Office of Inspector General

OIG-AR-26-04

September 4, 2026

Independent Audit of EXIM's Information Security Program and Practices Report – FY 2026

AUDIT OF EXIM'S INFORMATION SECURITY PROGRAM AND PRACTICES – FY 2026

WHAT OIG AUDITED

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to develop, document, and implement agency-wide information security programs to protect their information and information systems, including those provided or managed by another federal agency, contractor, or source. FISMA also requires offices of inspectors general to independently assess the effectiveness of those programs.

To fulfill these responsibilities, OIG contracted with KPMG LLP (KPMG) to independently audit the effectiveness of the Export-Import Bank of the United States' (EXIM) information security program and practices. The objective of the audit was to determine whether EXIM developed and implemented an effective information security program and practices, as required by FISMA.

WHAT OIG FOUND

KPMG conducted the performance audit under a contract monitored by OIG. KPMG did not identify any findings from its testing but included one opportunity to improve the effectiveness of EXIM's information security program.

KPMG determined that EXIM's information security program and practices were effective overall based on testing of the FY 2026 Inspector General FISMA Reporting Functions. All six functions—Govern, Identify, Protect, Detect, Respond, and Recover—were assessed at Level 4: Managed and Measurable, as described by applicable Department of Homeland Security (DHS) criteria. Appendix F contains EXIM's summary results for the DHS FY 2026 IG FISMA Reporting Metrics.

As outlined in Appendix E, KPMG also tested 25 additional NIST SP 800-53, Revision 5, controls for one randomly selected system and determined that EXIM effectively designed and implemented those controls.

WHAT OIG RECOMMENDS

OIG did not issue recommendations for the FY 2026 FISMA Performance Audit.

CONTENTS

Introduction 1
Objectives, Scope, and Methodology 1
Background 1
Federal Laws, Roles, and Responsibilities 2
DHS FY 2026 IG FISMA Reporting Metrics 3
Audit Results 4
Findings 4
Opportunity for Improvement 4
Appendices 6
Appendix A: Scope and Methodology 6
Appendix B: Federal Laws, Regulations, and Guidance 8
Appendix C: Status of Prior-Year Recommendations 11
Appendix D: Management's Response 12
Appendix E: Security Controls Section 13
Appendix F: DHS FY 2026 IG FISMA Reporting Metric Results 14
Appendix G: System Selection Approach 20
Abbreviations 21
KPMG Independent Auditor's Report 22

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) 2026.

OBJECTIVES, 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, KPMG 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 Department of Homeland Security's FY 2026 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (DHS FY 2026 IG FISMA Reporting Metrics), KPMG evaluated agency and system-level security control policies, procedures, and practices associated with the following DHS FY 2026 IG FISMA Reporting Metric Domains:

- Govern – Cybersecurity Governance and Cybersecurity Supply Chain Risk Management;
- Identify – Risk and Asset 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.

KPMG selected one EXIM information system for our performance of system-level security control testing procedures: EXIM Loan Management System (ELMS).

See Appendix A for more details on the scope and methodology of our performance audit.

BACKGROUND

EXIM 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 information technology (IT) systems supporting these programs and EXIM's mission are:

1. Financial Management System – Next Generation (FMS-NG)
2. Infrastructure General Support System (GSS)
3. EXIM Online (EOL)
4. EXIM Loan Management System (ELMS)
5. Application Processing System (APS)
6. Database General Support System (GSS)

EXIM's network infrastructure consists largely of networking devices with various servers running different operating system platforms. Enterprise managed personal computers and laptops use the Windows operating system. The networks are protected from external threats by a range of IT 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, 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.

The National Institute of Standards and Technology (NIST) is tasked to work with federal agencies in the development of federal information and information systems 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 the Office of Management and Budget (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 the effectiveness of an agency's information security program. OIGs must also report their results to DHS and OMB annually through CyberScope.

DHS FY 2026 IG FISMA REPORTING METRICS

DHS created the metrics for OIGs 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 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 Cybersecurity Governance, Cybersecurity Supply Chain Risk Management, Risk and Asset Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response and Contingency Planning. Table 1, below, contains a description of the associated DHS FY 2026 IG FISMA Reporting Metric Domains.

Table 1: DHS FY 2026 IG FISMA Reporting Metric Domains

Cybersecurity Framework Security Functions	DHS FY 2026 IG FISMA Reporting Metric Domains
Govern	**Cybersecurity Governance** **Cybersecurity Supply Chain Risk Management**
Identify	**Risk and Asset Management**
Protect	**Configuration Management** **Identity and Access Management** **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 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 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 (Govern, Identify, Protect, Detect, Respond, and Recover) and the overall program. A security program is considered effective if the majority of the DHS FY 2026 IG FISMA Reporting Metrics are assessed at Level 4: Managed and Measurable. KPMG 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.

AUDIT RESULTS

Consistent with applicable FISMA requirements, OMB policy and guidance, NIST SPs, and FIPS, EXIM established and maintained its information security program and practices for its systems across the six Cybersecurity Functions and ten FISMA Metric Domains. KPMG calculated the average of the DHS FY 2026 IG FISMA Reporting Metrics for the six 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 2026 IG FISMA Reporting Metrics assessment is in Appendix F.

FINDINGS

No findings were identified during the FY 2026 FISMA performance audit.

OPPORTUNITY FOR IMPROVEMENT

Over several years, KPMG has observed improvement in EXIM's information security program and practices across all six Cybersecurity Functions (Govern, Identify, Protect, Detect, Respond, and Recover) and ten FISMA Metric Domains (Cybersecurity Governance, Cybersecurity Supply Chain Risk Management, Risk and Asset Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning). EXIM achieved Level 4: Managed and Measurable in FY 2026. During the FY 2026 FISMA performance audit, KPMG assessed two metrics at Level 3: Consistently Implemented. These metrics were (1) Metric 19 (Protect and Identity and Access Management) and (2) Metric 30 (Respond and Incident

Response). Since two program metrics were assessed below Level 4 (Managed and Measurable), KPMG identified an opportunity for improvement for management's consideration as they evaluate whether to pursue this level:

EXIM management should re-assess their logging capabilities within its information security program to meet objectives required by OMB M-26-14. OMB M-21-31, now rescinded by the issuance of M-26-14, raised logging baselines, centralized ingestion, and established retention schedules. However, some requirements, such as retention of vast quantities of logging data without clear utility, proved neither operationally feasible nor cost-effective. OMB-26-14 established a revised logging maturity model to guide and measure agency implementation. KPMG presents this opportunity for improvement because this new adaptive framework could provide EXIM management with increased detection and response capabilities to defend against threat actors who continue to evolve in scale, speed, and sophistication with the advancements of artificial intelligence.

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 focused on the information security controls, program, and practices at the agency level (entity level) and for a selected information system.

KPMG conducted the performance audit in accordance with Generally accepted government auditing standards. Those standards require that KPMG 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. In addition to generally accepted government auditing standards, KPMG conducted this performance audit in accordance with the Consulting Services Standards established by the American Institute of Certified Public Accountants.

To assess EXIM's information security controls and practices, KPMG applied procedures to test agency and system-level controls, the latter of which were associated with EXIM Loan Management System (ELMS) - the one information system KPMG selected for our performance audit. Using the evaluation guidance prescribed in the FY 2026 IG FISMA Reporting Metrics) and the methodology steps outlined below for each of the six Cybersecurity Functions and ten FISMA Metric Domains from the DHS FY 2026 IG FISMA Reporting Metrics, KPMG:

- 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 and ELMS system-level controls were suitably designed and operating effectively to address requirements associated with Level 3: Consistently Implemented maturity models for all ten FISMA Metric Domains. If, based on the results of testing performed, KPMG determined that one or more controls did not meet those requirements, KPMG assessed those controls as Level 1: Ad Hoc or Level 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 and ELMS 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 and ELMS system-level controls 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 design of the controls.

As prescribed in the DHS FY 2026 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 2026 IG FISMA Metric Results.

In addition to the procedures above, KPMG selected 25 additional NIST SP 800-53, Rev. 5, security controls that were not referenced in the DHS FY 2026 IG FISMA Reporting Metrics and developed and executed test procedures to test those controls for ELMS. See Appendix E, Security Controls Section, for a list of the controls selected for testing.

To assess the effectiveness of the information security program and practices of EXIM, KPMG 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.

KPMG relied on computer-generated data as part of performing this audit. KPMG 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. KPMG determined that the data were sufficiently reliable for testing purposes.

KPMG performed our fieldwork with EXIM management and IT personnel from April 1, 2026, through July 17, 2026. During our audit, KPMG met with EXIM management to provide engagement status updates and discuss our preliminary conclusions.

See Appendix B for the federal laws, regulations, and guidance used as criteria for the performance audit.

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:

- Government Accountability Office (GAO) Government Auditing Standards, February 2024 Revision (GAO-24-106786)
- Federal Information Security Modernization Act of 2014 (Pub. L. 113-283, §2(a), 128 Stat. 3073, 3075-3078, Dec. 18, 2014)
- OMB Memorandum 25-04, Fiscal Year 2025 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 Federal Risk and Authorization Management Program (FedRAMP) Policy Memo, Security Authorization of Information Systems in Cloud Computing Environments, Dec. 8, 2011
- OMB M-21-31 Logging Compliance
- DHS FY 2026 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics
- NIST Cybersecurity Framework (CSF) 2.0
- 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

No exceptions were identified in the prior year that resulted in the issuance of Notice of Findings and Recommendations (NFRs).

Table 3: Status of Prior Audit Recommendations

Finding	Recommendation	FY Identified	Status
N/A	**N/A**	**N/A**	**N/A**

APPENDIX D: MANAGEMENT'S RESPONSE

DATE: September 2, 2026

TO: Eric Rivera, Assistant Inspector General for Audits

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

HOWARD SPIRA Digitally signed by HOWARD SPIRA Date: 2026.09.02 13:28:05 -04'00'

SUBJECT: EXIM Management Response to the draft Report *Audit of EXIM's Information Security Program and Practices – FY 2026 (OIG-AR-26-04)*

Dear Mr. Rivera,

Thank you for providing the management of the Export-Import Bank of the United States ("EXIM" or "EXIM Bank") with the Office of Inspector General's ("OIG") draft report titled Audit of EXIM's Information Security Program and Practices – FY 2026 (OIG–AR-26-04), dated August 18, 2026 (the "Report"). The OIG contracted with KPMG, LLP ("KPMG") to conduct a performance audit of EXIM's Information Security Program and Practices Report – FY 2026.

EXIM acknowledges KPMG's conclusion that no findings were identified during the audit. While noting that EXIM's information security program and practices are well-developed and effectively implemented, EXIM appreciates the opportunity to further enhance its security posture. The Bank remains dedicated to continuous improvement in information security and looks forward to maintaining a strong, collaborative working relationship with the OIG.

CC:
The Honorable John Jovanovic, President and Chairman of the Board of Directors
Jim Burrows, Vice President and Vice Chairman, Acting
Cathryn Collins, Chief Operating Officer
Darren Death, Chief Information Security Officer
Peter Hoang, Director, Infrastructure Operations & Engineering
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Tony Onorato, Senior Vice President and General Counsel
Victoria Coleman, Deputy General Counsel
Michaela Smith, Director of Audit and Internal Controls Program

Export-Import Bank of the United States | 811 Vermont Avenue, NW | Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380
exim.gov

APPENDIX E: SECURITY CONTROLS SECTION

During the planning phase of our performance audit, KPMG identified the NIST SP 800-53, Rev. 5 controls referenced in the DHS FY 2026 IG FISMA Reporting Metrics. From the remaining NIST SP 800-53, controls not referenced in the DHS FY 2026 IG FISMA Reporting Metrics, KPMG selected a nonstatistical sample of 25 controls presented in Table 4 below to test for ELMS. KPMG performed tests of design and operating effectiveness on the following controls for the ELMS system and noted no exceptions.

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

APPENDIX F: DHS FY 2026 IG FISMA REPORTING METRIC RESULTS

On July 29, 2026, KPMG provided EXIM OIG with the assessed maturity levels for each of the 20-core metrics and 5 supplemental metrics outlined in the DHS FY 2026 IG FISMA Reporting Metrics. The following tables present each of the FISMA Metric Domains that were assessed to respond to the DHS FY 2026 IG FISMA Reporting Metrics. Each of the six Cybersecurity Functions and ten FISMA Metric Domains had specific evaluation questions that were assessed for each metric. KPMG used the results of these assessments to derive a maturity level for each metric, Cybersecurity Function, and FISMA Metric Domain.

Based on the results of our performance audit procedures, KPMG assessed all six Cybersecurity Functions and ten FISMA Metric Domains at Level 4: Managed and Measurable. Therefore, KPMG 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 Metric Domains.

Table 5: EXIM's FY 2026 IG FISMA Reporting Metric Results

Core Metric Scoring

Function 1A: Govern – Cybersecurity Governance

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

Function 1B: Govern – Cybersecurity Supply Chain Risk Management

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

Function 2: Identify – Risk and Asset Management

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

Function 3A: Protect – Configuration Management

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

Function 3B: 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 3C: 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 3D: Protect – Security Training

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

Function 4: Detect – Information Security Continuous Monitoring

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

Function 5: Respond – Incident Response

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

Function 6: Recover – Contingency Planning

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

Supplemental Metric Scoring

Function 1A: Govern – Cybersecurity Governance

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

Function 1B: Govern – Cybersecurity Supply Chain Risk Management

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

Function 2: Identify – Risk and Asset Management

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

Function 3A: Protect – Configuration Management

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

Function 3B: Protect – Identity and Access Management

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

Function 3C: Protect – Data Protection and Privacy

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

Function 3D: Protect – Security Training

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

Function 4: Detect – Information Security Continuous Monitoring

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

Function 5: Respond – Incident Response

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

Function 6: Recover – Contingency Planning

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

Calculated Average by Function

Function	Calculated Maturity Level – Core Metrics	Calculated Maturity Level – Non-Core Metrics	FY 2026 Assessed Value
Govern	**4.00**	**4.00**	**Effective**
Identify	**4.00**	**4.00**	**Effective**
Protect	**3.875**	**Not Applicable**	**Effective**

Detect	**4.00**	**4.00**	**Effective**
Respond	**3.50**	**Not Applicable**	**Effective**
Recover	**4.00**	**Not Applicable**	**Effective**

APPENDIX G: SYSTEM SELECTION APPROACH

KPMG obtained a schedule of all systems from EXIM's FISMA system inventory and noted that there was a total of 44 systems listed. KPMG sorted the FISMA system inventory to identify systems managed and hosted by EXIM and removed EOL as it was selected for testing in the FY 2025 FISMA performance audit. KPMG judgmentally selected a sample of one system, ELMS, since that system was categorized as FIPS 199 Moderate risk, maintains financially relevant data, and had never been tested against the supplemental FISMA metrics. For ELMS, KPMG also tested 25 NIST SP 800-53 controls in addition to those identified within the Metrics as detailed in Appendix E, Security Controls Section.

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
ELMS	EXIM Loan Management System
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
GISRA	Government Information Security Reform Act of 2000
GSS	General Support System
HSPD	Homeland Security Presidential Directive
IG	Inspector General
ISCM	Information Security Continuous Monitoring
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 Connection

KPMG INDEPENDENT AUDITOR'S REPORT

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 2026

Dear Mr. Rivera,

KPMG is 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 its information security program and practices were effective for fiscal year (FY) 2026, as of September 4, 2026, 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). The EXIM Office of Inspector General (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 requirements were met.

KPMG conducted this performance audit in accordance with GAGAS. Those standards require that KPMG plans and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. KPMG believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In addition to GAGAS, KPMG 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 (SPs) and Federal Information Processing Standards (FIPS).

KPMG 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, KPMG responded to the DHS FY 2026 IG FISMA Reporting Metrics and assessed the metric maturity levels on behalf of EXIM OIG. Additional details regarding the scope of our independent performance audit are included in the "Objective, Scope, and Methodology" section, Appendix A, "Scope and Methodology", and Appendix C, "Status of 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 across the six Cybersecurity Functions and ten FISMA Metric Domains.

Based on the results of our performance audit procedures, all six 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 2026 IG FISMA Reporting Metrics.

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. KPMG cautions 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,

KPMG LLP

Washington, D.C.

September 4, 2026

CONTACT US

REPORT FRAUD, WASTE, AND ABUSE

1- 888-OIG-EXIM

(1-888-644-3946)

EXIM Hotline
Office of Inspector General
811 Vermont Avenue, NW
Washington, D.C. 20571

https://eximoig.oversight.gov/hotline

CONTACT US

For general inquiries or additional information about our operations, contact us at:

202-565-3908

OIG.Info@exim.gov

Office of Inspector General
811 Vermont Avenue, NW
Washington, D.C. 20571

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.

Under The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 Pub. L. No. 117-263, § 5274, if your organization has been mentioned in this report, and you would like to provide a written response for inclusion in the report, please reach out to us at OIG.Notices@exim.gov within 30 days.