EXPORT-IMPORT BANK OF THE UNITED STATES

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

Audit of EXIM's Cybersecurity Program

July 12, 2021
OIG-AR-21-05

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

The Office of Inspector General (OIG), an independent office within EXIM, was statutorily created in 2002 and organized in 2007. The mission of EXIM OIG is to conduct and supervise audits, investigations, inspections, and evaluations related to the Agency's programs and operations; provide leadership and coordination as well as recommend policies that will promote economy, efficiency, and effectiveness in such programs and operations; and prevent and detect fraud, waste, abuse, and mismanagement.

This audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

To: Howard Spira
Senior Vice President and Chief Information Officer

From: Jennifer Fain
Acting Inspector General

Subject: Audit of EXIM's Cybersecurity Program

Date: July 12, 2021

Attached is the final report on the audit of EXIM's cybersecurity program. The objective of this audit was to assess the effectiveness of the EXIM's cybersecurity program and its implementation, including compliance with federal laws, regulations, EXIM policies and procedures, and documented baseline security configurations.

This report contains three recommendations to improve the effectiveness of EXIM's cybersecurity program. EXIM management concurred with all three recommendations (see Appendix B). We consider management's proposed actions to be responsive. The recommendations will be closed upon completion and verification of the proposed actions.

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

EXECUTIVE SUMMARY

Audit of EXIM's Cybersecurity Program
OIG-AR-21-05 July 12, 2021

Why We Did This Audit

In order to protect federal agencies of the United States (U.S.) data, information, and ensure continuity of operations, leaders throughout organizations must take steps to manage risks relating to information systems. EXIM's enterprise-wide information security and privacy program protects the Agency against potential information technology (IT) threats and vulnerabilities. The cybersecurity program ensures compliance with federal mandates and legislation, including the Federal Information Security Modernization Act of 2002 (FISMA) and U.S. cybersecurity strategy.

We initiated this audit as part of our annual work plan. The objective of this audit was to assess the effectiveness of EXIM's cybersecurity program and its implementation, including compliance with federal laws, regulations, EXIM policies and procedures, and documented baseline security configurations.

What We Recommend

To improve the effectiveness of the cybersecurity program, we made three recommendations:

1. Initiate coordination with responsible agencies to develop and document an alternative methodology for (b) (4) ;
2. Update policies to ensure that pertinent system documentation is recorded and readily accessible, and systems are (b) (4) ; and
3. Implement an automated tracking mechanism designated to create, review, and maintain specialized security training records for all employees and contractors.

What We Found

EXIM's cybersecurity program was generally operating effectively and in compliance with the Agency's policies and procedures and federal guidelines. However, some EXIM systems were operating with expired authorizations and did not actively maintain training records per federally recommended guidelines. Specifically, EXIM needs to improve their (1) processes for (b) (4) and (2) process for monitoring compliance and effectiveness of specialized training for cybersecurity staff.

At the time of the audit, there were (b) (4) information systems supporting the operations of the Agency. We analyzed the requisite Authorities to Operate (ATO) and found that multiple systems had (b) (4) and one system did not have an ATO. Operating systems without federally mandated ATOs leaves the systems and the data they contain susceptible to unknown internal and external threats. Additionally, operating systems (b) (4) may leave officials unaware of risks associated with the systems and their operation.

Employees with cybersecurity responsibilities are required to take a Security Awareness training facilitated by EXIM in addition to any specialized training related to their role. We analyzed training records and found that while the employees had completed both the internal training and required specialized training, related training records were not monitored and maintained in accordance with recommended guidelines.

While we identified the aforementioned items through our assessment, in both instances EXIM was already aware of the deficiencies and had begun remediation activities to ensure compliance in the near future.

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

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

This audit report presents the results of our audit of the Export Import Bank of the United States' (EXIM or the Agency) cybersecurity program. The objective of this audit was to assess the effectiveness of EXIM's cybersecurity program and its implementation, including compliance with federal laws, regulations, the Agency's policies and procedures, and documented baseline security configurations. This is the first audit of EXIM's cybersecurity program.

As part of the FY 2020 FISMA audit, we contracted with an independent accounting firm to perform an independent vulnerability assessment over select EXIM systems. The findings and two recommendations are included in Finding 3 of the related report (OIG-AR-21-03, February 4, 2021).

SCOPE AND METHODOLOGY

To accomplish the audit objective, we reviewed federal laws, regulations, and guidance, as well as EXIM's policies, procedures, and guidelines applicable to the Agency's cybersecurity program. We interviewed EXIM officials to gain an understanding of the cybersecurity program, its implementation, and its path forward. Through collaboration with the independent public accounting firm, KPMG, we also conducted a vulnerability scan of EXIM's systems to assess compliance with applicable agency policies and procedures and federal laws.

We assessed the significance of internal controls necessary to satisfy the audit objective. In particular, we identified and assessed three internal control components (control activities, information and communication, and monitoring) and their underlying principles.[1] However, because our review was limited to these internal control components and their underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit. See appendix A for more details.

We conducted this performance audit from April 2020 through May 2021 at EXIM headquarters in Washington, D.C. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

BACKGROUND

In today's workplace, United States (U.S.) federal agencies are reliant upon information technology (IT) systems, and their correlating data to carry out operations and to obtain, develop, sustain, and report essential agency-specific information. These IT systems are technologically varied, adaptable and can be located throughout the U.S. and abroad. The Cybersecurity and Infrastructure Security Agency, located within the Department of Homeland Security, defines cybersecurity as "the art of protecting networks, devices, and

[1] GAO-14-740G (Sept. 2014).

data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." A primary purpose for a federal cybersecurity program is protecting the U.S. federal government's information and data. Additionally, this program should thwart attacks from cybercriminals while simultaneously ensuring compliance with federal statutes. Due to the complexity of these systems, it is vital to limit serious IT threats to minimize the risk of a cyberattack.

The number of cybersecurity incidents at federal agencies have increased per year, including in fiscal year (FY) 2020 where there was a new high of 30,819 cyber incidents, reaffirming the significance of sufficient cybersecurity protections.[2] To protect against cyber threats, agencies must make decisions that will secure their systems and data. The *Federal Information Security Modernization Act of 2014* (FISMA) [3] as well as National Institute of Standards and Technology (NIST) provide instructions and a framework for managing cybersecurity risks at the agency, business, and system levels. Specifically, FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. NIST is responsible for developing standards and guidelines for federal information systems, in coordination with the Office of Management and Budget (OMB) and other federal agencies. OMB is responsible for overseeing federal agencies' information security and privacy practices and for developing and directing implementation of policies and guidelines which support and sustain those practices. Intrusion detection and prevention capabilities, along with policy guidelines, is information contained within the FISMA reports. These reports are submitted by the executive agencies within the U.S. government on an annual basis.

Furthermore, Executive Order (EO) 13800, issued in May 2017, states that "agency heads will be held accountable … for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data."[4] As a result, there are specific actions agencies and OMB must take in order to evaluate and improve cybersecurity risk management across the executive branch. In order to protect the federal agencies of the U.S. data and information, and ensure continuity of operations, leaders throughout organizations must take steps to manage risks relating to information systems.

EXIM's Cybersecurity Program

EXIM's enterprise-wide information security and privacy program protects EXIM against potential IT threats and vulnerabilities. The cybersecurity program ensures compliance with federal mandates and legislation, including FISMA and the U.S. cybersecurity strategy. EXIM's cybersecurity program plays an important role in protecting the Agency's ability to provide mission-critical operations. The core functions of the cybersecurity program include cybersecurity operations, cybersecurity architecture and engineering, and

[2] Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report to Congres, Fiscal Year 2020* (May 2021).

[3] Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).

[4] Exec. Order No. 13800, 82 FR 22391 (May 11, 2017).

cybersecurity policy and audit management. The program's top priorities include addressing the Cybersecurity Advanced Persistent Threat (APT); Information Security Continuous Monitoring (ISCM); Identity, Credential, and Access Management (ICAM); Insider Threat Prevention and Detection; Security Architecture; and Supply Chain Management. As of FY 2020, EXIM's IT Cyber Portfolio had a budget of (b) (4) , with (b) (4)

AUDIT RESULTS

EXIM's cybersecurity program was generally effective in its implementation, including compliance with federal laws, regulations, EXIM policies and procedures, and documented baseline security configurations. However, we found that (1) EXIM's processes for (b) (4) needs improvement and (2) EXIM's process for monitoring compliance and effectiveness of specialized training for cybersecurity staff can be improved. Based on these results, we made three recommendations to improve the effectiveness of EXIM's cybersecurity program.

Finding 1: EXIM's Processes for (b) (4) Needs Improvement

At the time of the audit, there were (b) (4) supporting the operations of the Agency. EXIM maintains (b) (4) that contains (b) (4) . Through assessment of these documents, we found that one of the systems was operating without a federally mandated Authorization to Operate (ATO), and 11 systems had (b) (4) .

System in Operation without Authorization to Operate

An EXIM system used for managing critical events, was operating without an ATO from its procurement in FY 2016 through December 2020. An ATO is "[t]he official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed upon set of security controls."[5]

EXIM's Chief Information Security Officer (CISO) was informed in January 2020 of the issues that needed to be addressed within (b) (4) , and the system was identified through that activity as lacking an ATO. An initial ATO package developed in February 2020 was reviewed by the CISO. However, upon reviewing the package, the CISO requested that additional assessment activities be conducted. The additional assessment caused further delays in the completion of the ATO. As a result, the system did not receive an ATO memorandum until December 2020.

[5] NIST Special Publication (SP) 800-53, Revision 4 (Rev. 4).

Systems in Operation with (b) (4)

Eleven systems were operating under (b) (4) ((b) (4)). (b) (4) As such, (b) (4) determines whether (b) (4) and whether (b) (4) . Although EXIM uses these systems, they are hosted and operated by other federal agencies.[6] To properly complete (b) (4) EXIM requests (b) (4)

. After reviewing the documentation and attestations (b) (4) , the (b) (4) is reviewed and signed by EXIM's Chief Information Officer, CISO, and the designated system owner. Table 2 in Appendix C provides details on the 11 systems.

The (b) (4) the 11 federally hosted systems (b) (4) . (b) (4)

According to EXIM management, personnel responsible for (b) (4) were unable (b) (4)

. There is no definitive timeline for the completion of (b) (4) , as the completion is dependent upon (b) (4) .

Requirements for (b) (4)

(b) (4)

(b) (4)

(b) (4)

[6] As the hosting agencies, the responsibility of (b) (4) lies with (b) (4)

The operation of a system that operated for over four years despite its lack of authorization demonstrates that EXIM was not in compliance with the federal mandates. During our audit, we found that EXIM identified the lack of an ATO for the system and almost immediately began the authorization process. We attribute the delay in authorizing the system to earlier decisions to rely on: (1) the reviews and authorizations of other agencies; (2) the federal government's standardized process for security assessment, authorization, and continuous monitoring process for cloud products; and (3) resource constraints within EXIM.

For the 11 systems in operation (b) (4) , EXIM should remain aware of (b) (4)

Although EXIM does not hold responsibility for (b) (4) , there is an obligation for (b) (4) .

Cybersecurity posture refers to an organization's overall defense against cyber-attacks. It is the collective security status of all software and hardware, services, networks, and information, and how secure you are as a result of those tools and processes. Without an effective process to ensure compliance for all systems holding EXIM data and information with information security regulations, EXIM's cybersecurity program and its ability to defend against cyber-attacks is potentially more exposed.

EXIM's operation of systems (b) (4) leaves the Agency's systems and data vulnerable to internal and external risks and threats. Additionally, operating systems (b) (4) may leave officials unaware of risks associated with the systems and their operation.

RECOMMENDATION

To improve the cybersecurity program's compliance with federal requirements for systems to be authorized prior to storing or maintaining data, we recommend that EXIM:

1. Initiate coordination with responsible agencies to develop and document an alternative methodology for (b) (4) .

   Management Comments:

   Management agrees with this recommendation. EXIM will coordinate with responsible agencies to develop and document an alternative methodology for (b) (4) .

   OIG Response:

   Management's proposed actions are responsive to the recommendation. Therefore, the recommendation is considered resolved and will be closed upon completion and verification of the proposed actions.

2. Update policies to ensure that pertinent system documentation is recorded and readily accessible, and systems are (b) (4) .

Management Comments:

Management agrees with this recommendation. EXIM will update policies to ensure that pertinent system documentation is recorded and readily accessible, and systems are (b) (4)

.

OIG Response:

Management's proposed actions are responsive to the recommendation. Therefore, the recommendation is considered resolved and will be closed upon completion and verification of the proposed actions.

Finding 2: EXIM's Process for Monitoring Compliance and effectiveness of Specialized Training for Cybersecurity Staff Can be Improved

EXIM provided evidence that all staff with cybersecurity responsibilities completed security awareness training (SAT) and received required specialized training during the period of review. However, EXIM did not have an automated tracking system to monitor training completed by IT staff with cybersecurity responsibilities in accordance with NIST guidance. Specifically, the training records were provided via (b) (4)

.

Training Completion Not Monitored/Maintained in Accordance with Recommended Guidelines

EXIM policies and procedures require training records to be collected, maintained, and made available upon request for compliance reviews and audits. NIST guidance recommends that organizations put in place processes to monitor the compliance and effectiveness of their information security training program; this includes utilizing an automated tracking system designed to capture key information on program activity. Capturing this information is useful for identifying skill gaps and making updates or changes to the program.

In response to our request for training records/evidence/certificates, the cybersecurity team provided records, including a schedule documenting the completion of SAT by all Agency staff, and documentation to support the completion of system owner training and other required cybersecurity trainings. At that time, the records were not retained within an automated tracking tool, but instead were maintained in a variety of formats.

NIST 800-50, *Building an Information Technology Security Awareness and Training Program*, requires that once a program has been implemented, processes be put into place to monitor compliance and effectiveness. We found that EXIM's cybersecurity program records were not maintained in a way that allowed regular or simplified monitoring for compliance and effectiveness for specialized training.

EXIM's internal policy requires records of completion of training for participation in an appropriate training opportunity that meets the annual minimum training requirement

must be provided by all staff. The policy also requires that all records of specialized training be submitted to the Cybersecurity Team in a timely manner, and that these records will be stored and made available for compliance reviews and audits. We found that the training records submitted by EXIM staff were maintained in a variety of formats and locations which seemingly limited EXIM's ability to readily access them when requested by the OIG for this audit.

Without an effective process for monitoring compliance with specialized IT training, users may not have completed the specialized IT security training required to maintain access to EXIM's systems, and therefore, increasing the risk to systems and data. Further, with cybersecurity risks continually evolving and increasing at a rapid pace it is essential that specialized training for IT staff is up to date and monitored effectively.

RECOMMENDATION

To improve the cybersecurity program's ability to effectively track and maintain specialized training records, we recommend that EXIM:

3. Implement an automated tracking mechanism designated to create, review, and maintain specialized security training records for all employees and contractors.

   Management Comments:

   Management agrees with this recommendation. EXIM will implement an automated tracking mechanism designated to create, review, and maintain specialized security training records for all employees and contractors.

   OIG Response:

   Management's proposed actions are responsive to the recommendation. Therefore, the recommendation is considered resolved and will be closed upon completion and verification of the proposed actions.

CONCLUSION

Through our audit, we found that EXIM's cybersecurity program was generally operating effectively and in compliance with EXIM policies and federal guidelines. While our audit did identify areas for improvement related to the maintenance of training records and (b) (4) , in both instances EXIM had already identified the deficiencies and was working to address them. To assist the cybersecurity program in its effectiveness, we made three recommendations that address the areas identified for improvement.

APPENDICES

Appendix A: Objective, Scope, and Methodology

The objective of this audit was to assess the effectiveness of EXIM's cybersecurity program and its implementation, including compliance with federal laws, regulations, EXIM policies and procedures, and documented baseline security configurations. To accomplish the audit objective, we employed a combination of qualitative and quantitative techniques, including documentation reviews.

1. Researched and assessed laws, regulations, guidelines, policies, and procedures applicable to EXIM's cybersecurity program.
    - The Federal Information Security Modernization Act of 2014
    - OMB Circular A-130, *Managing Information as a Strategic Resource*
    - Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
    - NIST Special Publication (SP) 800-37, *Risk Management for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy*, Revision 2 (Rev. 2)
    - NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
    - NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, (Rev. 4)
    - NIST 800-100, *Information Security Handbook: A Guide for Managers*
    - DHS Continuous Monitoring Program
    - EXIM RIM-2012-02, *Records Management Program Policy*
    - EXIM 09-001-02, *Securing Sensitive Export-Import Bank Information and Systems*
    - EXIM 09-001-01, *Rules of Behavior (ROB) for Users of EXIM Information Systems*
    - EXIM 10-002-12, *Policy for Monitoring of Data Privacy Protection*
    - EXIM 2018-OCIO-XXXX, *Information Security Incident Handling Policy*
    - EXIM 2020-OCIO-XXXX, *Remote Access Guidelines*
    - EXIM NN-2010-##, *IT Security and Privacy Training Policy*
    - EXIM 09-002-11, *Policy* for Review of *Holdings of Personally Identifiable Information and Social Security Numbers*
    - EXIM Vulnerability Scanning, Testing, and Assessment Policy
    - Cyber Risk Escalation and Acceptance Process Guide

- Attachment D., *Procedures for Tracking and Reporting of IT Security and Privacy Training*

2. Interviewed EXIM management and staff in the Office of Information Management and Technology and additional staff with program responsibilities to gain an understanding of the cybersecurity program.
3. Engaged an independent contractor to conduct a vulnerability assessment of the five major IT systems and their identified high-risk subsystems.
4. Reviewed cybersecurity program plans/policies/procedures for adherence with prescribed internal/external criteria.

We relied in part, on cybersecurity program data from systems provided by EXIM staff. We assessed the reliability of the data by manually checking it against available source documents. We resolved inconsistencies identified with EXIM staff and determined that the data was sufficiently reliable for our reporting purposes.

In planning and performing the audit, we obtained an understanding of internal controls to the extent necessary to satisfy the audit objective. We assessed the five internal control components and identified the following internal control components and underlying principles significant to the audit objective:[7]

Table 1: Internal Control Components	
Components	**Underlying Principles**
Control Activities	11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.
Information & Communication	13. Management should use quality information to achieve the entity's objectives. 15. Management should externally communicate the necessary quality information to achieve the entity's objectives.
Monitoring	16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. 17. Management should remediate identified internal control deficiencies on a timely basis.

We performed our audit work from April 2020 through May 2021 at EXIM headquarters in Washington, D.C. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the

[7] *Supra* note 1. The federal internal control standards are organized into five components (control environment, risk assessment, control activities, information and communication, and monitoring) and 17 related principles (requirements).

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 objective.

Appendix B: Management Comments

EXIM
EXPORT-IMPORT BANK OF THE UNITED STATES

Reducing Risk. Unleashing Opportunity.

DATE: July 9, 2021

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

THROUGH: Mary Jean Buhler, SVP & Chief Financial Officer

FROM: Adam Martinez, Chief Management Officer

SUBJECT: EXIM Management Response to the OIG Audit of EXIM's Cybersecurity Program

---

Thank you for providing the Export-Import Bank of the United States ("EXIM Bank" or "the Bank") management with the Office of the Inspector General's ("OIG") Audit of EXIM's Cybersecurity Program, OIG-AR-21-05, dated May 26, 2021.

EXIM appreciates the work conducted by the OIG staff in evaluating EXIM's Cybersecurity Program. Management continues to support the OIG's work which complements EXIM's efforts to continually improve its processes.

This audit resulted in 3 recommendations that EXIM will work to implement. We agree with the proposed recommendations and we thank the OIG for your efforts to ensure EXIM's policies and procedures continue to improve, as well as the work you do with us to protect EXIM funds from fraud, waste, and abuse. We look forward to strengthening our working relationship and continuing to work closely with the Office of the Inspector General.

CC: Hazeen Ashby, SVP, Office of Congressional and Intergovernmental Affairs
Howard Spira, Chief Information Officer
Christopher Sutton, Chief Information Security Officer
Henry Pitney, SVP and General Counsel (acting)
Inci Tonguch-Murray, Deputy Chief Financial Officer
Cris Dieguez, Director, Internal Controls and Compliance

Appendix C: (b) (4)

Table 2: Systems with (b) (4)

(b) (4)

Appendix D: Distribution List

James Cruse, First Vice President and Vice Chairman (Acting)
Adam Martinez, Chief Management Officer
Madolyn Phillips, Deputy Chief Banking Officer
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Christopher Sutton, Chief Information Security Officer
Mary Jean Buhler, Chief Financial Officer
Inci Tonguch-Murray, Senior Vice President and Deputy Chief Financial Officer
Henry Pitney, Senior Vice President and General Counsel (Acting)
Jennifer Clark, Attorney-Adviser
Cristopolis Dieguez, Director, Internal Controls and Compliance
Courtney Potter, Deputy AIG for Audits and Evaluations, OIG
Jaquone Miller, Program Manager, OIG
Amanda Myers, Senior Counsel OIG

ACKNOWLEDGEMENTS

This report was prepared by the Office of Audits and Evaluations, Office of Inspector General for EXIM. Several individuals contributed to this report including Leah Garrison-Elder, Jahnae McCoy, Jaquone Miller, Courtney Potter, and Jennifer Fain.

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