



Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices Report for Fiscal Year 2024



OIG-AR-24-04
September 20, 2024

Office of Inspector General (OIG)
Export-Import Bank of the United States



To: Howard Spira
Senior Vice President and Chief Information Officer

From: Eric Rivera
Assistant Inspector General for Audits

Subject: Independent Audit on the Effectiveness of EXIM's Information Security
Program and Practices – Fiscal Year 2024

Date: September 20, 2024

This memorandum transmits the report of the independent audit on the effectiveness of the Export-Import Bank of the United States' (EXIM) information security program and practices for fiscal year (FY) 2024. Under a contract monitored by this office, we engaged the independent public accounting firm of KPMG LLP (KPMG) to conduct a performance audit. The objective of the audit 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 conducted the audit in accordance with generally accepted government auditing standards and is responsible for the findings and conclusions expressed in this report. As part of this engagement, KPMG did not express opinions on EXIM's internal controls or draw conclusions on compliance or other matters.

We appreciate the cooperation and courtesies provided to KPMG and this office during the audit. If you have questions, please contact me at (202) 565-3219.



KPMG LLP
Suite 3600
111 Monument Circle
Indianapolis, IN 46204

Eric Rivera
Assistant Inspector General for Audits
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 2024

Dear Mr. Rivera,

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) to determine whether their information security program and practices were effective for fiscal year (FY) 2024, as of September 20, 2024, in accordance 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 2023 - 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (DHS FY 2023-2024 IG FISMA Reporting Metrics). EXIM OIG contracted with KPMG LLP (KPMG) to conduct this independent performance audit. 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. 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.

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.

The objective for this independent performance audit was to determine whether EXIM developed and implemented an effective information security program and practices, as required by FISMA. KPMG evaluated EXIM's security plans, policies, and procedures in place for effectiveness as required by applicable federal law and regulations, guidance issued by OMB and standards and guidelines contained in the National Institute of Standards and Technology (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS).

¹ Contract No. 47QRAD19DU208 Order Number 83310123F0013, Item 1001, dated February 22, 2023 and subsequent contract modifications.



Eric Rivera
Export Import Bank of the United States
Page 2 of 2

We based our independent performance audit work on a selection of EXIM-wide security controls and system-specific security controls applicable to one selected EXIM information system. As part of our audit, we responded to the *DHS FY 2023-2024 IG FISMA Reporting Metrics* and assessed the metric 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 Functions² and nine FISMA Metric Domains.³

Based on the results of our performance audit procedures, all five of EXIM's Cybersecurity Functions were assessed at Level 4: Managed and Measurable. Therefore, the information security program was considered effective according to the instructions detailed within Appendix F, *DHS FY 2023-2024 IG FISMA Reporting Metrics*.

Also, during the past year, EXIM implemented corrective actions to remediate a prior-year finding related to the finalization of its migration to NIST SP 800-53, including the cybersecurity controls such as Personally Identifiable Information (PII) Processing and Transparency-2 and Supply Chain Risk Management-3.

We 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 use and reliance of EXIM, EXIM OIG, DHS, and OMB.

Sincerely,

September 20, 2024

² OMB, DHS, and CIGIE developed the *DHS FY 2023-2024 IG FISMA Reporting Metrics* in consultation with the Federal Chief Information Officers Council. In FY 2024, the nine 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*.

³ As described in the *DHS FY 2023-2024 IG FISMA Reporting Metrics*, the nine FISMA Metric Domains are: risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.



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

OIG-AR-24-04

Why OIG 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 Federal agency, contractor, or source. 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) 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 followed up on one prior-year FISMA finding.

What OIG Found

Under a contract monitored by our office, we engaged KPMG to conduct a performance audit. KPMG did not identify any findings as a result of testing, however KPMG included an opportunity to improve to improve the effectiveness of EXIM's information security program.

EXECUTIVE SUMMARY

Independent Audit of EXIM's Information Security Program and Practices Effectiveness – FY 2024 OIG-AR-24-04, September 20, 2024

What OIG Found

KPMG determined that EXIM's information security program and practices were effective overall as a result of the testing of the fiscal year (FY) 2024 Inspector General FISMA Reporting Functions, for which all (Identify, Protect, Detect, Respond, and Recover) were assessed at Level 4: Managed and Measurable as described by the DHS criteria. Consistent with applicable FISMA requirements, OMB's policy and guidance, the National Institute of Standards and Technology (NIST) Special Publications (SPs) and Federal Information Processing Standards (FIPS), EXIM's information security program and practices for its systems were established and maintained for the five Cybersecurity Functions and nine FISMA Metric Domains. Appendix F contains EXIM's information security program summary results of the DHS FY 2023-2024 IG FISMA Reporting Metrics (the Metrics).

Further, KPMG determined that EXIM had remediated the finding related to its migration to NIST SP 800-53 reported in the FY 2023 FISMA performance audit report (OIG-AR-23-06, September 18, 2023), which pertained to Risk Management.

Finally, as outlined in Appendix E, 25 NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, controls were tested in addition to those identified within the Metrics for one randomly selected system and determined that EXIM effectively designed and implemented these controls.

CONTENTS

EXECUTIVE SUMMARY	i
CONTENTS	ii
LIST OF TABLES	iii
INTRODUCTION	1
OBJECTIVE, SCOPE, AND METHODOLOGY	1
BACKGROUND	1
AUDIT RESULTS	5
FINDINGS & OPPORTUNITY FOR IMPROVEMENT	5
APPENDICES	7
Appendix A: Scope and Methodology	7
Appendix B: Federal Laws, Regulations, and Guidance	9
Appendix C: Status of Prior-Year Recommendations	11
Appendix D: Management’s Response	12
Appendix E: Security Controls Section	12
Appendix F: DHS FY 2023-2024 IG FISMA Reporting Metric Results	14
Appendix G: System Selection Approach	21
ABBREVIATIONS	22

LIST OF TABLES

Table 1: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the DHS FY 2023-2024 IG FISMA Reporting Metric Domains.....	3
Table 2: Inspector General Assessed Maturity Levels	4
Table 3: Status of Prior Audit Recommendations.....	11
Table 4: Additional Security Controls and Testing Results	13
Table 5: EXIM’s FY 2023-2024 IG FISMA Reporting Metric Results.....	14

INTRODUCTION

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) for fiscal year (FY) 2024. The objective was to determine whether EXIM developed and implemented an effective information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether EXIM developed and implemented an effective information security program and practices in accordance with FISMA. To address our objective, we evaluated EXIM's security program, plans, policies, and procedures in place for effectiveness as required by applicable federal law and regulations and guidance issued by the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST). Using evaluation guidance prescribed by the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (DHS FY 2023-2024 IG FISMA Reporting Metrics)*, we evaluated agency and system level security control policies, procedures, and practices associated with the following DHS FY 2023-2024 IG FISMA Reporting Metric Domains:

- Identify – Risk Management and Supply Chain Risk Management;
- Protect – Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
- Detect – Information Security Continuous Monitoring;
- Respond – Incident Response; and
- Recover – Contingency Planning.

We selected one EXIM information system for our performance of system level security control testing procedures: the (b) (7)(E)

We also followed up on the status of the prior-year FISMA audit finding. See Appendix A for more details on the scope and methodology of our performance audit.

BACKGROUND

The Export-Import Bank of the United States is an independent agency and a wholly owned U.S. government corporation that was first organized as a District of Columbia banking corporation in 1934. EXIM is the official export credit agency of the United States.

The mission of EXIM is to support U.S. exports by providing export financing through its loan, guarantee, and insurance programs in cases where the private sector is unable or unwilling to provide financing, or where such support is necessary to level the competitive playing field for U.S. exporters due to financing provided by foreign governments to their exporters. All EXIM

obligations carry the full faith and credit of the U.S. government. The mission-critical IT systems supporting these programs and EXIM's mission are:

(b) (7)(E)



EXIM's network infrastructure consists largely of networking devices with various servers running different operating system platforms. The networks are protected from external threats by a range of information technology security devices and software, including data loss prevention tools, firewalls, intrusion detection and prevention systems, antivirus, software, and spam-filtering systems.

Federal Laws, Roles, and Responsibilities. On December 17, 2002, the President signed into law the E-Government Act, Pub. L. 107-347, which included the Federal Information Security Management Act of 2002. FISMA, as amended,¹ permanently reauthorized the framework established in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA continues the annual review and reporting requirements introduced in GISRA. In addition, FISMA includes additional 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 (SPs). FIPS provide the minimum information security requirements that are necessary to improve the security of federal information and information systems, and SP 800 and selected 500 series SPs 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, as amended. 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 framework for establishing and maintaining 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 executives, in coordination with their Chief Information Officers and agency Information Security Officers, to report the security status of their information systems to Department of Homeland Security (DHS) and OMB, which

¹ On December 18, 2014, FISMA was amended by the Federal Information Security Modernization Act of 2014. Pub. L. 113-283. The amendment: (1) included the reestablishment of the oversight authority of the Director of OMB with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of DHS to administer the implementation of such policies and procedures for information systems.

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 the effectiveness of an agency's information security program. OIGs must also report their results to DHS and OMB annually through CyberScope.

DHS FY 2023-2024 IG FISMA Reporting Metrics. 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 agencies. The metrics are organized around the five Cybersecurity Functions² outlined in the NIST Cybersecurity Framework³ 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, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed and published maturity models for Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information System Continuous Monitoring, Incident Response and Contingency Planning. Table 1, below, contains a description of the NIST Cybersecurity Framework Security Functions and the associated DHS FY 2023-2024 IG FISMA Reporting Metric Domains.

Table 1: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the DHS FY 2023-2024 IG FISMA Reporting Metric Domains⁴

Cybersecurity Framework Security Functions	DHS FY 2023-2024 IG FISMA Reporting Metric Domains
Identify	Risk Management Supply Chain Risk Management
Protect	Configuration Management Identity and Access Management

² 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.

³ 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 leading 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.

⁴ DHS Reporting Metrics, https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf

Cybersecurity Framework Security Functions	DHS FY 2023-2024 IG FISMA Reporting Metric Domains
	Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

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. Table 2, below, provides the descriptions for each maturity level.

Table 2: Inspector General Assessed Maturity Levels⁵

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 strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The maturity level for a domain is based on a calculated average scoring model approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program. A security program is considered effective if the majority of the *DHS FY 2023-2024 IG FISMA Reporting Metrics* are assessed at Level 4: Managed and Measurable. We used this assessment method in our formation of a conclusion on the effectiveness of EXIM’s information security program and practices. For information about our conclusion and the results of our performance audit, see the section immediately below.

⁵ DHS Reporting Metrics, https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf

AUDIT RESULTS

Consistent with applicable FISMA requirements, OMB's policy and guidance, the NIST SP and FIPS, EXIM's information security program and practices for its systems were established and have been maintained for the five Cybersecurity Functions and nine FISMA Metric Domains. During the past year, EXIM fully implemented corrective actions to remediate a prior-year finding related to Risk Management. We calculated the average of the *DHS FY 2023-2024 IG FISMA Reporting Metrics* for the five Cybersecurity Functions at Level 4: Managed and Measurable and therefore found that EXIM's information security program and practices were effective, as prescribed by the DHS criteria.

A summary of the results for the *DHS FY 2023-2024 IG FISMA Reporting Metrics* assessment is in Appendix F.

As noted above, we evaluated the open prior-year finding from EXIM's FY 2023 FISMA performance audit. See Appendix C, Status of Prior-Year Findings, for additional details.

FINDINGS & OPPORTUNITY FOR IMPROVEMENT

Findings

No findings were identified during the performance of the FY 2024 FISMA performance audit.

Opportunity for Improvement

Over the span of several years, KPMG has observed improvement in EXIM's information security program and practices across all five Cybersecurity Functions (Identify, Protect, Detect, Respond, Recover) and nine FISMA Metric Domains (risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning) to achieve an average maturity level of Level 4: Managed and Measurable rating in FY 2024. During the performance of the FY 2024 FISMA performance audit, KPMG assessed two metrics at Level 3: Consistently Implemented. (b) (7)(E)

As these metrics were assessed at a maturity level lower than Level 4: Managed and Measurable, the overall rating for the program, we have identified the following opportunity for improvement that management may consider relative to EXIM's ability and intention to potentially achieve a Level 4 for these two metrics:

EXIM management could assess and, pending results of such assessment and in consideration of resource constraints and prioritization, (b) (7)(E)

We offer this opportunity for improvement because the (b) (7)(E)

(b) (7)(E) (b) (7)(E)
(b) (7)(E) , provided that management determines it necessary to prioritize a goal of potentially achieving Level 4: Managed and Measurable (b) (7)(E)

APPENDICES

Appendix A: Scope and Methodology

To evaluate the effectiveness of EXIM's information security program and its compliance with FISMA, KPMG conducted a performance audit that was focused on the information security controls, program, and practices at the agency level (entity level) and for a selected information system.

We conducted the performance audit in accordance with generally accepted government auditing standards and with Consulting Services Standards established by the American Institute of Certified Public Accountants. 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, we applied procedures to test agency and system level controls, the latter of which were associated with the (b) (7)(E) the one information system we selected for our performance audit. Using the evaluation guidance prescribed in the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (DHS FY 2023-2024 IG FISMA Reporting Metrics)* and the methodology steps outlined below for each of the five Cybersecurity Functions and nine FISMA Metric Domains from the *DHS FY 2023-2024 IG FISMA Reporting Metrics*, we:

- Requested that EXIM management communicate its self-assessed maturity levels, where applicable, to help us confirm our understanding of the FISMA-related policies and procedures, guidance, structures, and processes established by EXIM.
- Performed procedures designed to assess whether agency (b) (7)(E) system-level controls were suitably designed and operating effectively to address requirements associated with Level 3: Consistently Implemented maturity models for all nine FISMA Metric Domains. If, based on the results of testing performed, we determined that one or more controls did not meet such requirements, we assessed such controls as Level 1: Ad Hoc or 2: Defined for the associated FISMA Metric Domain questions.
- For controls that, based on testing performed, met requirements associated with Level 3: Consistently Implemented maturity models, performed additional procedures designed to assess whether agency (b) (7)(E) system-level controls were suitably designed and operating effectively to address requirements associated with Level 4: Managed and Measurable maturity models for applicable FISMA Metric Domain questions.
- For controls that, based on testing performed, met requirements associated with Level 4: Managed and Measurable maturity models, performed additional procedures designed to assess whether agency (b) (7)(E) system-level control were suitably designed to address requirements associated with Level 5: Optimized maturity models for applicable FISMA Metric Domain questions. The test procedures associated with this assessment focused specifically on the evaluation of the design of the controls.

As prescribed in the *DHS FY 2023-2024 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 2023-2024 IG FISMA Metric Results*.

In addition to the procedures above, we selected 25 additional NIST SP 800-53, Rev. 5, security controls that were not referenced in the *DHS FY 2023-2024 IG FISMA Reporting Metrics* and developed and executed test procedures to test such controls (b) (7)(E). See Appendix E, Security Controls Selection, for a list of the controls that were selected for testing.

To assess the effectiveness of the information security program and practices of EXIM, we performed various procedures, including:

- 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 EXIM's 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.

We relied on computer-generated data as part of performing this audit. We assessed the reliability of the data by (1) observing the generation of the data, (2) inspecting parameters or logic used to generate the data, and (3) interviewing EXIM officials knowledgeable about the data. We determined that the data was sufficiently reliable for testing purposes.

We performed our fieldwork with EXIM management and IT personnel during the period of April 19, 2024, through July 11, 2024. During our audit, we met with EXIM management to provide a status of the engagement and discuss our preliminary conclusions.

See Appendix B for 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:

- GAO Government Auditing Standards, July 2018 Revision (GAO-18-568G)
- Federal Information Security Modernization Act of 2014 (Pub. L. 113-283, §2(a), 128 Stat. 3073, 3075-3078, Dec. 18, 2014)
- OMB Memorandum 23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Circular A-130, *Managing Information as a Strategic Resource*
- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Memorandum 07-18, *Ensuring New Acquisitions Include Common Security Configurations*
- OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- OMB Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*
- OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
- OMB Memorandum 06-16, *Protection of Sensitive Agency Information*
- OMB Memorandum 05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
- OMB Memorandum 13-02, *Improving Acquisition through Strategic Sourcing*
- OMB Memorandum 11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
- OMB Memorandum 14-03, *Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum 15-14, *Management and Oversight of Federal Information Technology*
- OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*
- OMB Memorandum 17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- OMB Memorandum 19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Memorandum 19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*
- OMB Memorandum 19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB FedRAMP Policy Memo, *Security Authorization of Information Systems in Cloud Computing Environments*, Dec. 8, 2011

- DHS FY 2023 - 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics
- NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
- 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 2024 EXIM FISMA performance audit, we followed up on the status of the open prior-year finding. We inquired of EXIM personnel and inspected evidence related to current-year test work to determine the status of the finding. If the recommendation was implemented, we closed the finding. If the recommendation was 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 on the Effectiveness of EXIM’s Information Security Program and Practices Report for Fiscal Year 2022 (OIG-AR-23-04, March 2, 2023)</i>			
<i>Independent Audit on the Effectiveness of EXIM’s Information Security Program and Practices Report for Fiscal Year 2023 (OIG-AR-23-06, September 18, 2023)</i>			
<u>Finding 1</u> - Identify Function: EXIM needs to update its Enterprise Risk Management Program to comply with NIST SP 800-53 Rev. 5	We recommended that the OCIO: 1) Update and implement the Enterprise Risk Management program, including applicable policies and procedures, to align with the new requirements outlined in the NIST SP 800-53, Rev. 5, <i>Security and Privacy Controls for Information Systems and Organizations</i> , dated September 2020 ¹	2022 2023	Closed

¹ NIST, <https://doi.org/10.6028/NIST.SP.800-53r5>

Appendix D: Management's Response



Helping American Businesses Win the Future

DATE: September 11, 2024

TO: Eric Rivera, Assistant Inspector General for Audit

THROUGH: Ravi Singh, Senior Vice President and Chief Financial Officer (Acting) **RAVI SINGH**
Digitally signed by RAVI SINGH
Date: 2024.09.11
13:38:31 -0400

FROM: Howard Spira, Senior Vice President and Chief Information Officer **HOWARD SPIRA**
Digitally signed by HOWARD SPIRA
Date: 2024.09.11 13:28:25
-0400

SUBJECT: EXIM Management Response to the draft report, *Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices Report for Fiscal Year 2024* (OIG-AR-24-04)

Dear Mr. Rivera,

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 Report for Fiscal Year 2024*, OIG-AR-24-04, dated September 11, 2024 (the "Report"). The OIG contracted with KPMG, LLP ("KPMG") to conduct a performance audit of EXIM's information security program and practices.

EXIM appreciates KPMG's conclusion that they "calculated the average of the *DHS FY 2024 IG FISMA Reporting Metrics* for the five Cybersecurity Functions at Level 4: Managed and Measurable and therefore found that EXIM's information security program and practices were effective, as prescribed by the DHS criteria." In addition, EXIM appreciates OIG noting that "EXIM remediated the prior-year findings and related recommendations reported in the FY 2023 FISMA performance audit."

OIG identified an opportunity for improvement in its Report. EXIM will review it further and evaluate it for any potential action.

EXIM looks forward to continuing to strengthen our working relationship with the OIG.

CC:

The Honorable Reta Jo Lewis, President and Chair of the Board of Directors
Brad Belzak, Senior Vice President and Chief Staff
Hazeen Ashby, Deputy Chief of Staff & White House Liaison
Larry Decker, Senior Advisor to the President and Chair
James Coughlan, Senior Vice President and General Counsel
Lark Grier-Hapli, Deputy General Counsel

B11 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov

Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Courtney Chung, Senior Vice President and Chief Management Officer
Tomeka Wray, Deputy Chief Management Officer
Michaela Smith, Director of Audit and Internal Controls Program/Internal Controls and Compliance

Appendix E: Security Controls Section

During the planning phase of our performance audit, we identified the NIST SP 800-53, Rev. 5 controls referenced in the *DHS FY 2023-2024 IG FISMA Reporting Metrics*. From the remaining NIST SP 800-53, Rev. 5 controls not referenced in the *DHS FY 2023-2024 IG FISMA Reporting Metrics*, we selected a nonstatistical sample of 25 controls presented in Table 4 below to test (b) (7)(E)

Table 4: Additional Security Controls and Testing Results

No.	NIST SP 800-53 Security Control	Control Name	System	Conclusion
1	AC-19	Access Control for Mobile Devices	(b) (7)(E)	No exceptions noted
2	AC-2	Account Management	(b) (7)(E)	No exceptions noted
3	AC-3	Access Enforcement	(b) (7)(E)	No exceptions noted
4	AC-7	Unsuccessful Logon Attempts	(b) (7)(E)	No exceptions noted
5	AU-1	Policy and Procedures	(b) (7)(E)	No exceptions noted
6	AU-8	Time Stamps	(b) (7)(E)	No exceptions noted
7	CA-1	Policy and Procedures	(b) (7)(E)	No exceptions noted
8	IA-1	Policy and Procedures	(b) (7)(E)	No exceptions noted
9	IR-1	Policy and Procedures	(b) (7)(E)	No exceptions noted
10	IR-2	Incident Response Training	(b) (7)(E)	No exceptions noted
11	IR-3	Incident Response Testing	(b) (7)(E)	No exceptions noted
12	PE-2	Physical Access Authorizations	(b) (7)(E)	No exceptions noted
13	PE-8	Visitor Access Records	(b) (7)(E)	No exceptions noted
14	PM-1	Information Security Program Plan	(b) (7)(E)	No exceptions noted
15	PM-12	Insider Threat Program	(b) (7)(E)	No exceptions noted
16	PM-30	Supply Chain Risk Management Strategy	(b) (7)(E)	No exceptions noted
17	PM-4	Plan of Action and Milestones Process	(b) (7)(E)	No exceptions noted
18	SR-2	Supply Chain Risk Management Plan	(b) (7)(E)	No exceptions noted
19	PS-4	Personnel Termination	(b) (7)(E)	No exceptions noted
20	RA-7	Risk Response	(b) (7)(E)	No exceptions noted
21	SC-1	Policy and Procedures	(b) (7)(E)	No exceptions noted
22	SC-2	Separation of System and User Functionality	(b) (7)(E)	No exceptions noted
23	SC-23	Session Authenticity	(b) (7)(E)	No exceptions noted
24	SI-11	Error Handling	(b) (7)(E)	No exceptions noted
25	SI-8	Spam Protection	(b) (7)(E)	No exceptions noted

Appendix F: DHS FY 2023-2024 IG FISMA Reporting Metric Results

On June 12, 2024, we provided EXIM OIG with the assessed maturity levels for each of the 20 core metrics and 17 non-core metrics outlined in the *DHS FY 2023-2024 IG FISMA Reporting Metrics*. The following tables represent each of the NIST Cybersecurity Framework Functions and FISMA Domains that were assessed to respond to the *DHS FY 2023-2024 IG FISMA Reporting Metrics*. Each of the five Cybersecurity Functions and nine FISMA Domains had specific evaluation questions that were assessed for each metric. We used the results of these assessments to derive a maturity level for each metric, Cybersecurity Function, and FISMA Domain.

Based on the results of our performance audit procedures performed, we assessed all five Cybersecurity Functions and nine FISMA Metric Domains at Level 4: Managed and Measurable. Therefore, we concluded that EXIM’s information security program and practices were effective, as prescribed by the DHS criteria.

The tables below present the derived maturity level for the Cybersecurity Functions and FISMA Domains.

Table 5: EXIM’s FY 2023-2024 IG FISMA Reporting Metric Results

Core Metric Scoring

Function 1A: Identify - Risk Management

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	5
Optimized	0

Function 1B: Identify – Supply Chain Risk Management

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0

Maturity Level	Count of Metrics
Managed and Measurable	1
Optimized	0

Function 2A: Protect - Configuration Management

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	2
Optimized	0

Function 2B: Protect – Identity and Access Management

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	1
Managed and Measurable	2
Optimized	0

Function 2C: Protect – Data Protection and Privacy

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	2
Optimized	0

Function 2D: Protect – Security Training

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	1
Optimized	0

Function 3: Detect - ISCM

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	2
Optimized	0

Function 4: Respond - Incident Response

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	1
Managed and Measurable	1
Optimized	0

Function 5: Recover - Contingency Planning

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	2
Optimized	0

Non-Core Metric Scoring

Function 1A: Identify - Risk Management

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	2
Optimized	0

Function 1B: Identify – Supply Chain Risk Management

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	1
Optimized	0

Function 2A: Protect - Configuration Management

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	3
Optimized	0

Function 2B: Protect – Identity and Access Management

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	1
Optimized	0

Function 2C: Protect – Data Protection and Privacy

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	2
Optimized	0

Function 2D: Protect – Security Training

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	2
Optimized	0

Function 3: Detect - ISCM

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	1
Optimized	0

Function 4: Respond - Incident Response

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	3
Optimized	0

Function 5: Recover - Contingency Planning

Maturity Level	Count of Metrics
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	2
Optimized	0

Calculated Average by Function

Function	Calculated Maturity Level – Core Metrics	Calculated Maturity Level – Non-Core Metrics	FY24 Assessed Value
Identify	4	4	Effective
Protect	3.88	4	Effective
Detect	4	4	Effective
Respond	3.50	4	Effective
Recover	4	4	Effective

Appendix G: System Selection Approach

We obtained a schedule of all systems from EXIM's FISMA system inventory and noted that there was a total of 40 systems listed. We sorted the FISMA system inventory to identify systems managed and hosted by EXIM and (b) (7)(E) for testing in the 2023 FISMA performance audit. We judgmentally selected a sample of one system, (b) (7)(E) (b) (7)(E) we also tested 25 NIST 800-53 controls in addition to those identified within the Metrics as detailed in Appendix E, Security Controls Selection.

ABBREVIATIONS

AICPA	American Institute of Certified Public Accountants
APS	Application Processing System
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
EXIM	Export-Import Bank of the United States
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
(b) (7)(E)	[REDACTED]
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GISRA	Government Information Security Reform Act of 2000
GSS	General Support System
HSPD	Homeland Security Presidential Directive
IG	Inspector General
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SP	Special Publication
TIC	Trusted Internet Connections

**Office of Inspector General
Export-Import Bank of the United States**
811 Vermont Avenue, NW
Washington, DC 20571
Telephone 202-565-3908
Facsimile 202-565-3988



HELP FIGHT

FRAUD, WASTE, AND ABUSE

**1- 888-OIG-EXIM
(1-888-644-3946)**

<https://eximoig.oversight.gov/contact-us>

<https://eximoig.oversight.gov/hotline>

If you fear reprisal, contact EXIM OIG's Whistleblower Protection Coordinator at

oig.whistleblower@exim.gov

For additional resources and information about whistleblower protections and unlawful retaliation, please visit [the whistleblower's resource page](#) at oversight.gov.