EXPORT-IMPORT BANK OF THE UNITED STATES

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

SEMIANNUAL
REPORT TO CONGRESS
April 1, 2021 to September 30, 2021

Table of Contents

About Our Organization

THE EXPORT-IMPORT BANK OF THE UNITED STATES (EXIM) 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. Over 85 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

In the second half of fiscal year (FY) 2021, EXIM OIG continued its work advising EXIM management and Congress on recommendations for improving agency operations, as well as detecting, preventing, and prosecuting fraud. This semiannual report details that work and includes EXIM OIG's annual assessment of the major management and performance challenges facing the agency. The key challenges identified and discussed are: vacancies and turnover, resource management, information technology and cybersecurity, operational challenges arising from the coronavirus pandemic, and internal controls.

During this semiannual period, our office published three reports—an audit report on improper payments, an audit report on cybersecurity, and a memorandum report on the annual risk assessment of the government purchase card program. I am pleased to report that EXIM OIG passed its audit peer review with no deficiencies and was found to be in full compliance with required standards. In addition, our office continued its focus on investigating fraud related to EXIM transactions, as well as fraud targeted toward EXIM transaction participants. A defendant who previously pleaded guilty to wire fraud and making false statements to a federally-insured bank in connection with an EXIM working capital guarantee loan was sentenced to 34 months incarceration and 60 months supervised release. The defendant was also ordered to repay $1.6 million in restitution to EXIM. Additionally, EXIM OIG agents, working with the Department of Homeland Security (DHS) and the Department of Justice (DOJ), charged five individuals operating a Business Email Compromise (BEC) scheme. Our agents have also begun working with a task force overseen by CIGIE's Pandemic Response Accountability Committee (PRAC) investigating Coronavirus Aid, Relief, and Economic Security (CARES) Act fraud.

I would like to express my sincere gratitude to the staff of EXIM OIG. None of these accomplishments would have been possible without their hard work and dedication. We look forward to continuing to work effectively with EXIM, as well as Congress, to promote the efficiency and effectiveness of the agency's programs and operations.

Jennifer L. Fain

Acting Inspector General

Highlights

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

Independent Auditors' Report on EXIM's Compliance with the Payment Integrity Information Act of 2019 for FY 2020

(OIG-AR-21-04, April 22, 2021)

Under a contract overseen by OAE, an independent accounting firm performed an audit of EXIM's compliance with the Payment Integrity Information Act of 2019 (PIIA) for FY 2020. The independent accounting firm determined that EXIM complied with the annual reporting requirements of PIIA for FY 2020 and its reporting was accurate and complete. In addition, EXIM had taken adequate steps to prevent and reduce improper payments and maintained adequate internal controls over the improper payment process. The audit report did not include any recommendations.

Audit of EXIM's Cybersecurity Program

(OIG-AR-21-05, July 12, 2021)

Our audit of EXIM's cybersecurity program found that it 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 the agency did not actively maintain training records per federally recommended guidelines. The audit report included three recommendations to improve the effectiveness of EXIM's cybersecurity program.

Risk Assessment of EXIM's Government Purchase Card Program

(OIG-O-21-02, September 30, 2021)

Our risk assessment of EXIM's government purchase card (GPC) program found that EXIM's risk of illegal, improper or erroneous use was low. Further, EXIM's purchase card expenditures were immaterial in comparison to its total FY 2020 administrative expenditures; therefore, an audit of the GPC and government travel card (GTC) programs will not be included in EXIM OIG's annual work plan for FY 2022. The memorandum report included two recommendations to further strengthen the GPC program.

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

Sentencing

In January, a Virginia exporter pleaded 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 altered 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. On May 12, 2021, the exporter was sentenced to 34 months imprisonment, followed by 60 months of supervised release, and ordered to pay restitution of $1.6 million.

Defendants Charged

The foreign buyer in an EXIM-insured transaction fell victim to a BEC scheme and was deceived into sending payments to a bank account unrelated to the insured exporter. The scheme caused the exporter to file a claim for payment with EXIM. Working with DHS, Homeland Security Investigations (HSI), EXIM agents identified an Atlanta, Georgia-based fraud ring responsible for this fraud, as well as numerous other frauds. On September 21, 2021, a grand jury in the Northern District of Georgia indicted four members of the ring and several days later, the United States Attorney's Office charged a fifth member by Information. The charges included wire fraud, money laundering, and conspiracy. Agents have made some arrests.

PRAC Task Force

Under a Memorandum of Understanding between EXIM OIG and CIGIE's PRAC, EXIM OIG has begun assisting the PRAC in carrying out its mission to promote transparency and conduct and support oversight of funds disbursed under the CARES Act. To this end, EXIM OIG agents are assisting the PRAC in three ongoing investigations of suspected fraud by participants in the Paycheck Protection Program (PPP).

EXIM Management Challenges

The Reports Consolidation Act of 2000 (Pub. Law No. 106-531) requires Inspectors General "to summarize the most serious management and performance challenges facing [their respective agencies] and briefly assess the agenc[ies'] progress in addressing those challenges." This requirement conforms with EXIM OIG's statutory authority to conduct audits, investigations, inspections, and evaluations to promote the economy, efficiency, and effectiveness of EXIM programs and operations.[1] These challenges identify areas necessitating continuing focus from EXIM management and represent overarching issues affecting the agency's operations, as well as its ability to manage risk. The following five topics represent EXIM OIG's perspective on the critical issues and challenges that may pose a risk to EXIM's ability to meet its mission efficiently and effectively.

Vacancies and Turnover

Since the presidential transition in January 2021, two of three Senate-confirmed EXIM Board members vacated their positions.[2] To address the vacancies, the President nominated Judith Pryor to serve as EXIM's First Vice President/Vice Chairman on July 19, 2021, and Reta Jo Lewis to serve as President/Chairman on September 13, 2021. Both nominations remain pending in the Senate. Consequently, the President authorized James Cruse to serve as Acting First Vice President/Acting Vice Chairman, and James Burrows, Jr. to serve as Acting President/Acting Chairman during the nominations' pendency.

Recent changes in EXIM's 2019 reauthorization[3] and the designation of acting personnel ensure that EXIM maintains a quorum when lacking Senate-confirmed Board members. Although these changes limit repercussions arising from a quorum absence, they do not eliminate other substantial impacts arising from key leadership vacancies. At least 21 positions were vacated during the presidential transition. In deference to the nominated President/Chairman, the agency has assigned acting personnel to some of these vacant positions until the nominee is confirmed, although others remain vacant pending confirmation. EXIM management identified a number of systemic challenges it has been encountering due to leadership vacancies, including but not limited to operational instability, diminished competitiveness with other ECAs, political uncertainty, and underutilized resources.[4]

The instability from turnover is further affected by the high proportion of EXIM personnel nearing retirement eligibility: currently, at least 42 percent of EXIM's workforce is eligible to retire within the next five years, more than half of whom are eligible to retire immediately. The wave of potential retirements, which may transpire more rapidly given evolving circumstances surrounding the pandemic, could deplete EXIM's institutional knowledge and may increase enterprise risk. Although EXIM purports to have improved its controls to reduce single points of

[1] *See* Inspector General Act of 1978, as amended (5 U.S.C. app. §§ 2, 4, 5 and 6).

[2] Chairman Kimberly Reed's term expired on January 20, 2021, and Judith Pryor's extended term expired on July 20, 2021. Spencer Bacchus continues to serve on EXIM's Board, with his term expiring on January 20, 2023. The remaining two Board positions were not confirmed during the prior administration, and have remained vacant since July 20, 2015.

[3] Further Consolidated Appropriations Act, 2020, Division I, Title VI, § 409 (Pub. L. No. 116-94) (Dec. 20, 2019).

[4] *Infra* Resource Management, p. 7.

failure, the small size of the agency makes it more susceptible to operational disruption caused by turnover.

High turnover and transition in leadership affect EXIM's ability to meet mission-critical objectives and statutory responsibilities, potentially resulting in a lack of operational continuity and indeterminate policy direction. EXIM has undertaken steps to maintain continuity among changes in administration, such as designating the Chief Management Officer as a career position. Given the comprehensive investment necessary to obtain EXIM financing, customers have purportedly explained that lack of political support in combination with uncertainty about the long-term viability of the agency have induced them to seek support from external ECAs. Consequently, EXIM OIG assesses vacancies and turnover will constitute major management challenges for EXIM.

Resource Management

Although challenges affecting EXIM's human capital remain ongoing from our prior years' reporting, EXIM OIG anticipates that broader concerns involving the agency's resource management will create more immediate challenges to EXIM. Specifically, implementing expanded statutory responsibilities with numerous vacancies will require EXIM to carefully target limited resources to ensure the agency adequately performs mission-critical functions.

In the 2019 reauthorization, Congress expanded EXIM's statutory responsibilities.[5] However, the funds appropriated to EXIM remained at the same level pre- and post-reauthorization. Although the administration requested an increase in appropriations to account for EXIM's additional responsibilities, Congress has not yet authorized such appropriations.

As previously reported, the lack of adequate, predictable funding and staffing can negatively affect an agency's ability to meet its performance goals and fulfill its mission. EXIM management reported that budgetary concerns have prevented EXIM from enacting effective long-term strategic planning. They also reported that the agency has had to utilize rollover funds to ensure continuity of operations, rendering those funds unavailable for other intended purposes. Consequently, managing the allocation of limited resources to fulfill EXIM's mission and support operations in light of increased demands may present significant management and performance challenges for EXIM.

Information Technology and Cybersecurity Challenges

Information technology (IT) and cybersecurity challenges involve the protection of federal IT systems from intrusion or compromise by external and/or internal entities, as well as the planning and acquisition of IT infrastructure. Such infrastructure is critical to operations because federal agencies rely on secure IT systems to perform mission-critical functions. Consequently, IT and cybersecurity are long-standing government-wide management challenges that persist in light of systemic impediments, such as resource constraints and a shortage of cybersecurity professionals. Further, these challenges have become more urgent as

[5] *Supra* n. 3 at §§ 402, 404, 407 and 408 (establishing China and Transformational Exports program to reserve 20 percent of EXIM's exposure cap for financing exports that compete directly with China or other countries; increasing the small business threshold to 30 percent beginning on January 1, 2021; and consulting with Department of State regarding the potential national interest impacts of financing in excess of $25 million for transactions where the end user, lender, or obligor is the government of China).

the government faces increased cyber threats, heightened federal requirements,[6] and transformational operations during the coronavirus pandemic.

Key areas of concern related to IT security and management include: safeguarding sensitive data and information systems, networks, and assets against cyberattacks and insider threats; modernizing and managing federal IT systems; ensuring continuity of operations; and recruiting and retaining a highly skilled cybersecurity workforce. As discussed in the prior fall semiannual report, implementing EXIM's Continuity of Operations plan continuously over long-term periods raised new technological and operational challenges, requiring EXIM to adapt its network to support a primarily virtual workforce and provide an unprecedented number of remote employees with a reliable means to access critical applications and data. These challenges will persist after EXIM staff return to the physical facilities, as the agency intends to implement expanded telework and remote work flexibilities to its staff. Accordingly, the risk still exists that EXIM IT infrastructure may become overtaxed, remote users conducting business outside of secure facilities may create additional targets for cyberattacks, and insider threats may become more prevalent. EXIM's IT staff have worked diligently to support the agency's virtual workforce and ensure continuity of operations for over a year, although in some areas, the effectiveness of the cybersecurity program could be improved.[7]

EXIM management reported that it anticipates major challenges to deploy sufficient financial resources and human capital necessary to meet the objectives raised by Executive Order 14028. A pervasive concern in IT and cybersecurity is the shortage of cybersecurity professionals. EXIM management identified that IT positions are highly competitive, which has resulted in hampered efforts to recruit and retain talented staff to the agency. EXIM management explained that long-term retention of IT staff was difficult because IT positions involve highly transferrable skills that are compensated at significantly higher levels in the private sector. Accordingly, competing for a limited number of IT professionals is anticipated to remain a significant management challenge for EXIM.

Operational Challenges Arising from the Coronavirus Pandemic

As discussed in last year's fall semiannual report, the coronavirus pandemic generated a number of unique challenges to federal agencies government-wide. Specific to EXIM, these challenges involved: (1) protecting employee health and safety; (2) maintaining operations and mission success; (3) cybersecurity; and (4) responding to increased fraud risk. Because the pandemic is still ongoing, those challenges continue to persist. *See* Notice on the Continuation of the National Emergency Concerning the Coronavirus Disease 2019 (COVID-19) Pandemic (Feb. 24, 2021) (extending the national emergency regarding the coronavirus pandemic). Further, these challenges could be exacerbated by budgetary uncertainty, given that EXIM must restrict resources to account for the continuing resolution that expires on December 3, 2021.

EXIM plans to return its workforce to physical facilities in several phases during FY 2022. Accordingly, EXIM OIG anticipates that protecting employee health and safety will constitute a significant management challenge as more employees commute and occupy the physical worksite. EXIM continues to make progress to promote employee health and safety,

[6] *E.g.,* Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021).

[7] OIG-AR-21-05, Audit of EXIM's Cybersecurity Program (Jul. 12, 2021).

implementing guidance from the Centers for Disease Control and Prevention (CDC) and Occupational Safety and Health Administration (OSHA) in its facilities management. Additionally, EXIM has been working to implement Executive Orders 14042 and 14043, as well as corresponding administrative guidance, that require federal contractors and federal employees to be fully vaccinated on or before November 22, 2021 (unless there is an exception required by law).

EXIM OIG anticipates that turnover may be more pronounced as employees return to the physical worksite. Colloquially referred to as the "Great Resignation," employers nationwide have experienced increased resignations of staff as a result of the pandemic, largely comprised of mid-career employees.[8] EXIM management reported that it has already encountered a loss of staff during the pandemic, which may increase when employees return to the physical worksite. In light of EXIM's systemic challenges regarding human capital,[9] specifically staff recruitment and retention, a substantial increase in turnover could negatively impact operations and mission-critical functions, especially as highly skilled staff are more likely to be among those who transfer to different employers. As identified above, EXIM's workforce composition may further exacerbate this issue; specifically, the agency's high percentage of retirement-eligible staff increases the likelihood of disruptive turnover.

The coronavirus pandemic has not only affected EXIM's administrative duties, but also impacts the agency's operational activities and its portfolio. Aviation finance, for example, was widely affected by the change in economic conditions as a result of the pandemic.[10] Similarly, the two percent default cap[11] that was enacted before the economic downturn remains in effect regardless of economic conditions. EXIM management reported that it was able to manage the effects of these conditions by restructuring deals and entering into hybrid agreements with customers when there was still a reasonable assurance of repayment. EXIM management also explained that customers adapted to the conditions, decreasing the risk of default. Some airlines, for example, converted passenger aircrafts to transport cargo. As explained in our prior year's fall semiannual report, however, the flexibilities and relief measures offered to EXIM customers during the pandemic may increase risk of identifying and/or addressing noncompliance. Thus, these challenges will require continued attention and vigilance by EXIM for the foreseeable future.

[8] *See*, *e.g.*, "Who is Driving the Great Resignation," https://hbr.org/2021/09/who-is-driving-the-great-resignation (Sep. 15, 2021); "The Great Resignation is Accelerating," https://www.theatlantic.com/ideas/archive/2021/10/great-resignation-accelerating/620382/ (Oct. 15, 2021).

[9] Semiannual Report to Congress, April 1, 2020 to September 30, 2020, Management Challenges, pp. 8-10.

[10] OIG-AR-21-01, Audit of the Export-Import Bank of the United States Fiscal Year 2020 Financial Statements (Nov. 13, 2020).

[11] 12 U.S.C. § 635e(a)(3).

Internal Controls

Management uses an internal control system to achieve the agency's objectives, navigate change, and manage risk. A strong internal control system provides stakeholders with reasonable assurance that operations are effective and efficient, that decision-makers use reliable information, and that the agency complies with applicable laws and regulations. We are pleased to report that EXIM continues to make significant progress in improving internal controls in the agency's programs and operations.

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 Inspection and Evaluation* (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 two audit reports and one memorandum:

- Independent Auditors' Report on EXIM's Compliance with the Payment Integrity Information Act of 2019 for FY 2020
- Audit of EXIM's Cybersecurity Program
- Risk Assessment of EXIM's Government Purchase Card Program

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

- Audit of EXIM's Service Contracts
- 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
- Audit of EXIM's Implementation of Key Provisions of the 2019 Reauthorization Act and Other Priorities

Reports Issued

Independent Auditors' Report on EXIM's Compliance with the Payment Integrity Information Act of 2019 for FY 2020

(OIG-AR-21-04, April 22, 2021)

Under a contract overseen by OAE, an independent accounting firm performed an audit to: (1) determine whether EXIM has met all the requirements of PIIA in the payment integrity section of its FY 2020 Annual Report and accompanying materials; and (2) assess the accuracy and completeness of the agency's improper payment reporting and efforts to prevent and reduce improper payments. In addition, EXIM's assessment of the level of risk and quality of improper payments and methodology for its four payment programs (short-term authorizations, medium-term authorizations, long-term authorizations, and cash-control disbursements) was evaluated.

For FY 2020, the independent accounting firm determined that EXIM's reporting complied with the annual reporting requirements of PIIA and was accurate and complete. The agency had taken adequate steps to prevent and reduce improper payments and none of the four payment programs exceeded the PIIA-determined threshold to be considered susceptible to significant

improper payments. Further, the audit did not identify a higher risk score nor any additional areas that should be considered by EXIM in its risk assessment process. Lastly, the independent accounting firm concluded that EXIM maintained adequate internal controls over the improper payment process. The audit report did not include recommendations.

Audit of EXIM's Cybersecurity Program

(OIG-AR-21-05, July 12, 2021)

We conducted an audit 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. We found that 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 the agency did not actively maintain training records per federally recommended guidelines. Specifically, EXIM needs to improve their (1) processes for ensuring IT systems are operating with the proper authorizations and (2) process for monitoring compliance and effectiveness of specialized training for cybersecurity staff. We made three recommendations in the audit report to improve the effectiveness of EXIM's cybersecurity program.

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

EXIM management concurred with the recommendations.

Risk Assessment of EXIM's Government Purchase Card Program

(OIG-O-21-02, September 30, 2021)

In accordance with the Charge Card Act, 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 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 2020 administrative expenditures and travel expenses were below the $10 million threshold for audit. Therefore, audits of the GPC and GTC programs will not be included in EXIM OIG's annual work plan for FY 2022. The memorandum report includes two recommendations for EXIM to ensure:

1. All purchase card holders and approvers timely complete required training.
2. The responsibilities of the AOPC and OMB requirements are fulfilled.

Ongoing Projects

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 awarded using GSA's Federal Supply Schedule and to determine compliance with the Federal Acquisition Regulation. The report will be issued in the semiannual reporting period ending March 31, 2022.

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: (1) 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.

Audit of EXIM's Implementation of Key Provisions of the 2019 Reauthorization Act and Other Priorities

The objective of this audit is to determine the extent to which EXIM has: (1) implemented key provisions of the 2019 Reauthorization Act; and (2) improved transparency and accountability. The report will be issued in the semiannual reporting period ending September 30, 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, or individuals who target EXIM programs and participants. 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 tables below.

Activity	Investigations
Open as of April 1, 2021	26
Opened during period	8
Closed during period	9
Open as of September 30, 2021	25

Of the 25 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	12
Loan Guarantee	3
Working Capital	4
Letter of Interest	2
Employee Integrity	0
Other (i.e., proactive investigations)	4

Investigative Results

OI undertook the following investigative actions during this reporting period:

Description	OIG	Joint Activities*	Total
Matters Referred for Prosecution Consideration	6	0	6
Matters Referred for State and Local Consideration	0	0	0
Criminal Indictments, Informations, Complaints	0	5	5
Guilty Pleas Entered	0	0	0
Criminal Judgments	1	0	1
Civil Actions	0	0	0
Civil Recoveries	0	0	0
Prison Time (months)	34	0	34
Probation (months)	60	0	60
Court Ordered Fines, Assessments, Restitutions, and Forfeitures	$1,600,000	0	$1,600,000
Administrative Actions**	0	0	0
Administrative Employee Actions***	0	0	0
Administrative Cost Savings and Repayments	0	0	0
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:

Exporter Sentenced for 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 wire fraud (18 U.S.C. § 1343) and one count of making false statements to a federally-insured bank (18 U.S.C. § 1014) 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 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. On May 12, 2021, Lee was sentenced to 34 months incarceration followed by 60 months supervised release. Lee was also ordered to pay $1.6 million in restitution to EXIM, as well as a $100 special assessment to the court.

Five Defendants Charged in Business Email Compromise Scheme (Export Credit Insurance)

In 2017, a Wisconsin-based exporter made a shipment to a Chinese buyer under an EXIM insurance policy. Shortly after, the buyer began receiving "spoofed" emails, or emails made to appear to be from the exporter. The emails directed the buyer to make payment for the goods to a bank account unrelated to the true exporter, which the buyer did. The scheme caused the exporter to file a claim for payment with EXIM. EXIM OIG agents identified several people believed to be associated with the fraud and learned that agents from DHS' HSI, were investigating a BEC ring involving the same suspects. On September 21, 2021, a grand jury in the Northern District of Georgia indicted four members of the Atlanta-based ring. On September 28, 2021, the United States Attorney's Office charged a fifth member in an Information. EXIM OIG and HSI agents have made some arrests. The charges against the five include wire fraud (18 U.S.C. § 1343), money laundering (18 U.S.C. § 1957), and money laundering conspiracy (18 U.S.C. § 1956).

Other Investigative Results

EXIM OIG has not yet seen a substantial increase in investigative cases related to COVID-19. However, we still anticipate that the number of suspicious transactions referred to OIG are likely to increase as a result of the financial pressure on foreign and domestic businesses due to the COVID-19 pandemic. This would be consistent with the substantial increase in financial fraud associated with the various COVID-19 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—have been 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 be detected in future years.

While the effects of COVID-19 are not yet prevalent in EXIM OIG's caseload, other investigative agencies have been overwhelmed by fraud directed at CARES Act programs. In January 2021, the PRAC stood up a Fraud Task Force to serve as a resource for the IG community by surging investigative resources into those areas where the need is the greatest. Currently, the need is greatest for assistance with pandemic loan fraud. Agents from OIGs across the government have been detailed to work on Task Force cases. These agents have partnered with prosecutors at DOJ's Fraud Section and at United States Attorneys' Offices across the country.

The PRAC Fraud Task Force harnesses the expertise of the oversight community and approaches pandemic-associated crimes with every tool investigators have: criminal penalties, civil penalties, forfeitures of money and property, suspensions and debarments. The Task Force

works closely with other initiatives, such as DOJ's COVID-19 Fraud Enforcement Task Force, to combat pandemic fraud.

In June 2021, EXIM OIG assigned three agents to the PRAC Fraud Task Force on a part-time basis. Currently, the agents are assigned PPP cases while continuing to work their existing caseload. This initiative allows EXIM OIG to make a broader contribution to the IG community by assisting with investigations that might otherwise remain temporarily unstaffed.

Intra and Inter-Agency Cooperation

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

When possible, OI shares intelligence with OGC concerning potential wrongdoing by entities which have applied for or held EXIM financial products. During the current reporting period, OI made 20 such referrals to OGC for enhanced due diligence by EXIM. These referrals did not involve ongoing OIG criminal investigations. Additionally, OI investigative analysts responded to over 530 deconfliction requests from the DHS' 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 four hotline reports during this semiannual reporting period. Two were resolved and closed by the hotline operator, one was referred to the agency for any action deemed appropriate, and one was referred to OAE as it involved an ongoing audit.

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, including OI's collaboration with the PRAC Fraud Task Force. 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 financial institutions with common fraud identifiers and increase awareness of how to report suspicious activity to the OIG.

Council of Inspectors General on Integrity and Efficiency

EXIM OIG participates in various 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 working group and other legal working groups. Through CIGIE, EXIM OIG continues to coordinate and collaborate with other OIG partners to use resources more efficiently, 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 (GAO) officials. GAO issued one report during the reporting period on the end-use monitoring of dual-use exports.

Export-Import Bank: Status of End-Use Monitoring of Dual-Use Exports as of August 2021

(GAO-21-105227, September 1, 2021)

GAO is required to report annually on the end uses of dual-use exports financed by EXIM during the second preceding fiscal year. This report reviewed EXIM's monitoring of dual-use exports that it continued to finance in FY 2019. Specifically, GAO examined: (1) the status of the agency's monitoring of dual-use exports that it continued to finance in FY 2019, as of August 2021; and (2) identified any new dual-use exports financed by the agency in FY 2020. GAO found that EXIM continued to monitor a single dual-use export transaction that it continued to finance in FY 2019—receiving all documents for the transaction on time and making the annual determination of compliance with the agency's dual-use policy. Further, GAO determined that EXIM did not finance any new exports under its dual-use authority in FY 2020.

APPENDIX A

Open Recommendations from Prior Reporting Periods

This table shows that 34 recommendations from eight reports issued up to March 31, 2021, remain open at the end of this reporting period. Fourteen open recommendations are from reports issued in FY 2021. The remaining 20 open recommendations are from reports issued in FYs 2017, 2019, and 2020. 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 (10/1/20 –3/31/21)						
Audits						
OIG-AR-21-02 13 Nov 2020	FY 2020 Financial Statements Audit Management Letter	8	8	0	0	11/15/2021
OIG-AR-21-03 4 Feb 2021	Independent Audit on the Effectiveness of EXIM's Information Security Program and Practices—FY 2020	6	6	0	0	2/4/2022
Prior Periods (prior to 10/1/20)						
Audits						
OIG-AR-20-01 8 Nov 2019	Independent Auditors' Report on EXIM Bank's Data Act Submission	14	14	0	0	9/30/2021
OIG-AR-20-06 30 Sep 2020	Audit of EXIM's Suspension and Debarment Program	2	1	1	0	9/30/2021
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	9/30/2021
OIG-EV-20-01 2 Dec 2019	Evaluation of EXIM's PRM Procedures and CRO Responsibilities	3	2	1	0	9/30/2021
	Total	53	34	19	0	

APPENDIX B

Audit and Evaluation Reports Issued from April 1, 2021 – September 30, 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-21-04 22 Apr 2021	Independent Auditor's Report on EXIM's Compliance with PIIA for FY 2020	0/0	0	0	0	0
2	OIG-AR-21-05 12 Jul 2021	Audit of EXIM's Cybersecurity Program	3/3	0	0	0	0
3	OIG-O-21-02 30 Sep 2021	Risk Assessment of EXIM's Government Purchase Card Program	2/2	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 September 30, 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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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	9/30/2021	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
Audit of EXIM's Cybersecurity Program (OIG-AR-05, July 12, 2021)						
1	Initiate coordination with responsible agencies to develop and document an alternative methodology.	Open	7/12/2022	Agree	0	0
2	Update policies to ensure that pertinent system documentation is recorded and readily accessible.	Open	7/12/2022	Agree	0	0
3	Implement an automated tracking mechanism designated to create, review, and maintain specialized security training records for all employees and contractors.	Open	7/12/2022	Agree	0	0
Risk Assessment of EXIM's Government Purchase Card Program (OIG-O-21-02, September 30, 2021)						
1	Ensure all purchase card holders and approvers timely complete required training.	Open	09/30/2022	Agree	0	0
2	Ensure the responsibilities of the AOPC and OMB requirements are fulfilled.	Open	09/30/2022	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 of 1978, 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 Federal Elections Commission OIG, whose report was issued on June 29, 2021. OAE 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.

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.

In FY 2022, OAE is scheduled to conduct a peer review of SIGTARP OIG's audit function and a peer review of FCC OIG's inspection and evaluation function. The planned completion of the peer reviews is December 2021 and March 2022, respectively.

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; 12-13
Section 5(a)(3)	Prior Significant Audit Recommendations Yet to Be Implemented	25
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	17
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	24
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	31
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	31; 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	17
Section 5(a)(18)	Metrics Used for Developing Data for Statistical Tables	17
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

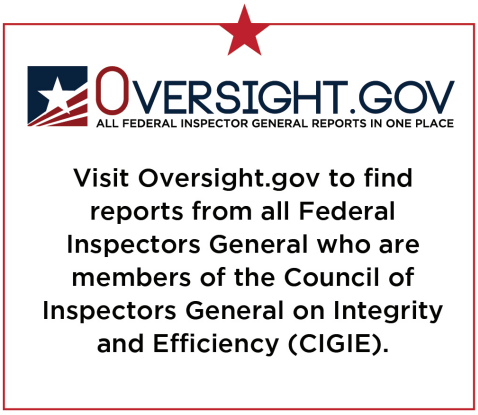
IGhotline@exim.gov

For information about EXIM OIG's Whistleblower Protection Coordinator, you may contact oig.whistleblower@exim.gov. For additional resources and information about whistleblower protections and unlawful retaliation, please visit the whistleblower's resource page at oversight.gov.

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).