EXPORT-IMPORT BANK OF THE UNITED STATES

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 2021

February 11, 2022
OIG AR 22 04

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

The Export-Import Bank of the United States (EXIM) is the official export credit agency of the United States. EXIM is an independent, self-financing executive agency and a wholly-owned U.S. government corporation. 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 the EXIM OIG is to conduct and supervise audits, investigations, inspections, and evaluations related to agency programs and operations; provide leadership and coordination as well as recommend policies that will promote economy, efficiency, and effectiveness in such programs and operations; and prevent and detect fraud, waste, abuse, and mismanagement.

This audit was conducted in accordance with the 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 the audit objectives.

EXPORT-IMPORT BANK OF THE UNITED STATES

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 – Fiscal Year 2021

Date: February 11, 2022

This memorandum transmits 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) 2021. Under a contract monitored by this office, we engaged the independent public accounting firm of KPMG LLP (KPMG) to conduct the 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). 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 EXIM's information systems are properly managed and configured to prevent unauthorized users from gaining access and whether significant security vulnerabilities and weaknesses exist.

According to the instructions detailed within **Appendix F**, *DHS' FY 2021 IG FISMA Reporting Metrics*, KPMG determined that EXIM's information security program and practices were considered effective overall as a result of all five of the FY 2021 Inspector General FISMA Reporting Functions were scored at a Level 4: Managed and Measurable (Identify, Protect, Detect, Respond, and Recover). However, deficiencies were found within the Cybersecurity Identify Function and two FISMA Metric Domains (Risk Management and Supply Chain Risk Management) that need improvement but were not pervasive enough to affect the overall effectiveness and assessment of the program. Management concurred with the recommendations in this 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. Also, during the past year, EXIM implemented corrective actions to remediate prior-year deficiencies.

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. Additional information about EXIM OIG and the Inspector General Act of 1978, as amended, is available at www.exim.gov/about/oig.

February 11, 2022

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 2021

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) to determine whether their information security program and practices were effective for fiscal year (FY) 2021, as of February 11, 2022, 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 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* Version 1.1, dated May 12, 2021 (FY 2021 Inspector General (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 requirements[1] 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 for FY 2021 in accordance with the criteria set forth by FY 2021 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, Item 3001, dated March 22, 2021

In addition, the OIG requested that KPMG perform an independent vulnerability assessment[2] 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.

We based our independent performance audit work on a selection of EXIM-wide security controls and a selection of system-specific security controls across (b) (4) EXIM information system. As part of our audit, we responded to the DHS FY 2021 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 Functions[3] and nine FISMA Metric Domains.[4]

Based on the results of our performance audit procedures, all five 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 2021 IG FISMA Reporting Metrics*.

Also, during the past year, EXIM implemented corrective actions to remediate prior-year deficiencies related to implementation of (b) (4) , establishment of (b) (4) , and vulnerabilities and weaknesses within (b) (4) .

However, we did identify deficiencies within the Cybersecurity Identify Function area. Specifically, we noted the following:

---

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

[3] OMB, DHS, and CIGIE developed the FY 2021 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. In FY 2021, the eight IG FISMA Metric Domains were aligned with the five Cybersecurity Functions of Identify, Protect, Detect, Respond, and Recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[4] As described in the FY 2021 IG FISMA Reporting Metrics, Version 1.1, May 12, 2021, 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. Supply chain risk management is a new domain that has been introduced into the Identify Function. The supply chain risk management domain is included for informational purposes only and is not considered in the function rating for the Identify Function. However, we assessed and determined the maturity level for the supply chain risk management domain would be (b) (4) if a rating was applicable.

Cybersecurity Function: Identify

1. EXIM's use of Plan of Action and Milestones (POA&Ms) did not fully address the NIST Special Publication (SP) 800-53, Revision 4, control CA-5. Specifically, we noted that EXIM management did not (b) (4)

. (FISMA domain: Risk Management)

Cybersecurity Function: Identify

2. EXIM management did not fully address NIST SP 800-53, Revision 5, (b) (4) . Specifically, EXIM management did not (b) (4)

(FISMA domain: Supply Chain Risk Management)

KPMG considered these deficiencies when we assessed the maturity levels for the FY 2021 IG FISMA Reporting Metrics. We provided recommendations related to these two 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 11, 2022

EXECUTIVE SUMMARY

Independent Audit of EXIM's Information Security Program and Practices Effectiveness – FY 2021
OIG-AR-22-04, February 11, 2022

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

This report includes recommendations to improve the effectiveness of EXIM's information security program.

What We Found

EXIM's information security program and practices were effective overall as a result of the testing of the fiscal year (FY) 2021 Inspector General FISMA Reporting Functions, for which all (Identify, Protect, Detect, Respond, and Recover) scored a 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) 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 nine FISMA Metric Domains. However, we found deficiencies within the Cybersecurity Identify Function area and two FISMA Metric Domains (Risk Management and Supply Chain Risk Management) that need improvement but were not pervasive to affect the overall effectiveness and assessment of the program. EXIM can further strengthen its overall security program by addressing the findings and recommendations in this report including the areas identified for improvement in Appendix F.

Further, we determined that EXIM remediated the three deficiencies reported in the FY 2020 FISMA performance audit report (OIG-AR-20-04, January 13, 2020) related to implementation of (b) (4) , establishment of (b) (4) , and vulnerabilities and weaknesses within (b) (4) .

Finally, we determined that EXIM effectively designed and implemented the 16 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 outlined in Appendix E.

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

TABLE OF CONTENTS

LIST OF TABLES

ABBREVIATIONS AND GLOSSARY

AICPA	American Institute of Certified Public Accountants
APS	Application Processing System
CIGIE	Council of the Inspectors General on Integrity and Efficiency
COVID-19	Novel Coronavirus
DHS	Department of Homeland Security
EOL	EXIM Online
EXIM	Export-Import Bank of the United States
FDOnline	Financial Disclosures Online
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
(b) (4)	(b) (4)
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
OPM	Office of Personnel Management
POA&M	Plans of Action and Milestone
SIEM	Security Incident and Event Management
SP	Special Publication
TIC	Trusted Internet Connections

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) 2021. The objective was to determine whether EXIM developed and implemented effective information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).

In addition, the Office of Inspector General (OIG) requested that KPMG perform an independent vulnerability assessment[5] 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.

OBJECTIVE, SCOPE, AND METHDOLOGY

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 FY 2021. 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 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2021 IG FISMA Reporting Metrics), version 1.1, dated May 12, 2021, to evaluate EXIM's policies, procedures, and practices for Identify – Risk Management and Supply Chain Risk Management;[6] 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 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.

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

[6] The supply chain risk management domain is included for informational purposes only and is not considered in the function rating for the Identify Function. However, we assessed and determined the maturity level for the supply chain risk management domain would be (b) (4) if a rating was applicable.

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 largely of networking devices with various servers running different operating system platforms. Standard desktop personal computers and laptops use (b) (4) operating system. The networks are protected from external threats by a range of information technology security devices, including data loss prevention tools, firewalls, intrusion detection and prevention systems, antivirus, and spam-filtering systems.

Federal Laws, Roles, and Responsibilities. On December 17, 2002, the President signed into law the E-Government Act (Public Law 107-347), which included the Federal Information Security Management Act of 2002 (FISMA). 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, Revisions (Rev.) 4

[7] On December 18, 2014, FISMA was amended by the Federal Information Security Modernization Act of 2014 (Public Law 113-283). The amendment included the: (1) 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.

and 5.[8] 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 2021 IG FISMA Reporting Metrics. DHS revised the FY 2020 IG FISMA Reporting Metrics and issued the FY 2021 IG FISMA Reporting Metrics, Version 1.1 on May 12, 2021. DHS created the metrics for IGs to use in conducting their annual independent evaluations to determine the effectiveness of the information security program and practices of their respective agency. The metrics are organized around the five Cybersecurity Functions[9] outlined in the NIST Cybersecurity Framework[10] 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, Supply Chain Risk Management,[11] 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 2021 IG FISMA Metric Domains.

[8] The *FY 2021 IG FISMA Reporting Metrics,* Version 1.1, dated May 12, 2021, prescribes that *NIST SP 800-53 Rev., 5, Security and Privacy Controls for Information Systems and Organizations* is only applicable for the Supply Chain Risk Management FISMA domain for FY 2021 assessments.

[9] 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.

[10] 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.

[11] The supply chain risk management domain is included for informational purposes only and is not considered in the function rating for the Identify Function.

Table 1: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2021 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metric Domains
Identify	Risk Management Supply Chain Risk 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: Ah-Hoc, Level 2: Defined, Level 3: Consistently Implemented, Level 4: Managed and Measurable, and Level 5: Optimized. The maturity level for a domain is determined by a simple majority, with the most frequently assessed level across the questions serving as the domain rating. For example, a security program is considered effective if the majority of the FY 2021 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 nine FISMA Metric Domains. During the past year, EXIM implemented corrective actions to remediate prior-year deficiencies related to implementation of (b) (4) , establishment of (b) (4) , and vulnerabilities and weaknesses within (b) (4) . We found the program was effective as a result of a majority of FY 2021 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 the Cybersecurity Identify Function and within the Risk Management and Supply Chain Risk Management FISMA Metric Domains. These deficiencies were aligned to metrics 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 2021 IG FISMA Reporting Metric assessment is in **Appendix F.**

As noted above, we evaluated the open prior-year findings from the FY 2020 FISMA performance audit and noted management took sufficient action to address the three deficiency conditions identified and related six recommendations. 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: Weakness in Risk Management Plan of Action and Milestones

During FY 2021, we noted that EXIM's use of POA&Ms did not fully address the NIST SP 800-53, Revision 4, control CA-5. Specifically, we noted that EXIM management did not (b) (4)

.

The following guidance is relevant to this deficiency:

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

> CA-5: Plan of Action and Milestones
> The organization:
> a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the

assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Independent Auditors' Recommendations:

In the *Fiscal Year 2021 Financial Statements Audit Management Letter* (OIG-AR-22-03, November 12, 2021), we made two recommendations to address weaknesses in the risk management of POA&Ms: (1) define (b) (4) , and (2) ensure (b) (4)
In its management response, EXIM agreed to (b) (4) to address the condition and recommendations. Finding 1 of this report as it relates to FISMA supports similar recommendations. Therefore, management's actions to address the condition and two recommendations will be responsive to the financial statements audit management letter and this performance audit report.

Management's Response and Evaluation Thereof:

Please see *Independent Auditors' Recommendations section* above.

Finding 2: Identify Function: Weakness in (b) (4)

During FY 2021, we noted that EXIM management did not fully address the NIST SP 800-53, Rev. 5, (b) (4) Specifically, EXIM management did not (b) (4)
.

The following guidance is relevant to this deficiency:

(b) (4)

We recommend that the Office of the Chief Information Officer (OCIO):

1. Formally design and implement (b) (4)
.

Management's Response:

EXIM management concurred with the finding. As part of the ongoing transition to NIST SP 800-53, Rev. 5, EXIM management will design and implement (b) (4) in FY 2022.

Evaluation of Management's Response:

If implemented properly, we believe the process EXIM management defined above for remediating this issue will help ensure compliance with (b) (4)
outlined in NIST SP 800-53, Rev. 5.

CONCLUSION

Based on our testing of the FY 2021 IG FISMA Reporting Metrics and the associated scoring guidance, all five Cybersecurity Functions and the majority of the nine 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 2021.

We determined that EXIM remediated all three of the prior year deficiencies and related recommendations reported in the FY 2020 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 nine FISMA Metric Domains to consistently evaluate and improve the effectiveness of its information security program.

In addition, EXIM should implement corrective actions to strengthen its risk management processes and procedures over POA&M management and (b) (4) process and procedures related to (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 (b) (4) . In addition, at the request of EXIM 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 2021 Inspector General Information Security Modernization Act of 2014 Reporting Metrics* (FY 2021 IG FISMA Reporting Metrics), we performed test procedures at the Agency level (entity level) and for the selected information systems. Our methodology for determining the maturity levels for each of the five Cybersecurity Functions and nine FISMA Metric Domains from the FY 2021 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 nine 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 and (b) (4) for the maturity level 4 questions within the nine 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 and (b) (4) for the maturity level 5 questions within the nine FISMA Metric Domains. The test procedures evaluated the design of the controls.

As prescribed in the FY 2021 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 2021 IG FISMA Metric Results.*

In addition to the procedures above, we selected 16 additional NIST SP 800-53, Rev. 4, security controls that were not referenced in the FY 2021 IG FISMA Reporting Metrics and developed and executed test procedures for these control for(b) (4) .[12] 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.

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 reporting purposes.

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 July 21, 2021, through September 30, 2021. 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.

[12] In addition to evaluating EXIM's maturity levels for the FY 2020 IG FISMA Reporting Metrics, Contract No. GS-00F-275CA, Task Order 83310118F0016, Item 3001, effective March 22, 2021, required us to test additional NIST 800-53 controls for(b) (4) .

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:

- Generally Accepted Government Auditing Standards (GAGAS)
- Federal Information Security Modernization Act of 2014 (Public Law 113-283, §2(a), 128 Stat. 3073, 3075-3078 [2014])
- Office of Management and Budget (OMB) Memorandum 21-02, Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Requirements
- OMB Circular A-130, Management of Federal Information Resources.
- 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 Common 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, December 8, 2011
- FY 2021 IG Federal Information Security Modernization Act of 2014 Reporting Metrics

- NIST SP 800-53, Revision (Rev.) 4, Security and Privacy Controls for Federal Information Systems and organizations
- NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and organizations
- NIST SP 800-53A, Rev. 1, Guide for Assessing Security Controls for Federal Information systems and Organizations
- NIST SP 800-30, Managing Information Security Risk
- NIST SP 800-34, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37, Rev. 1, Guide for Applying the Risk Management Framework to Federal information Systems
- NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-137, Rev. 1, Information Security Continuous Monitoring for Federal information Systems and Organizations
- Federal Information Processing Standards (FIPS) 199: Standards for Security categorization of Federal Information and Information Systems
- FIPS 200: Minimum Security Requirements for Federal Information and Information systems

Appendix C: Status of Prior-Year Recommendations

As part of the FY 2021 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
Independent Audit of EXIM's Information Security Program and Practices Effectiveness for FY 2020 (OIG-AR-21-03, February 4, 2021)			
Finding 1 - Identify Function: Deficiency in the implementation of (b) (4)	We recommended that the OCIO: 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) .	2020	Closed
Finding 2 - Detect Function: (b) (4) was not fully established.	We recommended that the OCIO: 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 procedure for (b) (4) and ensure operational effectiveness and compliance.	2018	Closed

Finding	Recommendation	FY Identified	Status
Finding 3 - Protect Function: (b) (4) vulnerabilities and weaknesses (b) (4) were identified	We recommended that the OCIO: 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)	2020	Closed

Appendix D: Management's Response

EXIM
EXPORT-IMPORT BANK
OF THE UNITED STATES

Reducing Risk. Unleashing Opportunity.

DATE: February 04, 2022

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: 2022.02.04 15:32:34 -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 2021 (OIG-AR-22-04)

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 2021*, OIG-AR-22-04, dated January 05, 2022 (the "Report"). The OIG contracted with KPMG, LLP ("KPMG") to conduct a performance audit of EXIM's information security program and practices. 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.

EXIM appreciates KPMG recognizing that consistent with applicable FISMA requirements, and OMB policy and guidance, that EXIM has maintained an effective information security program and practices for its systems.

In addition, EXIM appreciates that OIG noted that EXIM "remediated the three deficiencies reported in the FY 2020 FISMA performance audit related to implementation of an automated risk management tool, establishment of an Information Security Continuous Monitoring program, and vulnerabilities and weaknesses within the patch management program." Further, OIG recognized that "EXIM effectively designed and implemented the 16 additional NIST Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, controls that [were] tested for a randomly selected system outlined in Appendix E."

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 our continuous strengthening of our working relationship and working closely with the Office of the Inspector General.

1

Reducing Risk. Unleashing Opportunity.

CC:

Howard Spira, SVP and Chief Information Officer
Christopher Sutton, Chief Information Systems Officer
Kenneth Tinsley, SVP and Chief Risk Officer
Jonathan Feigelson, SVP and General Counsel
Inci Tonguch-Murray, SVP and Deputy Chief Financial Officer

2

Appendix E: Security Controls Section

During planning, we identified the NIST SP 800-53, Rev. 4 controls referenced in the FY 2021 IG FISMA Reporting Metrics. From the remaining NIST SP 800-53, Rev. 4 controls not referenced in the FY 2021 IG FISMA Reporting Metrics, we selected a nonstatistical sample of 16 controls presented in Table 4 below to test for (b) (4) .

Table 4: Additional Security Controls and Testing Results

No.	NIST SP 800 53 Security Control	Control Name	System	Conclusion
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
14	AC-1	Access Control Policy and Procedures	(b) (4)	No exceptions noted
15	AC-5	Separation of Duties	(b) (4)	No exceptions noted
16	CM-5	Access Restrictions for Change	(b) (4)	No exceptions noted

Appendix F: DHS FY 2021 IG FISMA Metric Results

On October 20, 2021, we provided EXIM OIG with the assessed maturity levels for each of the 57 metrics outlined in the FY IG 2021 FISMA Reporting Metrics. The following tables represent each of the NIST Cybersecurity Framework Functions and FISMA Domains that were assessed to respond to the FY 2021 IG FISMA Reporting Metrics. Each of the five Cybersecurity Functions and nine FISMA Domains had specific evaluation questions that were assessed, for each metric, which derived a maturity level for each metric, Cybersecurity Function, and FISMA Domain.

Based on the results of our performance audit procedures, the majority of EXIM's Cybersecurity Functions and FISMA Domains scored at a Level 4: Managed and Measurable, therefore, the information security program was considered effective.

However, we did identify deficiencies within the Cybersecurity Identify Function area, Risk Management and Supply Chain Risk Management FISMA Domains (See **Findings 1 and 2** in the ***Findings*** section above.

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

Table 5: EXIM's FY 2021 IG FISMA Metric Results

Function 1A: Identify - Risk Management

Maturity Level	Count
Ad-hoc	0
Defined	1
Consistently Implemented	1
Managed and Measurable	8
Optimized	0
Function Rating:	Managed and Measurable (Level 4)

Function 1B: Identify – Supply Chain Risk Management

Maturity Level	Count
Ad-hoc	(b) (4)
Defined	(b) (4)
Consistently Implemented	(b) (4)
Managed and Measurable	(b) (4)
Optimized	(b) (4)
Function Rating:	Not applicable per FY 2021 IG Reporting Metrics Supply Chain Risk Management is not to be

Maturity Level	Count
	considered in the Identity framework function rating. However, the maturity level for the Supply Chain Risk Management Function would be assessed at (b) (4) if rating was applicable.

Function 2A: Protect - Configuration Management

Maturity Level	Count
Ad-hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	8
Optimized	0
Function Rating:	Managed and Measurable (Level 4)

Function 2B: Protect - Identity and Access 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 2C: Protect – Data Protection and Privacy

Maturity Level	Count
Ad-hoc	0
Defined	0
Consistently Implemented	0

Maturity Level	Count
Managed and Measurable	5
Optimized	0
Function Rating:	Managed and Measurable (Level 4)

Function 2D: Protect – Security Training

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

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

Maturity Level	Count
Ad-hoc	0
Defined	0
Consistently Implemented	0

Maturity Level	Count
Managed and Measurable	7
Optimized	0
Function Rating:	Managed and Measurable (Level 4)

Function 5: Recover - Contingency Planning

Maturity Level	Count
Ad-hoc	0
Defined	0
Consistently Implemented	1
Managed and Measurable	5
Optimized	0
Function Rating:	Managed and Measurable (Level 4)

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation	Function Maturity Level
Function 1A: 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.	Identify: Managed and Measurable (Level 4)
Function 1B: Protect – Supply Chain Risk Management	Not Applicable	Not Applicable	Not applicable per FY 2021 IG Reporting Metrics Supply Chain Risk Management is not to be considered in the Identity framework function rating. However, the maturity level for the Supply Chain Risk Management Function would be assessed at Consistently Implemented (Level 3) if rating was applicable.	
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.	Protect: Managed and Measurable (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	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	We assessed EXIM's information security program and practices for Data Protection and Privacy at the Managed and Measurable maturity level 4.	
Function 2D: Protect – Security Training	Managed and 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	Calculated Maturity Level	Assessed Maturity Level	Explanation	Function Maturity Level
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.	Detect: Managed and Measurable (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.	Respond: Managed and Measurable (Level 4)
Function 5: Recover - Contingency Planning	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	We assessed EXIM's information security program and practices for Contingency Planning at the Managed and Measurable maturity level 4.	Recover: Managed and Measurable (Level 4)
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 nine FISMA program areas. Although we noted deficiencies impacting specific questions within the risk management and supply chain risk management metric domains, we determined its information security program was effective as we evaluated the majority of the FY 2021 IG FISMA Reporting Metrics at the Managed and Measurable (Level 4) or higher maturity levels.	Not applicable

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 (b) (4) systems listed. We sorted the FISMA system inventory to identify systems managed and hosted by EXIM and removed (b) (4) as they were selected for testing in the 2018, 2019, and 2020 FISMA performance audits. We selected a nonstatistical sample of (b) (4) , since it was categorized as FIPS 199 Moderate risk and maintains financially relevant data and was recently migrated to a new cloud service provider in FY 2020. For (b) (4) , we also tested 16 additional NIST 800-53 controls detailed in **Appendix E**, *Security Controls Selection*.

In summary, we selected the following as the representative subset of systems to test for the FY 2021 EXIM FISMA performance audit:

- (b) (4)
- (b) (4)

.

Appendix H: Distribution List

James Burrows, Jr., Acting President and Chair of EXIM Board of Directors
James Cruse, Acting First Vice President and Vice Chairman
Hazeen Ashby, Deputy Chief of Staff and SVP, Office of Congressional and Intergovernmental Affairs
Adam Martinez, Senior Vice President and Chief Management Officer
Madolyn Phillips, Deputy Chief Banking Officer
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Mary Jean Buhler, Chief Financial Officer
Jonathan Feigelson, General Counsel
Christopher Sutton, Chief Information Security Officer
Inci Tonguch-Murray, Senior Vice President and Deputy Chief Financial Officer
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
http://www.exim.gov/about/oig