

KPMG LLP

February 4, 2021

EXECUTIVE SUMMARY

Independent Audit of EXIM's Information Security
Program and Practices Effectiveness for FY 2020
OIG-AR-21-03, February 4, 2021

Why We Did This Audit

The Federal Information Security Modernization Act of 2014 (FISMA or 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 (KPMG) for an independent audit of the effectiveness of the Export-Import Bank of the United States' (EXIM or the Agency) 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, KPMG performed an independent vulnerability assessment over select EXIM information systems and followed-up on prior-year FISMA findings.

What We Recommend

Six recommendations were made 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 the testing of the fiscal year (FY) 2020 Inspector General FISMA Reporting Functions, for which the majority 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 three Cybersecurity Functions (Identify, Protect, and Detect) and three FISMA Metric Domains (

(b) (4)) 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 2019 FISMA performance audit and effectively designed and implemented the 13 additional 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. 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.

However, for Cybersecurity Function Protect and Recover and FISMA Metric Domain Data Protection and Privacy and Contingency Planning, EXIM should continue to develop and implement controls and practices that can meet the Level 4 maturity of Managed and Measurable to consistently evaluate and improve the effectiveness of its information security program. Lastly, EXIM can further strengthen its overall security program and the various cybersecurity functions by addressing the findings and recommendations in this report including the areas identified for improvement in Appendix F.

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
TABLE OF CONTENTS	ii
LIST OF TABLES.....	iii
ABBREVIATIONS AND GLOSSARY	iv
INTRODUCTION.....	5
OBJECTIVE, SCOPE, AND METHODOLOGY	5
BACKGROUND.....	6
AUDIT RESULTS	9
FINDINGS.....	9
Finding 1: Identify Function: Deficiency in the implementation of (b) (4)	9
Finding 2: Detect Function: (b) (4) was not Fully Established	11
Finding 3: Protect Function: (b) (4) Vulnerabilities and Weaknesses (b) (4) were Identified.	12
CONCLUSION.....	17
APPENDICES	18
Appendix A: Scope and Methodology	18
Appendix B: Federal Laws, Regulations, and Guidance	20
Appendix C: Status of Prior-Year Recommendations	21
Appendix D: Management’s Response	25
Appendix E: Security Controls Section	27
Appendix F: DHS FY 2020 IG FISMA Metric Results	28
Appendix G: System Selection Approach.....	35
Appendix H: Distribution List	36

LIST OF TABLES

Table 1: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2020 IG FISMA Metric Domains	8
Table 2: Inspector General Assessed Maturity Levels	8
Table 3: Status of Prior Audit Recommendations.....	21
Table 4: Additional Security Controls and Testing Results	27
Table 5: EXIM’s FY 2020 IG FISMA Metric Results	30

ABBREVIATIONS AND GLOSSARY

BIA	Business Impact Analysis
CIO	Chief Information Officer
CIGIE	Council of Inspectors General on Integrity and Efficiency
CP	Contingency Plan
DHS	Department of Homeland Security
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
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
SP	Special Publication

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) of the effectiveness of the information security program and practices of the Export-Import Bank of the United States (EXIM or the Agency) for fiscal year (FY) 2020. The objective was to determine whether EXIM developed and implemented effective information security program and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA).

In addition, the OIG requested that KPMG perform an independent vulnerability assessment⁶ over select EXIM information systems. The objectives of the vulnerability assessment were to determine whether EXIM information systems are properly managed and configured to prevent unauthorized users from gaining access and whether significant security vulnerabilities and weaknesses exist. Detailed results of the vulnerability assessment were transmitted in a restricted disclosure report to EXIM and EXIM OIG. The related findings and recommendations are incorporated in **Finding 3** below.

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, 2020. To address our objective, we evaluated the Agency'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) (4)

and performed the detailed steps prescribed in the *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2020 IG FISMA Reporting Metrics), version 4.0, dated April 17, 2020, 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). We also followed up on the status of prior-year FISMA findings. Finally, at the request of the OIG, we performed an independent internal and external vulnerability assessment over select EXIM information systems. The testing plan was conducted in accordance with NIST and FISMA requirements to evaluate internal controls that would prevent and detect unauthorized access, disclosure, modification, or deletion of sensitive data. See **Appendix A** for more details on the scope and methodology.

⁶ A vulnerability assessment is a technical review of security weaknesses, flaws, and misconfigurations in an information system.

BACKGROUND

EXIM is an independent, self-financing executive agency and a wholly owned United States (U.S.) government corporation. EXIM's charter, *The Export Import Bank Act of 1945*, as amended through Public Law 116-94, December 20, 2019, 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. EXIM 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 mission-critical systems supporting these programs and the Agency's mission are:

(b) (4)

EXIM's network infrastructure consists (b) (4)

The networks are protected from external threats by (b) (4)

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,⁷ 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.

⁷ 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 other 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 2020 IG FISMA Reporting Metrics. DHS revised the FY 2019 IG FISMA Reporting Metrics and issued the FY 2020 IG FISMA Reporting Metrics, Version 4.0 on April 17, 2020. 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 Functions⁸ outlined in the NIST Cybersecurity Framework⁹ 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, Data Protection and Privacy, Security Training, Information System Continuous Monitoring, Incident Response and Contingency Planning. See **Table 1** below for a description of the NIST Cybersecurity Framework Security Functions and the associated FY 2020 IG FISMA Metric Domains.

⁸ 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.

⁹ 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 2020 IG FISMA Metric Domains**

Cybersecurity Framework Security Functions	FY 2020 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 2020 IG FISMA Reporting Metrics are at Level 4: Management and Measurable. **Table 2** below 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, and many improvements to the contingency planning program. We found the program was effective as a result of a majority of FY 2020 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 three of the five Cybersecurity Functions (Identify, Detect, and Protect) and three of the eight FISMA Metric Domains (b) (4)) 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 2020 IG FISMA Reporting Metric assessment is in **Appendix F**.

As noted above, we evaluated the open prior-year findings from the FY 2019 FISMA performance audits 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, EXIM's Chief Management Officer concurred with our findings and recommendations (see **Appendix D**, *Management Response*).

FINDINGS

Finding 1: Identify Function: Deficiency in the implementation of (b) (4)

During FY 2020, we noted that EXIM had not implemented (b) (4) that provides

(b) (4)

EXIM was focused on implementing (b) (4) but did not employ (b) (4)

Without the implementation of (b) (4), EXIM
may not be able to identify and mitigate (b) (4) risks appropriately.

The following guidance is relevant to this deficiency:

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

(b) (4)

(b) (4)

We recommend that the Office of the Chief Information Officer:

1. Define the strategy and roadmap, including the policies and procedures for (b) (4) that encompasses all necessary sources of risk data.
2. Implement the (b) (4) based on the requirements defined within the strategy and ensure the policies and procedures are consistently implemented (b) (4).

Management's Response:

EXIM management concurred with the finding. (b) (4)

Evaluation of Management's Response: If implemented properly, we believe that the process management has defined above for remediating this issue will assist in establishing (b) (4)

Finding 2: Detect Function: (b) (4)
was not Fully Established

In the FY 2018 FISMA performance audit, we noted that EXIM had not fully established (b) (4)

. We reported that EXIM did not fully implement (b) (4)
. EXIM used (b) (4) ; however, (b) (4) did not meet the minimum requirements for a DHS Continuous Diagnostics and Mitigation (CDM) Program.

In the FY 2019 FISMA performance audit, to address this deficiency, we noted the Agency installed (b) (4) and began to implement (b) (4)

. During the FY 2020 FISMA performance audit, we noted that EXIM implemented and configured (b) (4) and staffed the (b) (4). This specific (b) (4) is a (b) (4)

. However, EXIM has not fully implemented policies and procedures for (b) (4)

. During FY 2020, EXIM successfully implemented and configured (b) (4) ; however due to timing constraints and limited resources, the activities associated with a (b) (4) have not been completed.

Without the full implementation of (b) (4) , the Agency's ability to identify and mitigate the impact of emerging cybersecurity threats on (b) (4) may be impacted.

The following guidance is relevant to this deficiency:

(b) (4)

(b) (4)

(b) (4)

We recommend that the Office of the Chief Information Officer:

3. Define audit review, analysis and reporting policies and procedures for (b) (4) and (b) (4).
4. Implement the defined audit review, analysis, and reporting policies and procedures for (b) (4) and ensure operational effectiveness and compliance.

Management's Response:

EXIM management concurred with the finding. (b) (4)

Evaluation of Management's Response: If implemented properly, we believe that the process management has defined above for remediating this issue will assist in establishing (b) (4).

Finding 3: Protect Function: (b) (4)
(b) (4)

**Vulnerabilities and Weaknesses
were Identified.**

Based on our internal vulnerability testing at EXIM, we identified (b) (4)

(b) (4)

(b) (4)

In addition, we determined (b) (4)

management self-identified (b) (4)
issue but required (b) (4)
formally documented as a Plan of Action and Milestone (POA&M).

We were informed that EXIM
and was aware of the
; however, the issue was not

Furthermore, (b) (4)

. We informed EXIM management of the
vulnerabilities described above and provided detailed results from the testing. Based on our
discussions with EXIM management and review of available documentation, we determined that
the weaknesses identified were due to the following:

(b) (4)

Without effective (b) (4)

practices, (b) (4)

(b) (4)
, which is vital to EXIM's mission. The organizational risks could lead to
can lead to increased risk to (b) (4)

In addition, absent effective (b) (4)

. Failure to remedy the underlying causes for the
conditions noted above could result in (b) (4)

The following guidance is relevant to this deficiency:

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

We recommend that the Office of the Chief Information Officer:

5. Enhance (b) (4) to ensure (b) (4) are applied in accordance with EXIM security policies in order to effectively (b) (4). If required (b) (4), consistently document the business rationale or technical issues delaying the remediation of vulnerabilities within a POA&M.
6. Expand (b) (4) procedures to ensure that (b) (4).

Management's Response:

Management concurred with the finding. (b) (4)

(b) (4)

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

CONCLUSION

Based on our testing of the FY 2020 IG FISMA Reporting Metrics and the associated scoring guidance, the majority of the five Cybersecurity Functions and eight FISMA Metric Domains were scored at a Level 4 (Managed and Measurable) for EXIM. Therefore, the Agency's information security program and practices were determined to be effective overall despite the findings discussed within this report for FY 2020.

We determined that EXIM remediated many of the prior year deficiencies reported in the FY 2019 FISMA performance audit (see **Appendix C** for details). 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.

In addition, EXIM should implement corrective actions to strengthen (b) (4)

.

APPENDICES

Appendix A: Scope and Methodology

To evaluate the effectiveness of EXIM's information security program and its compliance with FISMA, we conducted a performance audit that was focused on the information security controls, program, and practices at the Agency level (entity level) and for a selection of information systems. In addition, at the request of the OIG, we performed an independent vulnerability assessment over select EXIM information systems.

We conducted the performance audit and vulnerability assessment in accordance with GAGAS and with Consulting Services Standards established by the AICPA. 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 (b) (4), and tested (b) (4) for additional NIST security controls. See **Appendix G, System Selection Approach**.

To assess EXIM's maturity levels for *FY 2020 Inspector General Information Security Modernization Act of 2014 Reporting Metrics* (FY 2020 IG FISMA Reporting Metrics), we performed test procedures at the Agency 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 2020 IG FISMA Reporting Metrics:

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 Agency. 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 Agency and (b) (4) 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 SP 800-53, Rev. 4 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.
3. For maturity level 3 controls determined to be effective, we performed level 4 (Managed and Measurable) test procedures for the Agency, (b) (4) 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 Agency, (b) (4) 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 2020 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 2020 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 (b) (4) .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 Information 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.

As noted above, we also conducted a vulnerability assessment over select information systems. The security testing plan was conducted in accordance with NIST and FISMA requirements to evaluate internal controls that would prevent and detect unauthorized access, disclosure, modification, or deletion of sensitive data.

The test work was performed remotely due to the novel coronavirus (COVID-19) pandemic as the Office of Personnel Management (OPM) announced the exercise of maximum telework for government functions. We performed our fieldwork with EXIM management and IT personnel during the period of May 1, 2020, through October 23, 2020. During our audit, we met 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.

¹¹ In addition to evaluating EXIM's maturity levels for the FY 2020 IG FISMA Reporting Metrics, (b) (4) , effective March 22, 2020, required us to test additional NIST 800-53 controls for a selected information system.

Appendix B: Federal Laws, Regulations, and Guidance

Our performance audit of the effectiveness of EXIM's information security program and practices and vulnerability assessment were 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 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 4.0, dated April 17, 2020
- 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. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*
- NIST SP800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
- 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 the FY 2020 FISMA performance audit, we followed up on the status of open prior-year findings. We inquired of 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: Status of Prior Audit Recommendations

Finding	Recommendation	FY Identified	Status
<i>Independent Audit of the Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2018</i> (OIG-AR-19-03 , March 13, 2019)			
Finding 2: EXIM's (b) (4) was not fully established.	We recommended that EXIM Management: 7) Complete the (b) (4) and (b) (4) to analyze event data in real time for the (b) (4)	2018	Closed
<i>Independent Audit of EXIM's Information Security Program Effectiveness for Fiscal Year 2019</i> (OIG-AR-20-04 , January 13, 2020)			
Finding 1: 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 Act).	We recommended that the Office of the Chief Information Officer (OCIO): 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.	2019	Closed

EXPORT-IMPORT BANK – OFFICE OF INSPECTOR GENERAL

Finding	Recommendation	FY Identified	Status
<p><u>Finding 2:</u> (b) (4)</p> <p>was not fully established.</p>	<p>We recommended that the OCIO:</p> <p>2) Fully implement and configure (b) (4) across all of the Bank's information systems.</p> <p>3) Configure the (b) (4)</p> <p>4) Perform and document evidence of a periodic review of the reported activity and perform research and resolution, as appropriate.</p>	2019	<p>Closed – Recommendation #2</p> <p>Recommendations 3 and 4 were not fully remediated; therefore, the recommendations are closed and reissued in this report. Refer to Finding #2 in the Findings section above for the FY 2020 audit results and the updated recommendations.</p>

EXPORT-IMPORT BANK – OFFICE OF INSPECTOR GENERAL

Finding	Recommendation	FY Identified	Status
<p><u>Finding 3:</u> EXIM Bank does not have sufficient safeguards implemented to monitor and prevent unauthorized exfiltration of information from the Bank's information systems. Specifically, (b) (4)</p> <p>It was noted that the Bank does receive an automated email from (b) (4)</p>	<p>We recommended that the OCIO:</p> <p>5) Implement controls to review employees periodically who have an organizational exception for (b) (4) and (b) (4)</p> <p>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, 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.</p>	2019	Closed
<p><u>Finding 7:</u> EXIM management did not complete a formally documented analysis to determine mission/business processes and (b) (4)</p> <p>Additionally, the Bank did not (b) (4)</p>	<p>We recommended that the OCIO:</p> <p>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.</p>	2019	Closed

EXPORT-IMPORT BANK – OFFICE OF INSPECTOR GENERAL

Finding	Recommendation	FY Identified	Status
<p>(b) (4)</p> <p>However, the Bank did perform informal organizational and system-level 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.</p>			

Appendix D: Management's Response



Reducing Risk. Unleashing Opportunity.

DATE: January 22, 2021

TO: Jennifer Fain, Acting Inspector General, Office of Inspector General

THROUGH: Mary Jean Buhler, SVP & Chief Financial Officer

FROM: Adam Martinez, Chief Management Officer **ADAM MARTINEZ**
Digitally signed by
ADAM MARTINEZ
Date: 2021.01.22
15:05:24 -05'00'

SUBJECT: EXIM Management Response to the draft report, Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices for Fiscal Year 2020 (OIG-AR-21-03)

Dear Ms. Fain,

Thank you for providing the Export-Import Bank of the United States ("EXIM" or "EXIM Bank") management with the Office of Inspector General's ("OIG") *Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices for Fiscal Year 2020*, OIG-AR-21-03, dated December 23, 2020 (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 have been maintained for the five Cybersecurity Functions and eight FISMA Metric Domains." Further, EXIM appreciates KPMG recognizing that "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 a contingency planning program." EXIM also appreciates that KPMG found that EXIM's "program and practices were effective overall as a result of the testing of the FY 2020 Inspector General FISMA Reporting Functions, for which the majority scored a Level 4: Managed and Measurable (Identify, Protect, Detect, and Respond), as described by the DHS criteria".

EXPORT-IMPORT BANK – OFFICE OF INSPECTOR GENERAL



Reducing Risk. Unleashing Opportunity.

We agree with the recommendations and 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.

CC:

Kenneth Tinsley, SVP and Chief Risk Officer
Howard Spira, SVP and Chief Information Officer
Gabriel Smith-Sherman, Chief Information Systems Officer
Henry Pitney, Acting SVP and General Counsel
Andrea Bernardo, Assistant General Counsel for Administration
Inci Tonguch-Murray, Deputy Chief Financial Officer
Cris Dieguez, Director, Internal Controls and Compliance

Appendix E: Security Controls Section

During planning, we identified the NIST SP 800-53, Rev. 4, controls referenced in the FY 2020 IG FISMA Reporting Metrics, and we judgmentally selected additional NIST SP 800-53, Rev. 4 controls to obtain a total population of 25-35 controls.¹² To do so, we performed an analysis and determined that the FY 2020 DHS IG FISMA Reporting Metric had 22 unique NIST 800-53, Rev. 4 security controls that were to be tested at the system level. Therefore, we judgmentally identified the following 13 additional NIST SP 800-53, Rev. 4 controls to test for (b) (4).

Table 4: Additional Security Controls and Testing Results

No.	NIST SP 800-53 Security Control	Control Name	System	Results
1	PL-2	System Security Plan	(b) (4)	No exceptions noted
2	RA-3	Risk Assessment	(b) (4)	No exceptions noted
3	CA-4	Security Certification	(b) (4)	No exceptions noted
4	CA-6	Security Accreditation	(b) (4)	No exceptions noted
5	IA-2	User Identification and Authentication	(b) (4)	No exceptions noted
6	AC-2	Account Management	(b) (4)	No exceptions noted
7	AC-6	Least Privilege	(b) (4)	No exceptions noted
8	CM-3	Configuration Change Control	(b) (4)	No exceptions noted
9	CP-9	Information System Backup	(b) (4)	No exceptions noted
10	RA-4	Risk Assessment Update	(b) (4)	No exceptions noted
11	PS-4	Personnel Termination	(b) (4)	No exceptions noted
12	PS-5	Personnel Transfer	(b) (4)	No exceptions noted
13	CM-1	Configuration Management Policy and Procedures	(b) (4)	No exceptions noted

¹²*Supra* note 11.

Appendix F: DHS FY 2020 IG FISMA Metric Results

On October 16, 2020, we provided EXIM OIG with the assessed maturity levels for each of the 67 questions outlined in the FY IG 2020 FISMA Reporting Metrics. The following tables represent each of the NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond, and Recover) that were assessed to respond to the FY 2020 IG FISMA Reporting Metrics. Each of the five functions had specific evaluation questions that were 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 2020 IG FISMA Reporting Metrics guidance, a security program is considered effective if the majority of the FY 2020 IG FISMA Reporting Metrics are at Level 4: Management and Measurable.

For each of the FY 2020 IG FISMA Reporting Metrics, EXIM management generally self-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 KPMG assessed EXIM’s information security program for each of the FY 2020 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 KPMG evaluated and found would improve the effectiveness of its information security program, EXIM should address the following:

- Areas for improvement in the Identify Function – (b) (4) domain:
 - EXIM should implement (b) (4)

(see **Finding 2** in the Findings section above).
 - EXIM should define (b) (4)

.
- Areas for improvement in the Protect Function – (b) (4) domain:
 - The Agency should improves its policies and procedures around (b) (4)

see **Finding 3** in the Findings section above).
- Areas for improvement in the Protect Function – (b) (4) domain:
 - EXIM should employ (b) (4)

.

EXPORT-IMPORT BANK – OFFICE OF INSPECTOR GENERAL

- EXIM should (b) (4)
- EXIM should employ (b) (4)

 , as appropriate.
- Areas for improvement in the Protect Function – (b) (4) domain:
 - EXIM should ensure that (b) (4)
 - EXIM should analyze (b) (4)
- Areas for improvement in the Protect Function – (b) (4) domain:
 - Not applicable – No (b) (4) was assessed below a Level 4: Management and Measurable.
- Areas for improvement in the Detect Function – (b) (4) domain:
 - EXIM should implement (b) (4)
 - EXIM management did not fully implement (b) (4)
(see **Finding 1** in the Findings section above).
- Areas for improvement in the Respond Function – (b) (4) domain:
 - EXIM should fully implement (b) (4)
 - EXIM should (b) (4)
- Areas for improvement in the Recover Function – (b) (4) domain:
 - EXIM management did not manage (b) (4)
 . Management did not (b) (4)

- EXIM should integrate (b) (4)

- EXIM should employ (b) (4)

, as appropriate.

- EXIM should monitor (b) (4)

The following tables summarize our assessed maturity levels for the FY 2020 IG FISMA Metric Results.

Table 5: EXIM's FY 2020 IG FISMA Metric Results

Function 1: Identify - Risk Management

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

Function 2A: Protect - Configuration Management

Maturity Level	Count
Ad-hoc	0
Defined	0
Consistently Implemented	3
Managed and Measurable	5
Optimized	0
Function Rating:	Managed and Measurable (Level 4)

Function 2B: Protect - Identity and Access Management

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

Function 2C: Protect – Data Protection and Privacy

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

Function 2D: Protect – Security Training

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

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

Maturity Level	Count
Ad-hoc	0
Defined	0
Consistently Implemented	1
Managed and Measurable	6
Optimized	0
Function Rating:	Managed and Measurable (Level 4)

Function 5: Recover - Contingency Planning

Maturity Level	Count
Ad-hoc	0
Defined	0
Consistently Implemented	6
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 Measurable (Level 4)	Managed and Measurable (Level 4)	We assessed 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 Measurable (Level 4)	Managed and Measurable (Level 4)	We assessed EXIM's information security program and practices for Configuration Management at the Managed and Measurable maturity level 4.
Function 2B: Protect – Identity and Access Management	Managed and Measurable (Level 4)	Managed and Measurable (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	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	Managed and Measurable (Level 4)	Managed and Measurable (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 Measurable (Level 4)	Managed and Measurable (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 Measurable (Level 4)	Managed and Measurable (Level 4)	We assessed 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 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. Although we noted deficiencies (b) (4), we determined its information security program was effective as we evaluated the majority of the FY 2020 IG

EXPORT-IMPORT BANK – OFFICE OF INSPECTOR GENERAL

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
			FISMA Reporting Metrics at the Managed and Measurable (Level 4) or high maturity levels.

Appendix G: System Selection Approach

We obtained a listing of all systems from EXIM’s FISMA system inventory and (b) (4)

. We randomly selected (b) (4) to use for system-level testing for the FY 2020 IG FISMA Reporting Metrics. Additionally, (b) (4), we tested 13 additional NIST 800-53 controls detailed in **Appendix E, Security Controls Selection**.

We then (b) (4) to identify cloud-based contractor systems or managed by third parties that had a FIPS 199 Moderate impact rating and contained PII. We judgmentally (b) (4) to perform system-level test work over FY 2020 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 2020 EXIM FISMA performance audit:

(b) (4)

Appendix H: Distribution List

James Cruse, First Vice President and Vice Chairman (Acting)
Adam Martinez, Senior Vice President and Chief Management Officer
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Mary Jean Buhler, Chief Financial Officer
Henry Pitney, Acting Senior Vice President and General Counsel
Gabriela Smith-Sherman, Chief Information Security Officer
Inci Tonguch-Murray, Senior Vice President and Deputy Chief Financial Officer
Cristopolis Dieguez, Director, Internal Controls and Compliance
Jason Gould, Managing Director, KPMG LLP
Courtney Potter, Deputy AIG for Audits and Evaluations, OIG
Jaquone Miller, Project Manager, OIG
Amanda Myers, Senior 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

