EXPORT-IMPORT BANK OF THE UNITED STATES

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

SEMIANNUAL
REPORT TO CONGRESS
October 1, 2020 to March 31, 2021

Table of Contents

About Our Organization

THE EXPORT-IMPORT BANK OF THE UNITED STATES (EXIM or the Agency) is the official export credit agency (ECA) of the United States (U.S.). EXIM supports the financing of U.S. goods and services in international markets, turning export opportunities into actual sales that help U.S. companies of all sizes to create and maintain jobs in the United States. The Agency assumes the credit and country risks that the private sector is unable or unwilling to accept. EXIM also helps U.S. exporters remain competitive by countering the export financing provided by foreign governments on behalf of foreign companies. Approximately 90 percent of the Agency's transactions were made available for the direct benefit of U.S. small businesses in recent years.

For more information, please see EXIM's website.

THE OFFICE OF INSPECTOR GENERAL (OIG), an independent oversight office within EXIM, was statutorily authorized in 2002 and organized in 2007. The mission of EXIM OIG is to promote the integrity, transparency, and efficiency of EXIM programs and operations by conducting and supervising audits, investigations, inspections, and evaluations related to agency programs and operations; providing leadership and coordination, as well as recommending policies that promote economy, efficiency, and effectiveness in such programs and operations; and preventing and detecting fraud, waste, abuse, and mismanagement.

The OIG is dedicated to acting as an agent of positive change to help EXIM improve its efficiency and effectiveness. It keeps EXIM's President and Chairman and Congress fully informed about problems and deficiencies along with any positive developments relating to EXIM administration and operations.

Find more information about EXIM OIG, including reports of audits, inspections and evaluations, and press releases on our website. For more information on inspectors general in the U.S. government, please see the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and CIGIE's Oversight websites.

A Message from the Inspector General

I am pleased to submit this Semiannual Report on the activities and accomplishments of EXIM OIG for the six-month period ending March 31, 2021. In our last semiannual report, we anticipated that the challenges caused by the COVID-19 pandemic in fiscal year (FY) 2020 would persist into this year, especially as agencies determine how and when it will be safe for the workforce to return to physical facilities. Although there have been some adjustments to our operations due to adherence to public health and safety guidance, we continued our work in advising EXIM management and Congress on recommendations for improving agency programs and operations, as well as detecting, preventing, and prosecuting fraud.

The Office of Audits and Evaluations (OAE) concluded three engagements that were accomplished completely in a remote environment: the audits of EXIM's FY 2020 financial statements and information security program effectiveness, and a risk assessment of the Agency's government purchase card program. The engagements resulted in the issuance of a memorandum and three audit reports, two of which collectively contained 14 recommendations to improve EXIM operations. OAE also completed an external modified peer review of an OIG's evaluation program policies and procedures. At the close of the reporting period, audit work continued in two areas—cyber security and service contracts—and four statutory audits had been initiated.

While the pandemic continues to cause some delays in criminal and civil cases pending before courts and federal grand juries, the Office of Investigations (OI) continued its focus on investigating fraud related to EXIM transactions, traveling only for mission-critical work in accordance with public health and safety guidelines. Working with the U.S. Department of Justice (DOJ), OI obtained a conviction that resulted in 16 months' confinement and 24 months' probation for an individual who pled guilty to obstruction of justice in connection with one of EXIM OIG's criminal investigations. Our agents also worked with the Miami-Dade State Attorney's Office to obtain a plea and conviction for grand theft associated with fraud against EXIM. The individual was sentenced to 36 months' probation after making full restitution to EXIM and paying back the cost of the investigation to the U.S. Treasury. OI and DOJ obtained a guilty plea in another investigation for wire fraud and making false statements to a federally insured bank. The defendant is scheduled for sentencing later this year.

I would like to thank our staff for their hard work, professionalism, and dedication to executing the core mission and responsibilities of this office. We also appreciate the support and cooperation received from EXIM amid the ongoing pandemic. We look forward to continuing to work effectively with the Agency and staff, as well as Congress, to ensure the efficiency and effectiveness of EXIM's programs and operations.

Jennifer L. Fain

Acting Inspector General

Highlights

The **Office of Audits and Evaluations (OAE)** issued three audit reports and one memorandum:

Audit of the Export-Import Bank of the United States Fiscal Year 2020 Financial Statements

(OIG-AR-21-01, November 13, 2020)

Under a contract overseen by OAE, an independent accounting firm performed an audit of EXIM's financial statements for FY 2020 and found (1) the financial statements were fairly presented, in all material respects, in accordance with U.S. generally accepted accounting principles; (2) no material weaknesses in internal control over financial reporting; and (3) no instances of reportable noncompliance with provisions of laws and regulations tested or other matters.

Fiscal Year 2020 Financial Statements Audit Management Letter

(OIG-AR-21-02, November 13, 2020)

As a supplement to the Independent Auditor's report on the FY 2020 Financial Statements, an independent accounting firm issued a management letter that identified deficiencies in EXIM's internal control over financial reporting, which did not rise to the level of material weaknesses or significant deficiencies but should be corrected. The audit report contained eight recommendations to improve internal control over financial reporting. EXIM management concurred with the recommendations.

Risk Assessment of EXIM's Government Purchase Card Program

(OIG-O-21-01, November 24, 2020)

In accordance with the Government Charge Card Abuse Prevention Act of 2012 (the Charge Card Act), we conducted a risk assessment of EXIM's government purchase card (GPC). The Charge Card Act requires the OIG of each executive agency to conduct periodic assessments of agency purchase card, convenience check, and travel card programs to identify and analyze the risks of illegal, improper, or erroneous purchases and payments. The objective of our risk assessment was to determine the scope, frequency, and number of audits of these programs. We determined that EXIM's risk of illegal, improper, or erroneous use within the government purchase card (GPC) program was low.[1] EXIM's purchase card expenditures were immaterial in comparison to its total FY 2019 administrative expenditures; therefore, an audit of the GPC program will not be included in EXIM OIG's annual work plan for FY 2021. The memorandum report did not include recommendations.

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

(OIG-AR-21-03, February 4, 2021)

Under a contract overseen by OAE, an independent accounting firm performed an audit of EXIM's Information Security Program for FY 2020. The independent accounting firm determined

[1] EXIM's Government Travel Card program was not included as part of the assessment because travel expenditures for FY 2019 were below the $10 million requirement for audit or review under the Charge Card Act.

that EXIM's information security program and practices for its systems were effective overall and consistent with federal requirements, standards, and guidance. EXIM received a score of Level 4: Managed and Measurable for the majority of the five Cybersecurity Functions and eight Federal Information Security Modernization Act of 2014 (FISMA) Metric Domains as described by the U.S. Department of Homeland Security (DHS) criteria. However, deficiencies were identified in the Cybersecurity Function areas of Identify, Detect and Protect and three FISMA Metric Domains. In addition, EXIM implemented corrective actions to remediate many of the deficiencies identified in prior year audit. The audit report contained six recommendations to improve the effectiveness of EXIM's information security program. EXIM management concurred with the recommendations.

The **Office of Investigations (OI)** completed the following actions:

Sentencing

OI continued its focus on investigating fraud related to EXIM transactions. In October, a Maryland woman was sentenced to 16 months in prison for obstruction of justice after intentionally misleading investigators and a Louisiana grand jury about her role in a Business Email Compromise scheme that targeted the participants in an EXIM-insured transaction, among others. The woman made up a false story to explain how over $500,000 in fraudulent proceeds moved through several bank accounts that she controlled.

In February, a Miami-area exporter pled guilty to grand larceny in a Miami-Dade County court for causing the enhanced assignee in an EXIM-insured transaction to file a false claim with EXIM. After repaying the claim amount, over $140,000, to EXIM and reimbursing the U.S. Treasury for the cost of the OIG investigation, the exporter was sentenced to 36 months of supervised probation.

Guilty Plea

In January, a Virginia exporter pled guilty to committing wire fraud and making false statements to a federally insured bank for his role in a scheme to defraud a Pennsylvania-based bank and EXIM in connection with a $1.6 million Working Capital Guarantee loan. The exporter created fictitious accounts receivable and financial statements and doctored his company's actual bank statements to show non-existent, high-dollar transactions in order to maintain the line of credit guaranteed by EXIM. The loan eventually defaulted causing the commercial bank to file a claim with EXIM for the entire $1.6 million loan amount. The exporter is scheduled to be sentenced in May.

Suspension and Debarment

During this reporting period, four matters were referred to EXIM's suspension and debarment official for consideration. Additionally, EXIM debarred one individual from doing business with the federal government for three years based on a prior OIG referral.

Office of Audits and Evaluations

OAE conducts and oversees independent and objective audits, inspections, and evaluations to assess the efficiency and effectiveness of EXIM's programs, operations, and transactions. OAE staff may also perform reviews or assessments; conduct research projects; provide advisory or consulting services to EXIM management; or provide information, comments, and other services to outside parties. All audits, inspections, and evaluations are performed in accordance with the requisite standards—the *Government Auditing Standards* (Yellow Book) issued by the Comptroller General of the United States and the CIGIE *Quality Standards for Inspections and Evaluations* (Blue Book). OAE works in tandem with OI whenever appropriate and refers any irregularities and other suspicious conduct to OI for investigative consideration.

Summary of Activities

During this semiannual reporting period, OAE issued three audit reports and one memorandum:

- Audit of the Export-Import Bank of the United States Fiscal Year 2020 Financial Statements
- Fiscal Year 2020 Financial Statements Audit Management Letter
- Risk Assessment of EXIM's Government Purchase Card Program
- Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices Report – Fiscal Year 2020

At the end of the reporting period, OAE had six audits in progress:

- Audit of EXIM's Cybersecurity Program
- Audit of EXIM's Service Contracts
- Audit of EXIM's Compliance with the Reporting Requirements of PIIA for FY 2020
- Audit of EXIM's FY 2021 Financial Statements
- Audit of EXIM's Compliance with FISMA for FY 2021
- Audit of EXIM's Compliance with the DATA Act of 2014

Reports Issued

Audit of the Export-Import Bank of the United States Fiscal Year 2020 Financial Statements

(OIG-AR-21-01, November 13, 2020)

Under a contract overseen by OAE, an independent accounting firm performed an audit to issue an opinion on the accuracy and completeness of EXIM's financial statements for FY 2020 and found:

(1) The financial statements were fairly presented, in all material respects, in conformity with U.S. generally accepted accounting principles;

(2) There were no material weaknesses in internal control over financial reporting; and

(3) There were no instances of reportable noncompliance with provisions of laws and regulations tested or other matters.

Fiscal Year 2021 Financial Statements Audit Management Letter

(OIG-AR-21-02, November 13, 2020)

As a supplement to the Independent Auditor's report on the FY 2020 Financial Statements, an independent accounting firm issued a management letter that identified deficiencies in EXIM's internal control over financial reporting, which did not rise to the level of material weaknesses or significant deficiencies, but nevertheless should be corrected. Specifically, the independent accounting firm found deficiencies in areas such as information security continuous monitoring (ISCM), user recertification, and review of subsidy re-estimate source data. The audit report contained eight recommendations to improve internal control over financial reporting.

(1) Define audit review, analysis and reporting policies and procedures for the tool and the independent review of logged activity on a periodic basis (performed by one who is knowledgeable but not performing the activity).

(2) Implement the defined audit review, analysis, and reporting policies and procedures for the tool and ensure operational effectiveness and compliance.

(3) Align its process to approved policies to ensure they are congruent.

(4) Perform, document, and maintain supporting audit evidence.

(5) Ensure that all identified vulnerabilities are appropriately remediated per EXIM policies.

(6) Formally document and track all vulnerabilities that will not be mitigated accordingly.

(7) Enforce EXIM's existing policies and procedures regarding access control management related to recertification and formally document the performance of the timely review.

(8) Enhance the precision of the review control over the re-estimate model to ensure all relevant data is input accurately.

EXIM management concurred with the recommendations.

Risk Assessment of EXIM's Government Purchase Card Program

(OIG-O-21-01, November 24, 2020)

In accordance with the Government Charge Card Abuse Prevention Act of 2012, we conducted a risk assessment of EXIM's GPC program. The Charge Card Act requires the OIG of each executive agency to conduct periodic assessments of agency purchase card, convenience check, and travel card programs to identify and analyze the risks of illegal, improper, or erroneous purchases and payments. The objective of our risk assessment was to determine the scope, frequency, and number of audits of these programs. We determined that the EXIM's risk of illegal, improper, or erroneous use within the GPC program was low. EXIM's purchase card expenditures were immaterial in comparison to its total FY 2019 administrative expenditures; therefore, an audit of the GPC program will not be included in EXIM OIG's annual work plan for FY 2021. The memorandum report did not include recommendations.

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

(OIG-AR-21-03, February 4, 2021)

Under a contract overseen by OAE, an independent accounting firm performed an audit of EXIM's Information Security Program for FY 2020. The objective of the audit was to determine whether EXIM developed and implemented an effective information security program and practices as required by FISMA. The independent accounting firm determined that EXIM's information security program and practices for its systems were effective overall and consistent with federal requirements, standards, and guidance. EXIM received a score of Level 4: Managed and Measurable for the majority of the five Cybersecurity Functions and eight FISMA Metric Domains as described by the DHS criteria. However, deficiencies were identified in the Cybersecurity Function areas of Identify, Detect and Protect and three FISMA Metric Domains. In addition, EXIM implemented corrective actions to remediate many of the prior-year deficiencies over risk management policies and procedures, information security continuous monitoring program policies and strategies, and many improvements to the contingency planning program. The FY 2020 audit report contained six recommendations to improve the effectiveness of EXIM's information security program.

(1) Define the strategy and roadmap, including the policies and procedures that encompasses all necessary sources of risk data.

(2) Implement a means based on the requirements defined within the strategy and ensure the policies and procedures are consistently implemented.

(3) Define audit review, analysis and reporting policies and procedures.

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

(5) Enhance undertakings to ensure they are applied in accordance with EXIM security effectively. If required, consistently document the business rationale or technical issues delaying the remediation of vulnerabilities within a POA&M.

(6) Expand procedures accordingly.

EXIM management concurred with the recommendations.

Ongoing Projects

Audit of EXIM's Cybersecurity Program

The objective of this audit is 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. The report will be issued in the semiannual reporting period ending September 30, 2021.

Audit of EXIM's Service Contracts

The objective of this audit is to assess the effectiveness of EXIM's existing controls over contracts for services and to determine compliance with the Federal Acquisition Regulation. The report will be issued in the semiannual reporting period ending September 30, 2021.

Independent Auditor's Report on EXIM's Compliance with the Reporting Requirements of PIIA for FY 2020

Under a contract overseen by OAE, an independent public accounting firm is conducting an audit of EXIM's reporting compliance with the Payment Integrity Information Act of 2019 (PIIA) for FY 2020. The audit objective is to determine whether EXIM was in compliance with the reporting requirements of PIIA in the payment integrity section of the FY 2020 Annual Management Report and accompanying materials. In addition, the audit will assess the accuracy and completeness of EXIM's improper payment reporting and efforts to prevent and reduce improper payments. The report will be issued in the semiannual reporting period ending September 30, 2021.

Audit of EXIM's FY 2021 Financial Statements

An independent public accounting firm, working under OAE supervision, is conducting an audit to issue an opinion on the accuracy and completeness of EXIM's financial statements for FY 2021. The report will be issued, along with a related management letter report, in the semiannual period ending March 31, 2022.

Audit of EXIM's Compliance with FISMA for FY 2021

Under a contract overseen by OAE, an independent public accounting firm is conducting an audit to determine whether EXIM developed adequate and effective information security policies, procedures, and practices in compliance with FISMA. The report will be issued in the semiannual reporting period ending March 31, 2022.

Audit of EXIM's Compliance with the DATA ACT of 2014

Under a contract overseen by OAE, an independent public accounting firm is conducting an audit to determine the completeness, accuracy, timeliness, and quality of the financial and award data that EXIM submitted for publication on USASpending.gov, and (2) EXIM's implementation and use of the government-wide financial data standards established by the Office of Management and Budget (OMB) and the U.S. Department of the Treasury. The report will be issued in the semiannual reporting period ending March 31, 2022.

Office of Investigations

OI conducts and coordinates investigations relating to alleged or suspected violations of federal laws, rules, or regulations occurring in EXIM programs and operations, which may result in criminal or civil prosecution and/or administrative sanctions. The subjects of OI investigations may be program participants, contractors, agency management or employees. OI's investigations are supported by Investigative and Financial Analysts who conduct tactical and strategic intelligence analysis in support of OI's investigations.

Summary of Investigations

OI evaluates all reports of possible fraud or illegality affecting EXIM programs and activities. Such reports are received from a variety of sources including agency employees, EXIM's Office of General Counsel (OGC), participants in agency transactions, other government agencies, and the EXIM OIG Hotline. Evaluations that identify reasonable indications of fraud or illegality result in an investigation. These investigations are summarized in the table below.

Activity	Investigations
Open as of October 1, 2020	20
Opened during period	9
Closed during period	3
Open as of March 31, 2021	26

Of the 26 current open investigations, the following table depicts the category of EXIM program affected by the investigation based on the allegations received:

Program	Number of Investigations
Export Credit Insurance	9
Loan Guarantee	3
Working Capital	5
Letter of Interest	2
Employee Integrity	0
Other (i.e., proactive investigations)	7

Investigative Results

OI undertook the following investigative actions during this reporting period:

Description	OIG	Joint Activities*	Total
Matters Referred for Prosecution Consideration	1	2	3
Matters Referred for State and Local Consideration	0	0	0
Criminal Indictments, Informations, Complaints	1	0	1
Guilty Pleas Entered	2	0	2
Criminal Judgments	2	0	2
Civil Actions	0	0	0
Civil Recoveries	$100,000	0	$100,000
Prison Time (months)	16	0	16
Probation (months)	60	0	60
Court Ordered Fines, Assessments, Restitutions, and Forfeitures	$111,673	$0	$111,673
Administrative Actions**	0	0	0
Administrative Employee Actions***	0	0	0
Administrative Cost Savings and Repayments	$68,029	$0	$68,029
Suspensions and Debarments	1	0	1

* *Joint investigations with other law enforcement agencies.*

** *Administrative actions are responses by EXIM to stop transactions, cancel policies, or protect funds at risk based on investigative findings.*

*** *Administrative employee actions are responses by EXIM to terminate or discipline Bank employees based on investigative findings.*

The metrics used in this report were obtained from a system of records entitled, "EIB-35-Office of Inspector General Investigative Records" also known as "CMTS". CMTS is a Structured Query Language (SQL) database used by OI to store its records related to criminal, civil, and administrative investigations. The database contains assignments, allegations, investigative activities, actions, dates, and identifying information about potential subjects and individuals related to these investigations. The system is able to generate metrics reports, which track judicial, administrative, and other investigative actions and activities. The database generates statistical reports on a variety of OI products including: Hotlines, Complaints, Subpoenas, and Investigations.

Investigations

During the reporting period, successful criminal fraud investigative efforts involving EXIM programs include the following:

Co-Conspirator Sentenced for Obstruction of Justice (Export Credit Insurance)

During previous reporting periods, Fatima Mahdi Sesay of Laurel, MD was indicted and pled guilty in the Middle District of Louisiana to one count of violating 18 U.S.C. § 1503 (Obstruction of Justice). An investigation revealed that the proceeds from a Business Email Compromise fraud scheme targeting an EXIM-insured transaction, among others, were deposited into a Bank of America account that Sesay had opened. Across dozens of suspicious transactions, nearly $500,000 had passed through accounts in Sesay's name. EXIM OIG agents contacted Sesay and made several attempts to secure truthful information from her about her knowledge of the

scheme. Sesay made numerous evasive and misleading statements in an interview with agents and then knowingly provided false testimony before a federal grand jury. On October 20, 2020, Sesay was sentenced to serve 16 months in prison followed by 24 months supervised release.

Exporter Sentenced in Miami-Dade County for Causing False Claim (Export Credit Insurance)

On August 11, 2020, Romel Duran Martinez of Miami, FL was arrested and charged with section 812.014(2)(A) of the Florida Criminal Code, Grand Larceny. Through his company, Deoca Manufacturing Co. (Deoca), Duran exported automotive parts to a buyer in Colombia under an EXIM Short Term Multi-Buyer Credit Insurance policy. EXIM approved a third party to finance up to $150,000 against Deoca's receivables. Under the conditions of the policy, Duran was required to instruct Deoca's buyer to make payments directly to the third-party financier. On February 16, 2021, Duran pled guilty and admitted that Deoca received payment in full from the buyer, but that he falsely certified to the lender and EXIM that the buyer defaulted on payments, causing the financing company to file a false claim with EXIM in the amount of $142,472. Duran was sentenced to 36 months of supervised probation and ordered to pay $110,970.66 in restitution and $29,029.34 for investigative costs. Duran previously paid approximately $39,000 to EXIM in administrative repayments prior to his plea.

Exporter Pleads Guilty after Submission of Inflated Financial Records (Working Capital Guarantee)

On January 19, 2021, Tae Il Lee of Glen Allen, VA pleaded guilty to one count of 18 U.S.C. § 1343 (Wire Fraud) and one count of 18 U.S.C. § 1014 (Making False Statements to a Federally Insured Bank) as part of a scheme to defraud both a Pennsylvania-based bank and EXIM in connection with a $1.6 million loan. Lee was the Managing Director of New World Group, a Richmond-based exporter. In 2016, Lee obtained a $1.6 million line of credit for New World Group from a commercial bank guaranteed by EXIM under the Working Capital Guarantee Program. After obtaining the loan, Lee created fictitious accounts receivable and financial statements, and doctored New World Group's actual bank statements to show non-existent, high-dollar transactions that never took place to keep the line of credit open. New World Group never completed any payments to the commercial bank and the loan went into default causing the commercial bank to file a claim with EXIM for the full $1.6 million. Lee is scheduled to be sentenced on May 12, 2021.

Other Investigative Results

As reported in the previous Semiannual Report, the COVID pandemic has substantially disrupted judicial activity in many federal judicial districts. While many courts have begun to reopen, there is a backlog of case activity pending before the courts and many federal grand juries. While the pandemic has delayed a number of EXIM OIG criminal and civil court cases, the bulk of our investigative activity has continued. While most investigative staff continue to work remotely, EXIM OIG has procured personal protective equipment (PPE) for agents who are required to conduct field operations. EXIM OIG agents have traveled for mission-critical work in accordance with health and safety guidelines. OI has also been able to maintain most annual and periodic requirements contained in policy, CIGIE quality standards, and the Attorney General Guidelines for Offices of Inspectors General.

EXIM OIG has not seen a substantial increase in investigative cases related to COVID-19 to date. However, EXIM OIG anticipates that the number of suspicious transactions referred to OIG are

likely to increase as EXIM rebuilds its portfolio, and the financial pressure on foreign and domestic businesses increases as a result of the COVID pandemic, consistent with the substantial increase in financial fraud associated with the various COVID-related legislation such as the CARES Act and other relief measures. Currently, EXIM's COVID-19 temporary relief measures—which include waivers, deadline extensions, streamlined processing, and documentation flexibility—were extended through April 30, 2022. In light of the time lag which typically occurs between EXIM transactions and the identification of potential fraud, EXIM OIG anticipates that the majority of fraud arising from the current financial downturn will not be detected until later in 2021 or subsequent years, but expects a surge in fraud activity to increase OI's caseload in the coming years.

EXIM's suspension and debarment program serves as a critical tool to prevent fraud, waste, and abuse, and to protect the federal government. During this reporting period, EXIM OIG referred four entities to the EXIM suspension and debarment official for consideration. In addition, one individual was debarred from doing business with the federal government for three years based on a prior EXIM OIG referral to the Agency.

To the extent permissible and within the confines and limitations of an investigation, OI Special Agents work collaboratively to share investigative intelligence with OGC, the Office of Risk Management, and the Asset Management Division of EXIM to help identify potential and suspected fraudulent activity within EXIM transactions and to protect funds at risk.

OI shared intelligence with OGC on several matters concerning suspected criminal activity by participants involved in active insurance policies or transactions under review. OI made nine referrals of investigative information to OGC concerning potential fraud and funds at risk for enhanced due diligence by EXIM. Additionally, OI investigative analysts responded to nearly 275 deconfliction requests from the Department of Homeland Security and the Export Enforcement Coordination Center (E2C2).

Hotline Activity

EXIM OIG maintains a hotline to receive reports of fraud, waste, and abuse in EXIM programs and operations. Hotline reports are evaluated by our investigative team and, based on the available evidence, may result in the initiation of an investigation, audit, inspection, evaluation, referral to other law enforcement authorities, or referral to agency management for administrative action.

EXIM OIG received ten hotline reports during this semiannual reporting period. Seven were resolved and closed by the hotline operator, one was opened as an investigative matter, one was referred to the Agency for action as deemed appropriate, and one was referred to another agency with jurisdiction over the matter reported.

Hotline reports can be made by any of the following methods:

- Phone at 1-888-OIG-EXIM (1-888-644-3946);
- E-mail at IGhotline@exim.gov, or;
- In person or mail/delivery service to EXIM OIG Hotline, Office of Inspector General, 811 Vermont Avenue, NW, Room 1052-1, Washington DC 20571.

EXIM OIG will not disclose the identity of a person making a report through the hotline without their consent unless the Inspector General determines such disclosure is unavoidable during the course of an investigation.

Office of Inspector General Management Initiatives

COVID-19

The World Health Organization declared COVID-19 a global pandemic on March 11, 2020. The next day, OMB issued a memorandum to executive agency heads encouraging them to maximize telework flexibilities for federal employees, which EXIM implemented on March 16, 2020. Full-time remote work operations for EXIM and EXIM OIG persist. To proactively address the significant and evolving issues created by the pandemic, EXIM OIG continues to collaborate with internal and external COVID-19 working groups. EXIM OIG anticipates that this work will continue through the next reporting period.

Fraud Awareness Training and Outreach

As part of EXIM OIG's mission to prevent and detect fraudulent activity, continual efforts are made to meet with and educate stakeholders and other law enforcement partners about the various risks and fraud scenarios most commonly seen in trade finance, export credit fraud, and money laundering cases. OI management continues to work with the Agency's OGC and the Office of the Chief Risk Officer, as well as the Office of the Chief Information Officer to discuss intelligence sharing, OIG's enhanced due diligence referrals to OGC, and other ways the OIG and the Agency can work together to prevent bad actors from defrauding EXIM.

Further, OIG is looking into other ways to increase fraud awareness and outreach through other mechanisms such as using fraud alerts to notify the Agency and transaction participants of common fraud schemes reported to OI and how to detect and avoid falling victim to them in the future. Additionally, OI management plans to conduct outreach to EXIM's Delegated Authority partners to familiarize the financial institutions with common fraud identifiers and increase awareness of how to report suspicious activity to OIG.

Council of Inspectors General on Integrity and Efficiency

EXIM OIG participates in CIGIE activities, including the Audit Committee, the Inspection and Evaluation Committee, the Investigations Committee, the Legislation Committee, the Council of Counsels to the Inspectors General, as well as the Whistleblower Protection Coordinators and legal working groups. Through CIGIE, EXIM OIG continues to coordinate and collaborate with other OIG partners to use resources more effectively, share knowledge, strengthen oversight, and serve our critical mission.

Administrative and Risk Assessment Processes

EXIM OIG continues to focus on improving its current administrative and risk assessment processes to achieve the following desired outcomes:

- Streamlined internal processes and communication through automation and use of technology and collaborative platforms.
- Optimization of scarce resources through prioritizing assignments, setting performance metrics, clear allocation of responsibilities, using templates, etc.
- Greater use of data analytics by using a dashboard that provides a comprehensive historical database of EXIM transactions that will allow users to conduct queries, analysis, reporting, and data visualization.

- Incorporation of risk management within all key processes to ensure that risks can be managed effectively.

Review of Legislation and Regulations

Pursuant to section 4(a)(2) of the Inspector General Act of 1978, as amended, EXIM OIG reviews proposed and existing legislation and regulations related to EXIM's programs and operations. During this reporting period, EXIM OIG participated in a Whistleblower Protection Coordinator working group and assisted a CIGIE working group focused on IG legislative priorities.

Government Accountability Office

The IG Act states that each IG shall give particular regard to the activities of the Comptroller General of the United States with a view toward avoiding duplication and ensuring effective coordination and cooperation. During the reporting period, EXIM OIG shared information on ongoing and planned work with General Accountability Office officials.

APPENDIX A

Open Recommendations from Prior Reporting Periods

This table shows that 20 recommendations from six reports issued up to September 30, 2020, remain open at the end of this reporting period. Seventeen open recommendations are from reports issued in FY 2020. The remaining three open recommendations are from reports issued in FY 2017 and FY 2019. Reports from prior periods are no longer listed when all recommendations have been closed.

Report No./ Date	Report Title	Recommendations				Latest Target Closure Date
		Total	Open	Closed	Unresolved	
Last Period (4/1/20 –9/30/20)						
Audits						
OIG-AR-20-06 09/30/2020	Audit of EXIM's Suspension and Debarment Program	2	1	1	0	9/30/2021
Prior Periods (prior to 3/31/20)						
Audits						
OIG-AR-20-01 8 Nov 2019	Independent Auditors' Report on EXIM Bank's Data Act Submission	14	14	0	0	6/30/2021
Inspections and Evaluations						
OIG-EV-17-01 2 Dec 2016	Evaluation of Risk Management Procedures and CRO Responsibilities	8	1	7	0	6/30/2021
OIG-EV-17-03 30 Mar 2017	Report on EXIM Bank's CGF Program	5	1	4	0	3/31/2021
OIG-EV-19-03 19 Jun 2019	Evaluation of EXIM's CLF Model and Loss Reserve Process	7	1	6	0	3/31/2021
OIG-EV-20-01 2 Dec 2019	Evaluation of EXIM's PRM Procedures and CRO Responsibilities	3	2	1	0	3/31/2021 9/30/2021
	Total	39	20	19	0	

APPENDIX B

Audit and Evaluation Reports Issued from October 1, 2020 – March 31, 2021

	Report No./Date	Report Title	Management Decisions Reached on Recommendation	Total Questioned Cost	Unsupported Cost	Funds for Better Use	Disallowed Cost
1	OIG-AR-21-01 13 Nov 2020	Audit of the Export-Import Bank of the United States Fiscal Year 2020 Financial Statements	0/0	0	0	0	0
2	OIG-AR-21-02 13 Nov 2020	Fiscal Year 2020 Financial Statements Audit Management Letter	8/8	0	0	0	0
3	OIG-O-21-01 24 Nov 2020	Risk Assessment of EXIM's Government Purchase Card Program	0/0	0	0	0	0
4	OIG-AR-21-03 4 Feb 2021	Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices Report - Fiscal Year 2020	6/6	0	0	0	0
		Total		0	0	0	0

APPENDIX C

Significant Recommendations from Previous Semiannual Reports on Which Corrective Action Has Not Been Completed

We identified two significant recommendations that were agreed to by EXIM but have not been implemented as of March 31, 2021. We are committed to working with Bank management to expeditiously address the management decision and correct action process, recognizing that certain initiatives will require long-term, sustained, and concerted efforts.

Evaluation of Risk Management Procedures and Chief Risk Officer Responsibilities

(OIG-EV-17-01, December 2, 2016)

Recommendation 1: To clarify the authority and responsibility of the Chief Risk Officer with respect to the current allocation of risk management responsibilities across the agency, EXIM Bank should formally document the risk management roles, responsibilities and authority of its line of defense functions; clarify responsibilities and interaction between different senior management committees and divisions; identify the individuals and functions to be responsible for each; and address any gaps in those responsibilities.

Expected implementation date: June 30, 2021.

Report on EXIM Bank's Credit Guarantee Facility Program

(OIG-EV-17-03, March 30, 2017)

Recommendation 5: Review and update the reachback policy for the CGF program to be consistent with actual practice and reduce the need for waivers. In reviewing and updating the reachback policy, the Bank should analyze the case-by-case determination of a reachback relative to the average policy date (i.e., operative date); consider establishing limits on the utilization of the facility for reachback transactions; set requirements for communicating analysis of reachback issues to decision makers including the Board; and establish procedures for consideration of waivers to the policy. This would include documenting the supporting evidence in the credit file.

Expected implementation date: March 31, 2021.

APPENDIX D

Open Recommendations

	Recommendation	Status	Expected Implementation Date	Management Agree or Disagree	Questioned Cost	Funds for Better Use
Evaluation of Risk Management Procedures and Chief Risk Officer Responsibilities (OIG-EV-17-01, December 2, 2016)						
1	To clarify the authority and responsibility of the CRO with respect to the current allocation of risk management responsibilities across the agency, EXIM Bank should formally document the risk management roles, responsibilities and authority of its line of defense functions; clarify responsibilities and interaction between different senior management committees and divisions; identify the individuals and functions to be responsible for each; and address any gaps in those responsibilities.	Open	6/30/2021	Agree	0	0
Report on EXIM Bank's CGF Program (OIG-EV-17-03, March 30, 2017)						
5	Review and update the reach back policy for the CGF program to be consistent with actual practice and reduce the need for waivers. In reviewing and updating the reach back policy, the Bank should analyze the case-by-case determination of a reach back relative to the average policy date (i.e., operative date); consider establishing limits on the utilization of the facility for reach back transactions; set requirements for communicating analysis of reach back issues to decision makers including the Board; and establish procedures for consideration of waivers to the policy. This would include documenting the supporting evidence in the credit file.	Open	3/31/2021	Agree	0	0
Evaluation of EXIM's Credit Loss Factor Model and Loss Reserve Process (OIG-EV-19-03, June 19, 2019)						
7	Expanding the current model program into a formal MRM framework, particularly with an expansion to include better risk mitigation surrounding error checking, statistical reporting, execution of model changes, and role definition. One of these roles should include documentation updates (i.e., a checklist item) to ensure that the SOP matches the current process to reduce errors.	Open	3/31/2021	Agree	0	0
Independent Auditors' Report on EXIM's DATA Act Submission (OIG-AR-20-01, November 8, 2019)						
1	Revise the internal control activities around Files A, B, and C to ensure that the Bank performs accurate and appropriately designed validations and reconciliations before the SAO submits and certifies the Bank's quarterly DATA Act submissions. Procedures should ensure that the reconciliations use all amounts shown in each file and that personnel itemize all reconciling items and identify corrective actions. Once the Bank has completed the corrective actions, it should re-perform the	Open	6/30/2021	Agree	0	0

	Recommendation	Status	Expected Implementation Date	Management Agree or Disagree	Questioned Cost	Funds for Better Use
	reconciliations until all reconciling items are resolved or no further action is required.					
2	Design, document, and implement a formalized document signoff process that includes the names of the preparer and the reviewers and the dates that the preparer and reviewers completed and approved the internal control activities (i.e., the reconciliations) so the Bank can perform proper monitoring of the control procedures in conjunction with each DATA Act submission.	Open	6/30/2021	Agree	0	0
3	Develop, document, and implement a policy requiring that all journal vouchers that adjust obligated balances include object classes and program activity codes.	Open	6/30/2021	Agree	0	0
4	Review the Bank's current policies and procedures for entering obligations in FMS-NG to ensure that they reiterate requirements for accurately and completely entering object classes and program activity codes in FMS-NG.	Open	6/30/2021	Agree	0	0
5	Develop and document a corrective action plan to assure that the Bank accurately and completely reports object classes and program activity codes in all financial and award data submissions (Files B and C). The corrective action plan should document EXIM's root-cause analysis, steps required to correct missing object classes in financial and award data submissions, and the planned timeline.	Open	6/30/2021	Agree	0	0
6	Determine the root cause of the errors identified during the testing of the first-quarter FY 2019 File D1 and take the necessary corrective action to (a) correct the errors for records shown in USASpending.gov, (b) identify the risk of reporting incorrect data for each data element containing an error, and (c) modify the policies and procedures for recording data in Comprizon and FPDS to address the risks, and to include adequate verification and validation review processes performed by the data owner and a supervisor or other independent party.	Open	6/30/2021	Agree	0	0
7	Determine the root cause of the errors identified during the testing of the first-quarter FY 2019 File D2 and take the necessary corrective action to (a) correct the errors for records shown in USASpending.gov, (b) identify the risk of reporting incorrect data for each data element containing an error, and (c) modify the policies and procedures for recording data in FABS to address the risks, and to include adequate verification and validation review processes performed by the data owner and a supervisor or other independent party.	Open	6/30/2021	Agree	0	0

	Recommendation	Status	Expected Implementation Date	Management Agree or Disagree	Questioned Cost	Funds for Better Use
8	Improve the design of its review of the procurement and financial assistance award data in FPDS and FABS by reviewing additional data elements and performing more comprehensive reviews.	Open	6/30/2021	Agree	0	0
9	Design, document, and implement a process for reviewing Files D1 and D2 before the SAO submits and certifies the quarterly DATA Act submissions, and a process for notifying the DATA Broker of any errors identified in data derived by the DATA Broker. Review procedures should include steps for documenting any errors or concerns identified, including any necessary corrective actions.	Open	6/30/2021	Agree	0	0
10	Establish policies and procedures that address timelines for submitting FABS files that comply with P.L. 109-282, including internal milestones to ensure that the files can be extracted, validated, and uploaded to FABS by required due dates. The policies and procedures should also address cut-off dates for submitting correcting data that ensure sufficient time for the SAO certification of quarterly DATA Act submissions, commensurate with EXIM's risk tolerance related to data accuracy, completeness, and quality.	Open	6/30/2021	Agree	0	0
11	Establish policies and procedures to help ensure that all data reported in FABS and included in EXIM's certified File D2 are reported as intended by the DATA Act Standards and seek clarification from OMB and Treasury as necessary to ensure appropriate interpretation of the DATA Act Standards.	Open	6/30/2021	Agree	0	0
12	Complete a data inventory to govern its DATA Act activities and help ensure compliance with government-wide financial data standards.	Open	6/30/2021	Agree	0	0
13	Develop and implement a review process for the data inventory that the Bank will perform at regular intervals and after each DAIMS update.	Open	6/30/2021	Agree	0	0
14	Develop, test, and implement a DQP that covers significant milestones and major decisions pertaining to: (a) Organizational structure and key processes providing internal control activities for spending reporting; (b) Management's responsibility to supply quality data to meet the reporting objectives for the DATA Act in accordance with OMB Circular No. A-123; (c) EXIM's testing plan and identification of high-risk reported data, including (1) specific data that the Bank determines to be high-risk that are explicitly referenced by the DATA Act and (2) confirmation that these data are linked	Open	6/30/2021	Agree	0	0

	Recommendation	Status	Expected Implementation Date	Management Agree or Disagree	Questioned Cost	Funds for Better Use
	through the inclusion of the award identifier in the agency's financial system and are reported with plain English award descriptions; and (d) Actions taken to manage identified risks.					
Evaluation of EXIM's Portfolio Risk Management Procedures and CRO Responsibilities (OIG-EV-20-01, December 2, 2019)						
2	Create a Bank-wide Model Risk Management framework to ensure integrity of data products and continuity of model production.	Open	3/31/2021	Agree	0	0
3	Develop the Bank-wide Risk and Control Matrix and a Risk and Controls Self-Assessment that covers both financial and non-financial internal controls identification and mitigation of risks.	Open	9/30/2021	Agree	0	0
Audit of EXIM's Suspension and Debarment Program (OIG-AR-20-06, September 30, 2020)						
1	Update, finalize, and implement internal procedures to ensure that S&D referrals are processed consistently and in accordance with a designated time-frame. The internal procedures should require but are not limited to: (a) Establish preliminary and SDO review timelines for processing of referrals differentiated by case types; (b) Implement a process to alert responsible staff to send timely notification of suspension, proposed debarment, and debarment decisions to affected parties; (c) Require entry of excluded individuals into SAM within 3 business days as required and sending timely notification of decisions to the affected parties; and (d) Include controls and process validation for the various phases and steps involved (e.g., queues by case type, milestones or follow-up dates for phase and step(s) completion, monitoring reports, and periodic reconciliation of exclusion information to SAM).	Open	9/30/2021	Agree	0	0
Fiscal Year 2020 Financial Statements Audit Management Letter (OIG-AR-21-02, November 13, 2020)						
1	Define audit review, analysis and reporting policies and procedures for the tool and the independent review of logged activity on a periodic basis (performed by one who is knowledgeable but not performing the activity).	Open	11/15/2021	Agree	0	0
2	Implement the defined audit review, analysis, and reporting policies and procedures for the tool and ensure operational effectiveness and compliance.	Open	11/15/2021	Agree	0	0
3	Align its process to approved policies to ensure they are congruent.	Open	11/15/2021	Agree	0	0
4	Perform, document, and maintain supporting audit evidence.	Open	11/15/2021	Agree	0	0
5	Ensure that all identified vulnerabilities are appropriately remediated per EXIM policies.	Open	11/15/2021	Agree	0	0
6	Formally document and track all vulnerabilities that will not be mitigated accordingly.	Open	11/15/2021	Agree	0	0

	Recommendation	Status	Expected Implementation Date	Management Agree or Disagree	Questioned Cost	Funds for Better Use
7	Enforce EXIM's existing policies and procedures regarding access control management related to recertification and formally document the performance in a timely manner.	Open	11/15/2021	Agree	0	0
8	Enhance the precision of the review control over the re-estimate model to ensure all relevant data is input accurately.	Open	11/15/2021	Agree	0	0
Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices Report – Fiscal Year 2020 (OIG-AR-21-03, February 4, 2021)						
1	Define the strategy and roadmap, including the policies and procedures that encompasses all necessary sources of risk data.	Open	2/4/2022	Agree	0	0
2	Implement a means based on the requirements defined within the strategy and ensure the policies and procedures are consistently implemented.	Open	2/4/2022	Agree	0	0
3	Define audit review, analysis and reporting policies and procedures.	Open	2/4/2022	Agree	0	0
4	Implement the defined audit review, analysis, and reporting policies and procedures and ensure operational effectiveness and compliance.	Open	2/4/2022	Agree	0	0
5	Enhance undertakings to ensure they are applied in accordance with EXIM security effectively. If required, consistently document the business rationale or technical issues delaying the remediation of vulnerabilities within a POA&M.	Open	2/4/2022	Agree	0	0
6	Expand procedures accordingly.	Open	2/4/2022	Agree	0	0
				Total	$0	$0

APPENDIX E

Peer Review Reporting

Pursuant to Sections 5(a)(14), (15), and (16) of the Inspector General Act, as amended, this section provides information on peer reviews of EXIM OIG's audit, inspection, evaluation, and investigation functions.

Office of Audits and Evaluations

The latest peer review of EXIM OIG's audit function was conducted by the National Archives and Records Administration OIG, whose report was issued on September 8, 2017. The Office of Audits received an external peer review rating of pass on the system of quality control for the audit function. There are no outstanding recommendations from this peer review. Due in part to the uncertainty associated with COVID-19, the completion of the peer review of the audit function scheduled for FY 2020 has been extended until June 30, 2021.

The first peer review of EXIM OIG's inspection and evaluation function was conducted by the Farm Credit Administration and the Corporation for National and Community Services OIGs (the Review Team), whose report was issued on September 25, 2018. The Review Team concluded that EXIM OIG's Office of Inspections and Evaluations generally met the seven CIGIE quality standards assessed and complied with internal policies and procedures. There are no outstanding recommendations.

On December 3, 2020, OAE completed a modified external peer review of the EEOC OIG's evaluation program policies and procedures. The review team, comprised of a lead from OAE and a team member from SIGTARP OIG, concluded that EEOC OIG's internal policies and procedures, as presented in its manual, generally met the seven CIGIE Blue Book standards (Quality Control; Planning; Data Collections and Analysis; Evidence; Records Maintenance; Reporting; and Follow-up) addressed in the peer review.

Office of Investigations

The most recent peer review of EXIM OIG's investigation function was conducted by the Board of Governors of the Federal Reserve System OIG, whose report was issued on September 11, 2017. OI received a rating of compliant with the standards required by CIGIE and the applicable Attorney General guidelines. There are no outstanding recommendations from this peer review. Due to the uncertainty associated with COVID-19, the peer review of the investigation function scheduled for FY 2020 has been extended pursuant to the government-wide waiver issued by the U.S. Department of Justice.

APPENDIX F

Inspector General Act Reporting Requirements

Inspector General Act Citation	Requirement Definition	Page
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	3-4
Section 5(a)(2)	Recommendations for Corrective Actions	3-4; 6-8
Section 5(a)(3)	Prior Significant Audit Recommendations Yet to Be Implemented	21
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	12
Sections 5(a)(5) and 6(c)(2)	Summary of Refusals to Provide Information	None
Section 5(a)(6)	Audit, Inspection and Evaluation Products Issued Including Total Dollar Values of Questioned Costs, Unsupported Costs, and Recommendations That Funds Be Put to Better Use	20
Section 5(a)(7)	Summary of Particularly Significant Reports	3-4
Section 5(a)(8)	Total Number of Reports and Total Dollar Value for Audits, Inspections and Evaluations with Questioned and Unsupported Costs	None
Section 5(a)(9)	Total Number of Reports and Total Dollar Value for Audits, Inspections and Evaluations with Recommendations That Funds Be Put to Better Use	None
Section 5(a)(10)(A) – (C)	Summary of Prior Audit, Inspection and Evaluation Products for Which No Management Decision Has Been Made, No Comment was Returned Within 60 Days, Recommendation Exists Regarding Aggregate Cost Savings	None
Section 5(a)(11)	Description and Explanation of Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions with Which the Inspector General Disagreed	None
Section 5(a)(13)	Reporting in Accordance with Section 804(b) of the Federal Financial Management Improvement Act of 1996 Remediation Plan	None
Section 5(a)(14)	Results of Peer Review Conducted by Another IG; or Date of Last Peer Review If No Peer Review Conducted During Reporting Period	27
Section 5(a)(15)	List of Outstanding Recommendations from Peer Review Conducted by Another IG That Have Not Been Fully Implemented	None
Section 5(a)(16)	List of Peer Reviews of Another IG During the Reporting Period Including Outstanding Recommendations from Previous Peer Review That Remain Outstanding or Have Not Been Fully Implemented	27; None

Inspector General Act Citation	Requirement Definition	Page
Section 5(a)(17)(A) – (D)	Total Investigative Reports, Referred to the DOJ, Number of Persons Referred to State and Local Authorities, Total Indictments, etc. That Resulted from Prior Referral to Prosecuting Authorities	12
Section 5(a)(18)	Metrics Used for Developing Data for Statistical Tables	12
Section 5(a)(19)(A) – (B)	Senior Government Employee Substantiated Misconduct, Facts, Disposition	None
Section 5(a)(20)	Whistleblower Retaliation	None
Section 5(a)(21)(A) – (B)	Interfered with OIG Independence Through Withholding Budget or Causing Delay	None
Section 5(a)(22)(A) – (B)	Report Closed but Not Disclosed to the Public	None

HOW TO REPORT FRAUD, WASTE, AND ABUSE

The Inspector General Act of 1978, as amended, empowers the Inspector General (IG) to receive and investigate complaints or information concerning the possible existence of an activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health and safety. Whether reporting allegations via telephone, mail, or in person, EXIM OIG will not disclose the identity of persons making a report without their consent unless the IG determines such disclosure is unavoidable during the course of the investigation. You may submit your complaint or information by these methods:

In person

Office of Inspector General
Export-Import Bank of the U.S.
811 Vermont Avenue, NW
Washington, D.C. 20571

Telephone

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

Mail

Office of Inspector General Hotline
Export-Import Bank of the U.S.
811 Vermont Avenue, NW
Washington, D.C. 20571

E-mail

IGhotline@exim.gov

For information about EXIM OIG's Whistleblower Protection Coordinator, you may contact oig.info@exim.gov. For additional resources and information about whistleblower protections and unlawful retaliation, please visit https://oversight.gov/Whistleblowers.

Office of Inspector General
Export-Import Bank *of the* United States
811 Vermont Avenue, NW
Washington, DC 20571

Telephone 202-565-3908
Facsimile 202-565-3988

www.exim.gov/about/oig

Visit Oversight.gov to find reports from all Federal Inspectors General who are members of the Council of Inspectors General on Integrity and Efficiency (CIGIE).