United States Government Accountability Office

Report to Congressional Committees

May 2026

EXPORT-IMPORT BANK

Improved External Stakeholder Engagement Could Enhance Fraud Risk Management

GAO-26-108469

GAO Highlights

EXPORT-IMPORT BANK

Improved External Stakeholder Engagement Could Enhance Fraud Risk Management

GAO-26-108469 May 2026

A report to congressional committees

For more information, contact: Seto J. Bagdoyan at BagdoyanS@gao.gov

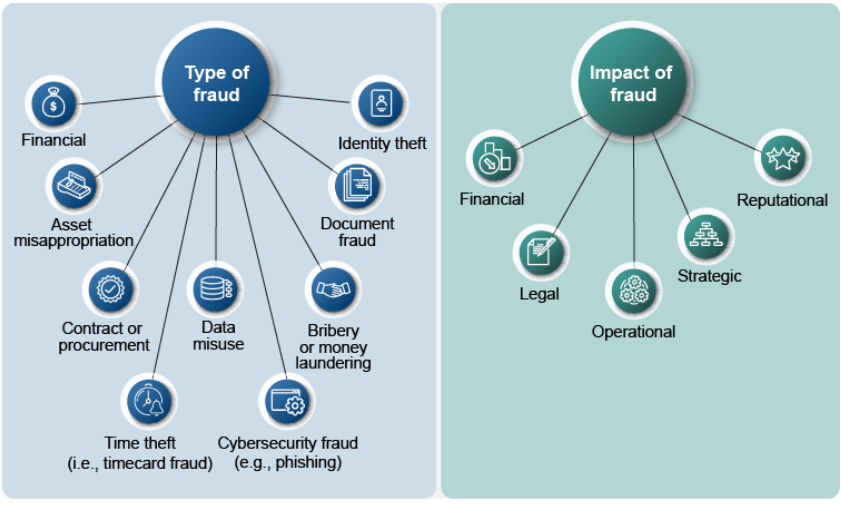
What GAO Found

The Export-Import Bank of the United States (EXIM) has generally monitored and evaluated the effectiveness of its fraud prevention activities in accordance with GAO's leading practices. For example, EXIM surveys internal stakeholders, such as program managers and loan officers, to evaluate its fraud risk assessments.

However, EXIM does not fully engage with external stakeholders to inform its fraud risk management activities, as called for in leading practices. EXIM works with external stakeholders, such as lenders and export credit insurance partners, to process transactions that carry EXIM's guarantees. These stakeholders have antifraud responsibilities, but EXIM does not involve them in its fraud risk assessment process. EXIM officials explained they do not think it is feasible to include these external stakeholders in the risk assessment process, or in the evaluation of those assessments, as there are many external stakeholders of varying sizes and types. By not engaging with external stakeholders, EXIM is not well positioned to fully understand the landscape of fraud risks and vulnerabilities facing the agency, such as risks posed by tariff evasion and the malicious use of artificial intelligence, therefore putting taxpayers at risk.

Further, EXIM collects information about potential fraud from internal loan officers to inform real-time monitoring efforts across its programs, but EXIM does not collect such information from external stakeholders (see fig. on the types and impacts of potential fraud at EXIM). According to leading practices, program managers should collect information from external stakeholders for real-time monitoring of fraud trends. By not collecting this information, EXIM is missing opportunities to proactively address fraud risks.

Types and Impacts of Potential Fraud at Export-Import Bank of the United States



Sources: GAO analysis of Export-Import Bank of the United States information and stas111/stock.adobe.com (images). | GAO-26-108469

GAO also reviewed EXIM transaction data from January 1, 2022, to June 30, 2025, to determine if entities that were banned from receiving federal assistance were present in the transaction data. GAO's analysis did not identify any excluded parties within the EXIM transaction data during that period.

Why GAO Did This Study

EXIM's mission is to support American jobs by facilitating the export of U.S. goods and services. Taxpayers could be responsible for losses arising from EXIM's operations, including losses due to fraud.

Congress included a provision in statute for GAO to periodically review EXIM's antifraud controls. This report assesses the extent to which (1) EXIM has monitored and evaluated its fraud risk management activities and engaged its stakeholders in the monitoring process; and (2) excluded parties can be identified in EXIM's transaction data from January 1, 2022, to June 30, 2025.

GAO reviewed EXIM's activities against relevant leading practices for fraud risk management identified by GAO, reviewed EXIM documentation, and interviewed EXIM managers and select external stakeholders responsible for fraud risk management. GAO selected external stakeholders to obtain a range of perspectives and based the selection on a variety of considerations including geographic location, asset size, the length of time associated with EXIM, and the number of active transactions. GAO also reviewed EXIM transaction data from January 1, 2022, to June 30, 2025.

What GAO Recommends

GAO is making four recommendations to EXIM, including the following three recommendations, to engage external stakeholders with its (1) fraud risk assessment process, (2) evaluation of assessments, and (3) collection and use of information on instances of potential fraud for its fraud risk monitoring effort. EXIM agreed with GAO's recommendations.

Contents

Figures

Abbreviations

CRTI	character, reputational, and transaction integrity
DAL	delegated authority lender
DNP	Do Not Pay portal
ECI	export credit insurer
EXIM	Export-Import Bank of the United States
Fraud Risk Framework	*A Framework for Managing Fraud Risks in Federal Programs*
FRO	Fraud Risk Oversight team
OFAC	Office of Foreign Assets Control
OGC	Office of the General Counsel
OIG	Office of Inspector General
SAM	System for Award Management
UEI	Unique Entity Identifier

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 19, 2026

Congressional Committees

The mission of the Export-Import Bank of the United States (EXIM) is to help support American jobs by facilitating the export of U.S. goods and services and financing imports.[1] To support these exports and imports, EXIM offers direct loans, loan guarantees, working capital loan guarantees, and export credit insurance. In fiscal year 2025, EXIM authorized $8.7 billion of loan guarantees, insurance, and direct loans to support an estimated $10.1 billion of U.S. export sales.[2] EXIM's obligations are backed by the full faith and credit of the U.S. government. As a result, U.S. taxpayers could be responsible for losses arising from EXIM's operations, including those due to fraud.

To continue its operations, EXIM requires periodic reauthorization from Congress. As part of the legislation that reauthorized EXIM in 2015, Congress included a provision for GAO to review the adequacy of the design and effectiveness of the controls used by EXIM to prevent, detect, and investigate fraudulent applications for loans and guarantees. The legislation also includes a provision for us to examine EXIM's compliance with the controls, including by auditing a sample of EXIM transactions within 4 years of reauthorization, and every 4 years thereafter.[3] Without reauthorization, EXIM's general statutory authority will end after December 31, 2026.[4]

The most recent legislation reauthorizing EXIM, enacted in December 2019, added an antifraud requirement to EXIM's consideration of

[1]EXIM is a wholly owned government corporation that serves as the export credit agency of the United States and, according to EXIM, it is intended to support financing and serve as a financier of last resort for U.S. companies that seek to sell and export their goods or services to foreign buyers and that cannot obtain private financing for their deals. EXIM is overseen by a Board of Directors, which has five members. The President of EXIM serves as the Board's Chair.

[2]Export-Import Bank of the United States, *Annual Management Report, A Subsection of the Annual Report for the Year Ended September 30, 2025,* (Jan. 2026).

[3]See 12 U.S.C. § 635a-6(b), as added by the Export-Import Bank Reform Reauthorization Act of 2015, Pub. L. No. 114-94, div. E, title LI, 129 Stat. 1763.

[4]The Further Consolidated Appropriations Act, 2020 (P.L. 116-94, Div. I, title IV, 133 Stat. 2534, 3021-26, enacted December 20, 2019), extended EXIM's general statutory authority for 7 years, through December 31, 2026.

applications for assistance.[5] Specifically, this legislation stated that EXIM shall deny an application for assistance if the end-user, borrower, lender, or exporter has been convicted of an act of fraud or corruption in connection with an application for support from EXIM made in the preceding 5 years.[6] The legislation further states that EXIM may proceed with an application if an end-user, borrower, lender, or exporter who might be subject to the antifraud requirement can be fully excluded from the transaction.[7] In addition, parties that are delinquent on debt owed to the federal government, other than debt owed to the Internal Revenue Service, are also prohibited from obtaining federal financial assistance, including EXIM transactions.[8]

As discussed in GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), effective fraud risk management helps to ensure that federal programs' services fulfill their intended purpose, funds are spent effectively, and assets are safeguarded.[9] Implementing a risk-based approach to addressing potential fraud in the federal government poses a unique set of challenges to federal managers, given their programs' mission to provide the public with a broad range of critical, often time-sensitive, services, and financial assistance. The Fraud Risk Framework describes leading practices for agency managers to use when developing activities to combat fraud in a strategic, risk-based way within four components: (1) commit, (2) assess, (3) design and implement, and (4) evaluate and adapt. For example, according to the Fraud Risk Framework, managers

[5]The Further Consolidated Appropriations Act, 2020 (P.L. 116-94, Div. I, title IV, 133 Stat. 2534, 3021-26, enacted December 20, 2019).

[6]According to EXIM, the end-user is the foreign entity that uses the U.S. goods and services. The borrower is the entity that agrees to repay the loan. The lender is the company that extends the EXIM-guaranteed or -insured loan to the borrower. The exporter is the U.S. entity that contracts with the buyer for the sale of the U.S. goods and services. In the case of a finance lease, if the lessor is a U.S. entity and takes title to the goods and services for lease to the foreign lessee, the lessor is the exporter.

[7]EXIM has compiled a convicted parties list pursuant to the procedures implementing Section 406 of the Export-Import Bank Reauthorization Act of 2019. Section 406 has been incorporated into the EXIM Charter under Section 2(f) (12 U.S.C. § 635(f)) and directs EXIM to deny applications for transactions in which certain parties have been convicted of fraud or corruption in connection with EXIM transactions.

[8]31 C.F.R. § 901.6. When appropriate, this provision may be waived by the head of an agency. 31 C.F.R. § 901.6(a).

[9]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

who effectively manage fraud risks develop and document an antifraud strategy that describes the program's approach for addressing the fraud risks identified during the fraud risk assessment. Program managers should also conduct ongoing monitoring. In addition, periodic evaluations provide assurances that they are effectively preventing, detecting, and responding to potential fraud.

This report is the fourth in a series in response to provisions in the 2015 EXIM reauthorization.[10] Specifically, this report focuses on EXIM's implementation of the fourth component of the Fraud Risk Framework. Specifically, the report assesses the extent to which (1) EXIM has monitored and evaluated its fraud risk management activities and engaged its stakeholders in the monitoring process and (2) excluded parties can be identified in EXIM's transaction data from January 1, 2022, to June 30, 2025.[11]

To assess the extent to which EXIM has monitored and evaluated its fraud risk management activities and engaged its stakeholders in the monitoring process, we analyzed EXIM documentation related to its antifraud efforts and interviewed EXIM officials responsible for their development. Specifically, we reviewed EXIM's fiscal year 2023 and fiscal year 2025 fraud risk assessments, its fraud risk profiles, and its fiscal year 2025 Antifraud Strategy.[12] We analyzed the extent to which these activities aligned with all leading practices in the Fraud Risk Framework's

[10]For our prior reports, see GAO, *Export-Import Bank: The Bank Needs to Continue to Improve Fraud Risk Management,* GAO-18-492 (Washington, D.C.: July 19, 2018); *Export-Import Bank: EXIM Should Explore Using Available Data to Identify Applicants with Delinquent Federal Debt,* GAO-19-337 (Washington, D.C.: May 23, 2019); and *Export-Import Bank: Additional Documentation about Stakeholder Roles and Clarity about Fraud Risks Would Strengthen Antifraud Efforts*, GAO-22-105340 (Washington, D.C.: Sept. 27, 2022).

[11]For this report, we define excluded parties as any entity listed on the U.S. Department of the Treasury's Office of Foreign Assets Control's (OFAC) sanctions list and the General Services Administration System for Award Management's (SAM) exclusion list. The entities on these lists are generally prohibited from doing business with U.S. persons or are excluded from receiving federal financial and nonfinancial assistance and benefits. For this review, we selected these dates to cover the most recent data available from when we began our work. Our prior report under this mandate reviewed EXIM transactions from January 1, 2020, to December 31, 2021.

[12]EXIM conducts a fraud risk assessment on a biennial basis.

fourth component.[13] We reviewed documentation and information from interviews with EXIM officials about efforts to evaluate outcomes, using a risk-based approach, and to adapt activities to improve fraud risk management.

We also interviewed 10 selected external stakeholders, Delegated Authority Lenders (DAL) and Export Credit Insurers (ECI), responsible for specific fraud risk management activities.[14] Although the findings of these interviews are not generalizable to all stakeholders, they provide illustrative examples of fraud risk management activities at EXIM and insight on EXIM's efforts to engage with, and communicate to, stakeholders in its monitoring and evaluation process. To obtain a range of external stakeholder types and perspectives, we selected DAL and ECI stakeholders based on a variety of considerations. These considerations included the geographic location of the stakeholder; the stakeholder's classification, as assigned by the Federal Deposit Insurance Corporation; asset size; tier rating, as assigned by EXIM; the length of time associated with EXIM; and the number of active loans or policies held by the stakeholder.

To assess the extent to which excluded parties can be identified in EXIM's transaction data from January 1, 2022, to June 30, 2025, we compared EXIM participant transaction data from January 1, 2022, through June 30, 2025, with federal excluded parties databases, using the U.S. Department of the Treasury's Bureau of the Fiscal Service's Do Not Pay portal (DNP) to identify applicants or participants that may have

[13]We assessed EXIM's activities and efforts against all 10 leading practices from the Fraud Risk Framework's fourth component. We determined that five of the 10 leading practices were relevant to our reporting objective based on a review of EXIM documents and discussions with EXIM managers responsible for fraud risk management. The five practices included in this report are (1) monitoring and evaluating the effectiveness of fraud prevention activities, (2) collecting and analyzing data for the real-time monitoring of fraud trends, (3) engaging stakeholders responsible for fraud risk management in the monitoring and evaluation process, (4) using the results of monitoring and evaluation to improve fraud risk management activities, and (5) communicating the results of monitoring and evaluations to relevant stakeholders. GAO-15-593SP.

[14]EXIM works with external, commercial lenders to fulfill its mission. EXIM's products handled by Delegated Authority Lenders (DAL) carry the same EXIM guarantees as EXIM's own offerings. Export Credit Insurers (ECI) brokers may represent and assist insured parties in the ECI program. According to EXIM's antifraud strategy, DALs and ECIs have fraud risk management responsibilities, which is a key fraud risk control.

not been appropriately denied.[15] We did not review the extent to which participants within EXIM's convicted parties list were present in its participant transaction data because, as of January 2026, there were no entities on Part 1 of the convicted parties list.[16]

We assessed the reliability of EXIM's participant transaction data by performing electronic testing on specific data elements, reviewing related documents, and interviewing knowledgeable officials responsible for the data and related information systems. We determined that the data we used in our analysis were sufficiently reliable for the purposes of our reporting objective. For more information about our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from May 2025 to May 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

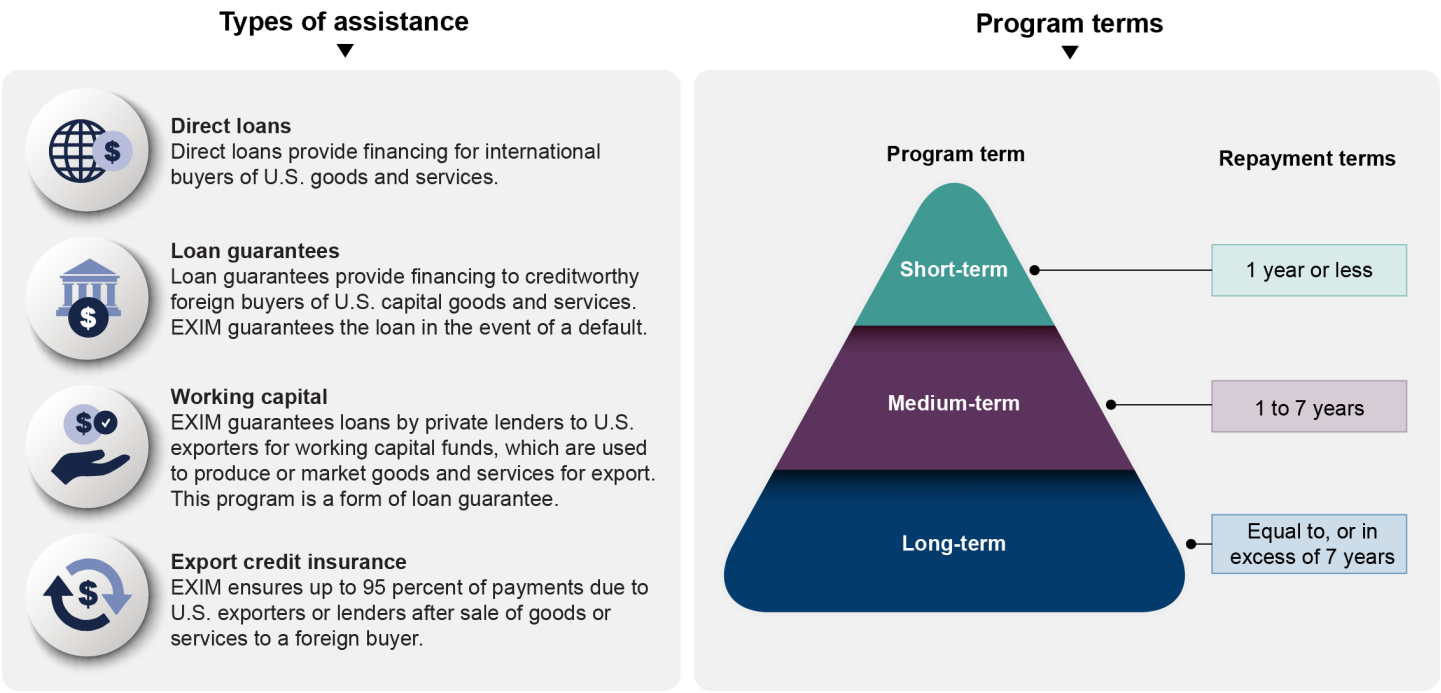
EXIM offers four types of financing: direct loans, loan guarantees, working capital guarantees, and export-credit insurance. EXIM products generally have three maturity periods: short-term transactions are for 1 year or less;

[15]DNP is a data search system, hosted and administered by the U.S. Department of the Treasury's Bureau of the Fiscal Service. It compares the data submitted by an agency with several federal debarment lists. Agencies can use DNP to screen participants for possible improper payments. DNP is also a data-matching service for agencies to use in preventing payments to ineligible individuals, such as those who are deceased.

[16]EXIM has compiled a convicted parties list pursuant to the procedures implementing Section 406 of the Export-Import Bank Reauthorization Act of 2019. Section 406 has been incorporated into the EXIM Charter under Section 2(f) (12 U.S.C. § 635(f)) and directs EXIM to deny applications for transactions in which certain parties have been convicted for fraud or corruption in connection with EXIM transactions. We reported in 2022 that EXIM created the convicted parties list, which has two parts. Part 1 lists those individuals and companies that meet the Section 406 definition of having been convicted "in connection with an application made in the preceding 5 years." EXIM designed a broader scope for Part 2 of the convicted parties list based on what it believed was the intent of the Section 406 antifraud requirement. See GAO-22-105340. As of January 5, 2026, there were four entities on Part 2 of the convicted parties list. However, we did not include Part 2 entities in our review because they are not necessarily excluded from doing business with EXIM. According to EXIM, parties on Part 2 of the list are not necessarily excluded from EXIM transactions, but they must get EXIM's express written permission before proceeding with an EXIM-supported transaction in which any individual or company listed on Part 2 is a buyer, borrower, end-user, lender, or exporter.

medium-term transactions are from 1 to 7 years long; and long-term transactions are equal to, or in excess of, 7 years. See figure 1.

Figure 1: Export-Import Bank of the United States (EXIM) Financing Programs and Program Terms



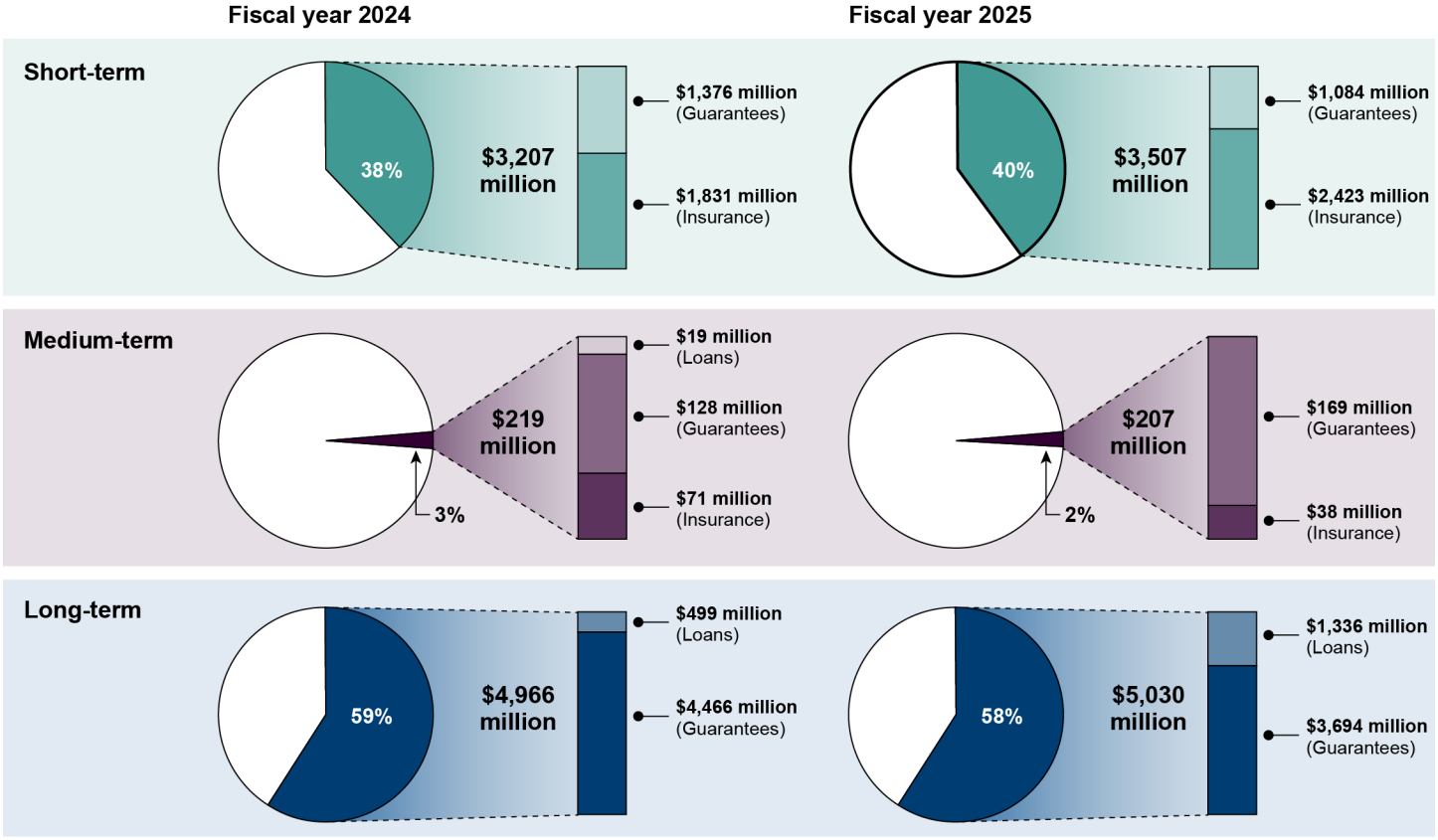
Source: GAO analysis of Export-Import Bank of the United States information. | GAO-26-108469

EXIM works with external, commercial lenders to fulfill its mission. For instance, EXIM's products handled by DALs carry the same EXIM guarantees as EXIM's own offerings. DAL transactions can be found within EXIM's loan guarantee and working capital programs. DAL transactions rely on underwriting that is conducted by these outside lenders. In fiscal year 2025, DAL transactions comprised about 6 percent of EXIM's transactions.

Additionally, EXIM's ECI program supports U.S. exporters by insuring them to reduce the risk of a foreign buyer or other foreign debtor default for political or commercial reasons, such as military conflict or bankruptcy. This risk protection permits exporters to extend credit to their international customers where it would otherwise not be possible. In fiscal year 2025, ECI transactions comprised about 85 percent of EXIM's transactions.

In fiscal year 2025, EXIM authorized $8.7 billion of loan guarantees, insurance, and direct loans to support an estimated $10.1 billion of U.S. export sales. See figure 2 for fiscal years 2024 and 2025 authorizations by term and by program.[17]

Figure 2: Export-Import Bank of the United States Authorizations, by Term and Program, for Fiscal Years 2024 and 2025



Source: GAO analysis of Export-Import Bank of the United States data. | GAO-26-108469

Fraud Risk Management

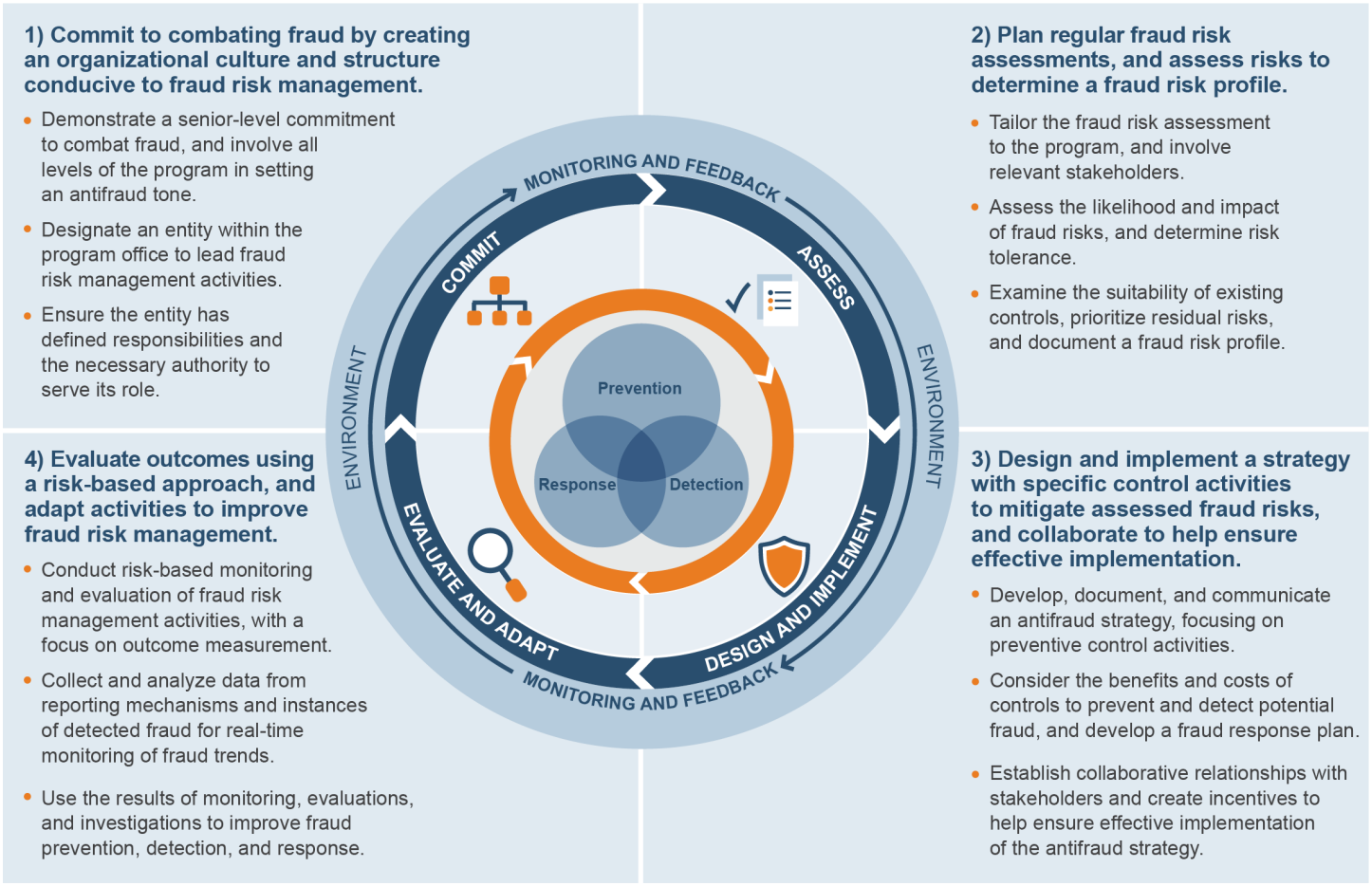
Fraud and fraud risk are distinct concepts. Fraud—obtaining something of value through willful misrepresentation—is challenging to detect because of its deceptive nature. Fraud risk (which is a function of likelihood and impact) exists when people have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or are able to rationalize committing fraud. Fraud risk management is a process

[17]See app. II for the top five countries that received support from EXIM in fiscal year 2025.

for ensuring program integrity by mitigating the likelihood and impact of fraud. When fraud risks can be identified and mitigated, fraud may be less likely to occur. Although the occurrence of fraud indicates there is a fraud risk, a fraud risk can exist, even if actual fraud has not yet been identified or occurred.

Executive branch agency managers, including those at EXIM, are responsible for managing fraud risks and implementing practices for combating those risks. In July 2015, we issued the Fraud Risk Framework, which provides a comprehensive set of key components and leading practices that serve as a guide for agency managers to use when developing efforts to combat fraud in a strategic, risk-based way. As depicted in figure 3, the Fraud Risk Framework describes leading practices within four components: (1) commit, (2) assess, (3) design and implement, and (4) evaluate and adapt.

Figure 3: The Four Components of the Fraud Risk Framework, and Selected Leading Practices



Source: GAO. | GAO-26-108469

The fourth component—evaluate and adapt—calls for federal managers to evaluate outcomes using a risk-based approach to improve fraud risk management.[18] Ongoing monitoring and periodic evaluations provide assurances to managers that they are effectively preventing, detecting, and responding to potential fraud. Monitoring and evaluation activities can also support managers' decisions about allocating resources and help

[18]To assist program managers with implementing component four of the Fraud Risk Framework, we developed a technical appendix, which supplements and complements the Fraud Risk Framework. See GAO, *Combating Fraud: Approaches to Evaluate Effectiveness and Demonstrate Integrity*, GAO-26-107609 (Washington, D.C.: Jan. 14, 2026).

them to demonstrate their commitment to effectively managing fraud risks.

Effective managers assess activities related to all components of the Fraud Risk Framework and not just control activities built into operational processes, such as system edit checks. Specifically, managers should monitor and evaluate the effectiveness of preventive activities, including fraud risk assessments and the antifraud strategy, as well as controls to detect fraud and response efforts. Effective managers of fraud risks use the results of monitoring and evaluations to improve the design and implementation of fraud risk management activities. They also communicate lessons learned from fraud risk management activities and corrective actions taken, if any, to relevant stakeholders. Communicating the results of monitoring activities and evaluations can promote collaboration across the organization.

Prior GAO Reports on EXIM Fraud Risk Management

We have reviewed EXIM's fraud risk management efforts under provisions in the 2015 reauthorization in three prior reports. Across those three reports, we made 11 recommendations to improve EXIM's fraud risk management. EXIM has implemented all 11 recommendations.[19]

In 2018, we issued our first report on EXIM's fraud risk management efforts.[20] We found that EXIM had identified a dedicated antifraud entity to lead the fraud risk management efforts, as described within the first component of the Fraud Risk Framework, and that EXIM managers and staff generally held positive views of EXIM's antifraud culture, even though their points of view on that culture differed. However, we also found that EXIM had not conducted a comprehensive fraud risk assessment, as described in the second component of the framework. We made seven recommendations for EXIM to improve its fraud risk management activities.

In 2019, we issued our second report.[21] We found that EXIM had antifraud controls in place for mitigating the fraud risks that we had previously identified and communicated to EXIM officials. We made two recommendations to EXIM that EXIM should assess and document the practicality of incorporating into its preauthorization and postauthorization

[19]See app. III for a listing of these fraud risk management recommendations.

[20]GAO-18-492.

[21]GAO-19-337.

character, reputational, and transaction integrity (CRTI) reviews searches for delinquent federal debts owed by applicants. These searches should, if practical, implement relevant approaches, such as manual searches or batch matching.

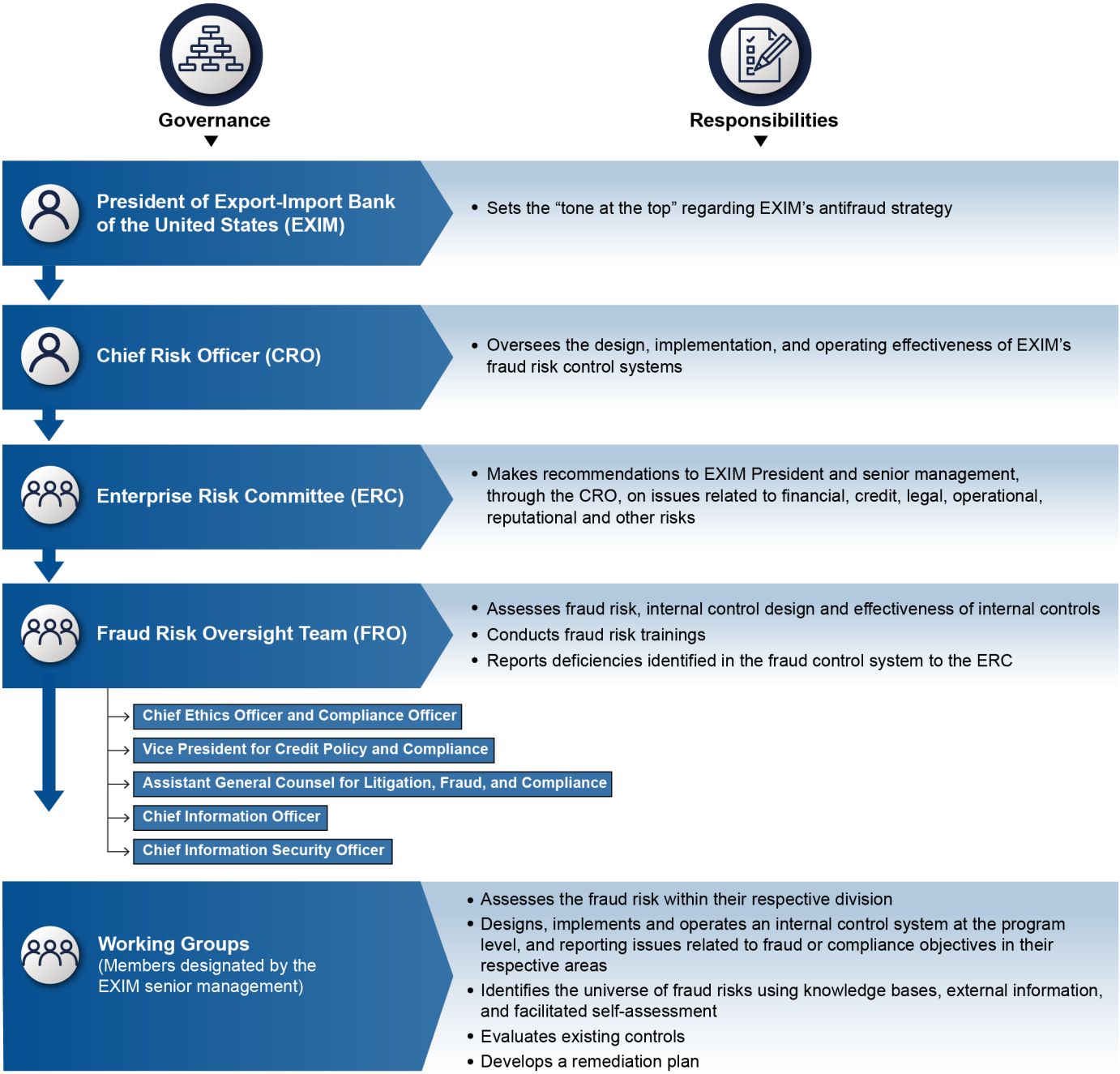
In 2022, we issued our third report.[22] We found that EXIM had developed an antifraud strategy, as described in the third component of the Fraud Risk Framework, but it had not used this strategy to address residual fraud risks. We also found that EXIM had not documented the roles and responsibilities external stakeholders would play in enforcing antifraud efforts. We made two recommendations to EXIM to update its antifraud strategy to address residual fraud risks and to document the roles and responsibilities of its external stakeholders.

EXIM's Fraud Risk Management Roles and Responsibilities

EXIM has taken steps to manage fraud, as described within the first three components of the Fraud Risk Framework. For example, in 2018, EXIM designated an entity, the Fraud Risk Oversight team (FRO), to lead EXIM's fraud risk management activities. The FRO's roles and responsibilities related to managing and assessing fraud risk have not changed since 2019, according to EXIM officials. According to EXIM's antifraud strategy, the FRO is responsible for assessing overall fraud risk, along with EXIM's internal control design, fraud risk training, and the effectiveness of its internal controls. Since 2019, the FRO has expanded to include the Chief Information Officer, the Chief Information Security Officer, and the Chief Compliance Officer, according to officials. Figure 4 illustrates the roles and responsibilities of the FRO and other EXIM entities for fraud risk management, as documented within the antifraud strategy.

[22]GAO-22-105340.

Figure 4: Roles and Responsibilities for Fraud Risk Management at the Export-Import Bank of the United States

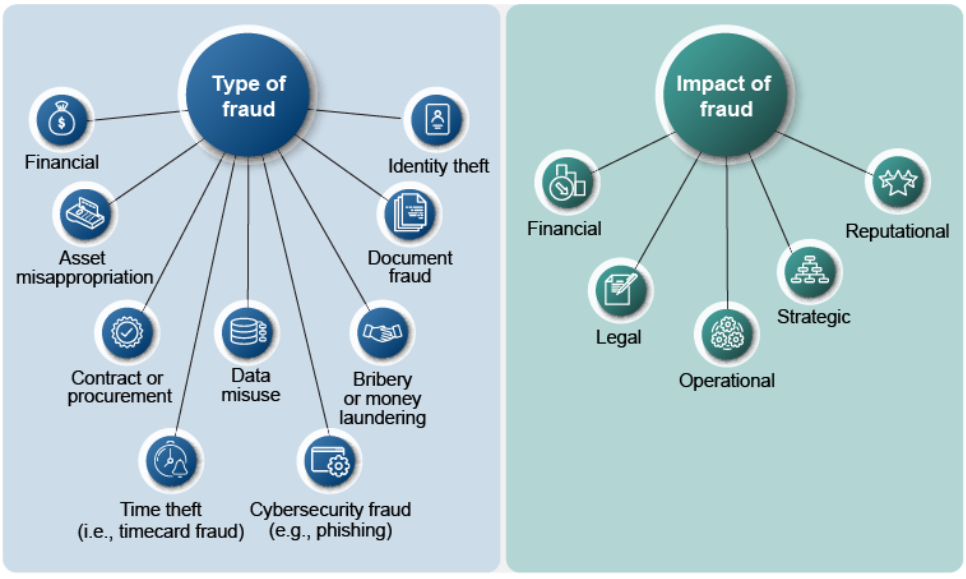


Source: GAO analysis of Export-Import Bank of the United States (information); and stas111/stock.adobe.com (images). | GAO-26-108469

The FRO also oversees EXIM's biennial fraud risk assessment process, which includes working groups designated by EXIM senior management. EXIM conducted fraud risk assessments for fiscal years 2019, 2021, 2023, and 2025. According to EXIM's antifraud strategy and EXIM's fraud risk assessment documentation, EXIM created nine working groups, made up of key personnel from EXIM's business offices, to assess fraud risks at EXIM.

EXIM's fraud working groups are comprised of a variety of EXIM staff, including loan officers, contracting officers, Treasury officials, and other EXIM functions, according to officials. According to EXIM's antifraud strategy, EXIM maintains working groups that are directly responsible for assessing the fraud risk within their respective EXIM divisions; designing, implementing, and operating an internal control system at the program level; and reporting issues related to fraud or compliance objectives in their respective areas. Key activities of the working groups include identifying fraud risks using knowledge bases and external information, assessing fraud risks, and evaluating existing controls. Working group team members consist of a cross-functional representation of EXIM to ensure that all key fraud risks are identified across EXIM, according to the strategy. Figure 5 shows the types and impacts of potential fraud that EXIM has identified.

Figure 5: Types and Impacts of Potential Fraud Identified by the Export-Import Bank of the United States



Sources: GAO analysis of Export-Import Bank of the United States (information); stas111/stock.adobe.com (icons). | GAO-26-108469

Following the fiscal year 2023 and fiscal year 2025 fraud risk assessments, EXIM documented a fraud risk profile for the organization.[23] In response to our July 2018 recommendation, EXIM developed an antifraud strategy in 2019 after its fiscal year 2019 fraud risk assessment.

The purpose and objective of EXIM's antifraud strategy is to provide a formal process to assist EXIM in systematically managing fraud risks and identifying vulnerabilities both inside and outside of EXIM. EXIM maintains the antifraud strategy in 2025, according to officials. The antifraud strategy states it will be updated on an ongoing basis to reflect dynamic conditions and the organization's continuing commitment to the fraud risk management program.

The Antifraud Strategy

Once managers have determined their risk responses, it is a leading practice for them to document an antifraud strategy based on the fraud risk profile.

The antifraud strategy describes existing fraud control activities, as well as any new control activities a program may adopt to address residual fraud risks. The antifraud strategy may be agency-wide or directed at the individual program level.

Effective antifraud strategies reflect the leading practices: Who is responsible for fraud risk management activities, what is the program doing to manage fraud risk, when is the program implementing fraud risk management activities, where is the program focusing its fraud risk management activities, and why is fraud risk management important.

Source: GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015). | GAO-26-108469

[23]As described in the Fraud Risk Framework, the fraud risk profile involves documenting the key findings and conclusions from the identification of fraud risks affecting the program and the assessment of the likelihood and impact of inherent fraud risks, including the risk tolerance and the prioritization of risks. The fraud risk profile is an essential piece of the overall antifraud strategy and informs the specific control activities that managers design and implement within the antifraud strategy.

EXIM Takes Various Actions to Monitor and Evaluate Its Fraud Risk Management Activities but Should More Fully Engage Its External Stakeholders to Inform These Activities

EXIM generally monitors and evaluates the effectiveness of its preventative activities, such as its fraud risk assessment and antifraud strategy, consistent with leading practices. However, we found that EXIM has opportunities to more fully adhere to leading practices by (1) engaging external stakeholders responsible for specific fraud risk management activities within its evaluation of its fraud risk assessment process, (2) involving external stakeholders within its fraud risk assessment process, (3) collecting and using information about potential fraud from external stakeholders to inform real-time monitoring trends, and (4) communicating the results of its monitoring and evaluations to external stakeholders.

EXIM's Fraud Risk Oversight Entity Uses Various Approaches to Monitor and Evaluate Its Fraud Risk Management Activities

Fraud Risk Framework Component:
Evaluate outcomes using a risk-based approach, and adapt activities to improve fraud risk management

Source: GAO. | GAO-26-108469

EXIM's efforts to monitor and evaluate the effectiveness of its preventive activities generally align with the leading practices in the fourth component of the Fraud Risk Framework. This component—evaluate and adapt—calls for federal managers to evaluate outcomes using a risk-based approach and to adapt activities to improve fraud risk management. [24] Specifically, one of the leading practices within this component states that managers should monitor and evaluate the effectiveness of its preventive activities, including fraud risk assessments and the antifraud strategy, as well as controls to detect fraud and response efforts.

One way that EXIM monitors and evaluates the effectiveness of its antifraud controls is by reviewing the number of suspicious activity fraud referrals, which are made to the EXIM Office of Inspector General

[24] GAO-15-593SP.

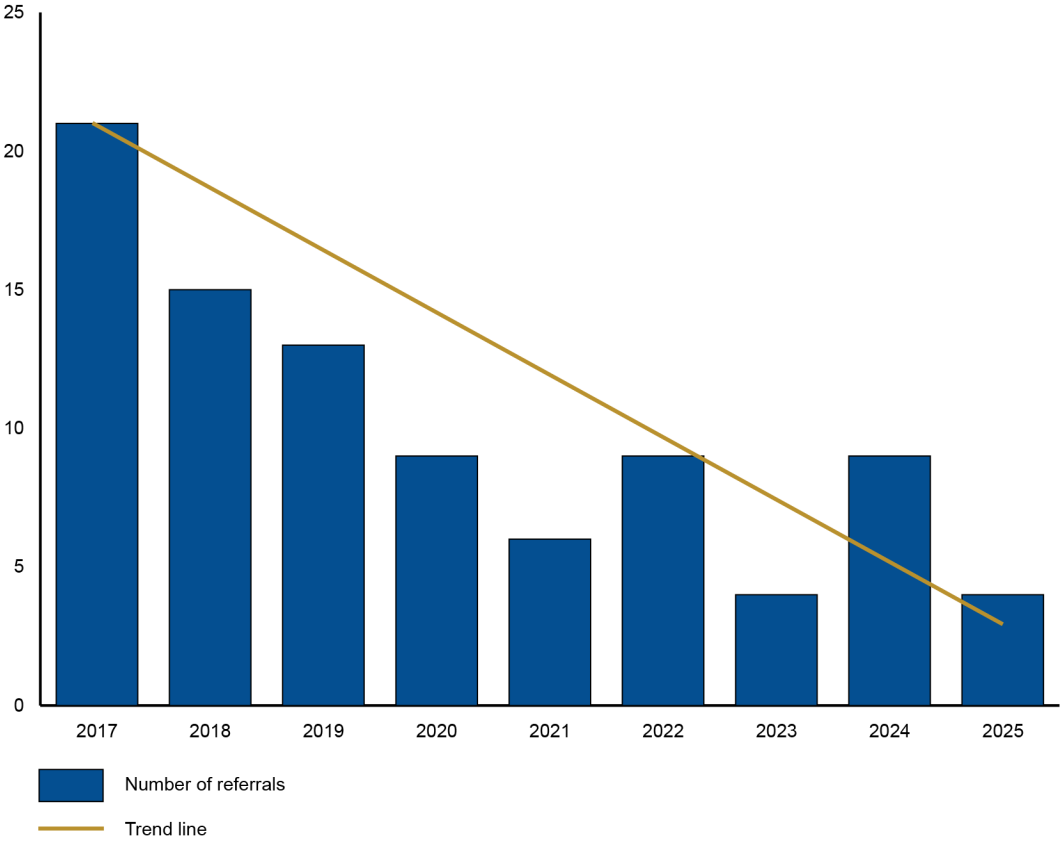
(OIG).[25] As described in EXIM's antifraud strategy, EXIM's Office of General Counsel's (OGC) Litigation, Fraud, and Compliance group maintains a log of EXIM's suspicious activity fraud referrals.[26] This log tracks the outcomes of such referrals and is used for analytical purposes, such as reviewing fraud risk trends and the effectiveness of EXIM's antifraud controls, according to the antifraud strategy. EXIM officials told us the FRO takes the information from the suspicious activity fraud referral that is shared with the OIG and OGC to evaluate the effectiveness of its antifraud controls, and the OIG investigates the referral. According to officials, if it is determined that fraud may have been committed, EXIM may pursue additional measures, as appropriate, including adjustments to its antifraud controls, suspension and debarment, referral to civil litigation, or criminal prosecution.

EXIM officials stated that they think their controls have been effective because the number of suspicious activity fraud referrals is low and has not materially increased over the years. We reviewed EXIM's suspicious activity fraud referral log from fiscal years 2017 through 2025. See figure 6 for the number of suspicious activity fraud referrals from fiscal years 2017 through 2025.

[25]The number of suspicious activity fraud referrals is based on what is reported by EXIM employees, according to EXIM officials. This number does not include the undetected fraudulent activity that may have occurred but was missed by employees.

[26]According to EXIM officials, prior to March 13, 2024, EXIM employees would typically email fraud referrals to the OGC and copy the OIG on the email. On March 13, 2024, the OIG requested that employees notify the OIG directly about suspected fraud, waste, abuse, or mismanagement at EXIM via an electronic submission form, according to EXIM officials. Therefore, EXIM officials told us that OGC no longer receives employee fraud referral emails, because such referrals are now submitted via a web-based electronic submission form, which does not provide a mechanism to copy or notify OGC. As of around March 13, 2024, the suspicious activity fraud referral log reflects only those referrals that the EXIM OGC is aware of, according to EXIM officials. EXIM receives information on fraud referrals from EXIM's OIG, according to EXIM officials.

Figure 6: Export-Import Bank of the United States Suspicious Activity Referrals, from Fiscal Years 2017 Through 2025



Sources: GAO analysis of Export-Import Bank of the United States information. | GAO-26-108469

EXIM officials provided an example of how their antifraud controls halted a suspicious transaction. Specifically, officials told us they were able to stop a transaction in fiscal year 2023 from moving forward because an employee conducted a credit compliance review during the application review process. During the review, the employee noted discrepancies within the application documents and typos in the financial statements. The transaction was withdrawn because of the discrepancies, according to officials.

EXIM also has activities to evaluate the effectiveness of its fraud risk assessment. For instance, EXIM conducts a fraud risk survey in the years between EXIM's biennial fraud risk assessments to evaluate its fraud risk assessment process. This survey assesses whether there have been any

changes to EXIM's fraud risk factors or controls to determine if any immediate action is needed or if there should be adjustments to the following year's fraud risk assessment. EXIM surveys internal stakeholders, according to our review of the survey. The fiscal year 2024 fraud risk survey noted fraud risk trends associated with using artificial intelligence, launching new EXIM business products, and continuing human resource capacity issues.[27] Based on the fiscal year 2024 fraud risk survey results, EXIM officials did not determine any need for immediate actions regarding its antifraud controls. Similarly, our review of the results did not identify the need for immediate action.

In addition, EXIM's antifraud strategy outlines its monitoring and evaluation activities. These activities are performed by the FRO, together with the Chief Risk Officer. The antifraud strategy is updated on an ongoing basis to reflect dynamic conditions and the organization's continuing commitment to the fraud risk management program, and ongoing monitoring will occur during regular operations. The scope and frequency will depend on the fraud risk assessment results and the effectiveness of monitoring procedures. Information regarding the implementation of the antifraud strategy is provided to the members of the Enterprise Risk Committee on a regular basis, according to our review of the strategy.

Further, EXIM used a consultant to evaluate the effectiveness of its enterprise risk management activities and provide recommendations, if needed, to improve its efforts. The external consultant's May 2025 report reviewed EXIM's risk management activities and did not provide any recommendations for improvement.

[27]EXIM's OIG has reported on management challenges that are significant risks to EXIM and its ability to execute the mission. For example, EXIM faces challenges filling key positions within EXIM and recruiting the talent necessary to improve EXIM's performance and competitiveness, according to the OIG. The OIG reported that EXIM continued to experience high attrition in senior positions during fiscal year 2024. Between 2022 and 2023, the OIG reported that employee attrition increased from 13 percent to 17 percent–reflecting the highest annual percentage over the 6-year period from 2018 to 2023. In addition, as of September 2024, nearly a quarter of EXIM's workforce is retirement eligible–a figure expected to rise to 38 percent of the workforce in the next 5 years, according to the OIG. The OIG determined that the management challenges identified in fiscal year 2024 remained the management challenges in fiscal year 2025. Export-Import Bank of the United States, Office of Inspector General, *Fiscal Year 2024: Major Management Challenges*, OIG-O-24-12 (Washington, D.C.: Sept. 2024); and *Fiscal Year 2025: Major Management Challenges,* OIG-O-25-08 (Washington, D.C.: Sept. 2025).

EXIM Does Not Fully Engage Its External Stakeholders in Its Fraud Risk Management Activities

EXIM's DAL and ECI stakeholders have antifraud responsibilities that EXIM documented within its antifraud strategy, as a result of our 2022 recommendation. However, contrary to leading practices, EXIM does not (1) engage these stakeholders within the evaluation of its fraud risk assessment process, (2) involve these stakeholders within its fraud risk assessment process, (3) collect and use information about potential fraud from external stakeholders to inform its monitoring activities, and (4) communicate the results of its monitoring activities to its external stakeholders.

EXIM Does Not Engage External Stakeholders in Fraud Risk Assessment Evaluation or the Fraud Risk Assessment Process

The Fraud Risk Framework states that program managers should engage stakeholders responsible for specific fraud risk management activities in the monitoring and evaluation process.[28] For instance, external stakeholders can aid managers in monitoring the effectiveness of control activities they implement or directly oversee. Managers should consider using ongoing monitoring, separate evaluations, or a combination of the two to obtain reasonable assurance of the operating effectiveness of the service organization's internal controls over the assigned process, according to the Fraud Risk Framework.

EXIM monitors and evaluates the effectiveness of its fraud risk assessment by surveying internal stakeholders responsible for fraud controls, such as loan officers and program managers, in between the years that it conducts a fraud risk assessment. For instance, this means that in between the assessments that EXIM conducted in fiscal years 2023 and 2025, it conducted a survey in fiscal year 2024.

EXIM's fraud risk survey asks respondents about its antifraud controls and emerging risk factors. For instance, the fiscal year 2024 survey included questions such as on the monitoring of antifraud controls and the emergence of risk factors not covered in the prior year's assessment.

EXIM's evaluative activity of its fraud risk assessments does not engage external stakeholders, even though EXIM's external stakeholders, such as the DAL and ECI, are responsible for specific antifraud controls. Additionally, we found that EXIM does not involve external stakeholders within its fraud risk assessment process, which is a leading practice from the second component of the Fraud Risk Framework.

[28]GAO-15-593SP.

Specifically, the second component of the Fraud Risk Framework states that managers should involve relevant stakeholders in the assessment process, including individuals responsible for designing and implementing fraud controls.[29] This should include external stakeholders with responsibilities for specific control activities or knowledge about emerging fraud risks. In addition, according to EXIM's antifraud strategy, a key activity of the fraud risk assessment working group is to identify the universe of fraud risks, using external information.

EXIM does not include DAL and ECI stakeholders within its fraud risk assessment process, such as its working groups, or in its assessment of its antifraud controls. However, these stakeholders comprised over 90 percent of EXIM's transactions in fiscal year 2025 and have antifraud responsibilities. None of the 10 external stakeholders we interviewed told us they had been invited to participate within EXIM's fraud risk assessment process.

In 2022, we found that EXIM's external stakeholders, such as the DAL and ECI stakeholders, have antifraud responsibilities, but they were not documented as part of EXIM's antifraud strategy.[30] In response to our recommendation, EXIM revised its antifraud strategy by outlining the roles and responsibilities of the external parties, specifically DAL and ECI parties, responsible for fraud controls. For example, EXIM documented within its strategy the DAL and ECI partners' fraud risk management and due diligence responsibilities when reviewing the participant and the transaction.[31] By taking that step, EXIM helped ensure that the roles and responsibilities related to fraud risk management were clearly understood by all parties involved in fraud risk management.

External stakeholders also have experience combating potential fraud while working with businesses and may have knowledge of emerging

[29]GAO-15-593SP.

[30]GAO-22-105340.

[31]We have previously reported that external parties conduct "Know Your Customer" due diligence on buyers, obligors, end-users, exporters, lenders, agents, and other major transaction parties, according to EXIM. Due diligence is conducted on transaction participants and on the transaction itself. Due diligence on transaction participants includes the review of credit and financial history, character, professional experience, and reputation. Due diligence on the transaction includes the review of all matters that may affect the likelihood of timely repayment, such as information about the goods and services being financed and related contracts and may include a review of financial projections. GAO-22-105340.

fraud. For instance, all 10 external stakeholders we interviewed told us they had experience offering EXIM's products to businesses or companies as a stakeholder for EXIM. External stakeholders could also provide information that could be useful to EXIM. For example, one external stakeholder told us they were paying more attention to tariff evasion, given current trade policies. Another stakeholder told us they adapted their antifraud controls to respond to emerging technology, such as artificial intelligence.

EXIM officials explained why they did not engage these stakeholders within the evaluation of its fraud risk assessment or involve them in the fraud risk assessment process. First, officials told us that the monitoring and evaluative activity of surveying stakeholders responsible for fraud controls is internal to EXIM personnel and that they do not intend to direct the fraud risk survey to external stakeholders. Second, when asked why external stakeholders were not included in the fraud risk assessment process, EXIM officials explained that fraud risk assessment working groups are focused on its internal controls, and they expect external stakeholders to adhere to their own due diligence standards and internal controls. In addition, officials stated that, given the many external stakeholders of varying sizes and types, they do not think it is feasible to direct the fraud risk survey to DAL and ECI stakeholders or involve them in the fraud risk assessment process.

EXIM has the information needed to survey external stakeholders that have insights into emerging risks and adapting antifraud controls. For example, EXIM maintains an email listserv to disseminate information to DAL and ECI stakeholders and could use this listserv to send the survey to external stakeholders. External stakeholders may also have insights into emerging risks and adapting antifraud controls. For example, one stakeholder described antifraud controls it has adapted over time to mitigate against false documentation. Further, while EXIM expects these external stakeholders to adhere to their own due diligence standards and internal controls, that does not preclude the stakeholders from providing input to EXIM's fraud risk assessments.

In addition to focusing on internal controls, the fraud risk assessment working groups have a key activity in identifying the universe of fraud risks facing EXIM. To inform and, therefore, enhance its fraud risk assessment processes, EXIM could identify fraud risks from external stakeholders through existing communication mechanisms, such as through its annual conference. For example, EXIM could identify fraud risks from external stakeholders, and two stakeholders told us that they

have attended EXIM conferences where fraud risk management topics were discussed.

Ongoing monitoring and periodic evaluations provide assurances to managers that they are effectively preventing, detecting, and responding to potential fraud. Monitoring activities, because of their ongoing nature, can serve as an early warning system for managers. By engaging external stakeholders in its monitoring activities, such as the fraud risk survey, EXIM would be better prepared to identify and promptly resolve issues before they arise and to support decisions about allocating resources in a resource-constrained environment.

Additionally, by involving external stakeholders with knowledge of fraud risks, including emerging risks posed by tariff evasion and the malicious use of artificial intelligence, within its fraud risk assessment process, EXIM would be better positioned to fully understand the landscape of fraud risks and vulnerabilities facing the organization. Involving external stakeholders within its fraud risk assessment process would also allow EXIM to meet its antifraud strategy's objective to systematically identify vulnerabilities both inside and outside of EXIM. Further, EXIM's fraud risk assessment working groups could better execute a key activity, outlined within the strategy, to identify the universe of fraud risks, using external information.

EXIM Does Not Collect and Use Information About Potential Fraud from External Stakeholders for Monitoring Activities

In spring 2025, EXIM began an effort to track and monitor fraud risk metrics in its portfolios. This effort is designed to track potential, suspected, and actual fraud, according to officials. The tracking process is intended to allow EXIM to gauge the level of risks within its portfolio and further align EXIM's efforts with the Fraud Risk Framework's fourth component, according to officials.

According to another leading practice within the fourth component of the Fraud Risk Framework, managers should collect and analyze information for real-time monitoring of fraud trends and identification of potential control deficiencies.[32] The Fraud Risk Framework states that managers should collect feedback from sources of information about actual and potential fraud risks. Potential sources of feedback include external stakeholders.

[32]GAO-15-593SP.

Consistent with the leading practice, EXIM collects information about potential fraud from internal stakeholders to inform its effort to track and monitor fraud risk metrics. For instance, according to officials, the metrics are based on suspected fraud referrals from EXIM employees. EXIM also uses data from its Enterprise Reporting System and information from its due diligence reviews to inform the metrics, according to officials.

EXIM developed "red flags," or fraud indicators, to use in the fraud risk metric tracking process. For instance, the FRO, with help from EXIM information technology staff, built "red flags" into the metric tracking process. EXIM's "red flags" are based on fraud that EXIM experienced years ago.[33] According to officials, EXIM will compare application information to the "red flags," or fraud indicators, to track potential instances of fraud. EXIM plans to review these data points every 6 months for trends. The review will look back through past transactions to see how many of these "red flags," or fraud indicators, were present in those transactions, according to officials.[34]

In the absence of adjudicated cases of fraud, EXIM uses proxies for information on potential fraud that may be undetected to manage fraud risks. According to officials, there have been no adjudicated cases of fraud related to EXIM transactions in recent years, and they rely on the EXIM's OIG to inform them of adjudicated cases of fraud.[35] EXIM officials

[33]According to officials, EXIM has five "red flags" it considers to be characteristics of heightened fraud risk. The "red flags" are derived from actual incidents of fraud perpetrated against EXIM in the early 2000s: (1) transactions involving nonoriginal equipment manufacturer exporters, (2) transactions involving used equipment, (3) transactions involving nonbank financial institutions, (4) transactions involving reimbursement, and (5) transactions originating from selected zip codes.

[34]EXIM analyzed the fraud risk metrics from fiscal year 2019 through fiscal year 2024. EXIM presented the initial analyses of these fraud risk metrics to the Chief Risk Officer and the FRO, according to officials. EXIM's review of the fraud risk metrics did not reveal anything that required immediate action, according to officials. As of February 2026, this analysis remains ongoing, according to officials.

[35]A judicial system or other adjudicative system determines whether an act is, in fact, fraud. This determination is beyond management's professional responsibility. GAO, *Standards for Internal Control in the Federal Government,* GAO-25-107721 (Washington, D.C.: May 15, 2025).

also told us that, given the low volume of fraud in recent years, they must look at other proxies for information on potential fraud.[36]

External stakeholders, such as DAL and ECI stakeholders, can serve as sources of information on potential fraud. However, they inconsistently report such instances to EXIM. We asked external stakeholders if they had reported instances of suspected fraud to EXIM. Of the 10 stakeholders we interviewed, one stakeholder told us it had communicated an instance of suspected fraud to EXIM in the past 1 to 2 years.[37] Two stakeholders told us that if they suspected an application to be fraudulent, they would no longer work with the client. One stakeholder told us that they would notify EXIM that they are no longer working with the client, but they would not explain the reason to EXIM because EXIM does not ask the stakeholder for a reason for the resignation. Another stakeholder told us that they were not required to report suspected fraud to EXIM.

Unlike with its internal stakeholders, EXIM has no process to track and monitor information on potential fraud from external stakeholders. According to EXIM officials, there are no plans to do so to inform the fraud risk metric tracking process. EXIM officials told us it expects external stakeholders to follow "Know Your Customer" due diligence requirements and inform EXIM of suspected fraud or actual fraud experienced.[38] EXIM officials told us they believe this expectation is communicated to external stakeholders through email communications.

By collecting and using information from external stakeholders on potential fraud, EXIM would be better positioned to proactively address fraud risks, as well as potential vulnerabilities facing the organization. It

[36]We have previously reported that, given the hidden nature of fraud, a certain portion of fraud will go undetected and that not all potential fraud is investigated or prosecuted. GAO, *Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments,* GAO-24-105833 (Washington, D.C.: Apr. 16, 2024).

[37]Seven stakeholders responded "no," and two stakeholders responded "unsure," when asked if they had reported a suspected instance of fraud to EXIM. Of the seven stakeholders who replied "no" to this question, two told us they would report the instance to EXIM, if encountered.

[38]On its website, EXIM states that it requires lenders under its programs to have in place written "Know Your Customer" practices substantially similar to the "Customer Identification Program" described at 31 C.F.R. §1020.220 and the due diligence program described at 31 CFR §1010.620, as amended.

would also provide opportunities for EXIM to fully inform its fraud risk metric tracking process, in the absence of adjudicated fraud.

EXIM Does Not Communicate Monitoring Results to External Stakeholders

According to a leading practice in component four of the Fraud Risk Framework, managers should communicate the results of monitoring and evaluations, including corrective actions taken, if any, to relevant stakeholders. [39] The Fraud Risk Framework states that newsletters, among other mechanisms, can be used for disseminating the results of reviews. Communicating the results of monitoring activities and evaluations can promote cross-organizational collaboration, and publicizing the results of evaluations of fraud control efforts can have a deterrent effect that can aid in fraud prevention.

EXIM communicates the results of its monitoring and evaluative efforts, including corrective actions taken, to internal stakeholders. For instance, according to EXIM's antifraud strategy and officials, the FRO identifies and presents any recommendations, deficiencies, or lessons learned as a result of the fraud risk assessment to the Enterprise Risk Committee and senior management. According to officials, EXIM has made changes to its fraud controls because of its fraud risk assessment process. For example, officials told us that EXIM added fraud controls around the contracting process in 2019 after a fraud risk assessment found that risk levels were greater than its stated appetite. EXIM communicated these results to senior management.

In contrast, EXIM's fraud risk assessment results, and changes to fraud controls made as a result of the assessment process, have not been communicated to the DAL and ECI. We asked external stakeholders whether EXIM had communicated the results of its fraud risk assessments. Seven of the 10 stakeholders we interviewed reported that EXIM had not communicated the results of fraud risk assessments, and the other three stated that they were unsure. One stakeholder told us that it would be helpful, as lenders and advisors, to be aware of issues identified by EXIM. Another stakeholder told us they would be receptive to recommendations or areas of concern raised by EXIM.

According to EXIM officials, the results of monitoring efforts are not communicated to external stakeholders because EXIM does not believe that these activities have much value to the DAL and ECI, as these activities focus on EXIM-specific internal fraud risk controls and

[39] GAO-15-593SP.

operations. Officials also told us that, to the extent that a fraud risk assessment recommendation applies to external stakeholders, the FRO would communicate the recommendation to them, but it depends on the nature of the recommendation.

EXIM officials also told us that if they believed a recommendation ever needed to be communicated to external stakeholders, there are communication channels in place to do so, such as a newsletter. The nature of the recommendation would determine if the communication needs to go out to the entire external stakeholder community, according to officials, or just one stakeholder. Officials further told us that the FRO would be open to communicating with external stakeholders regarding corrective actions on a need-to-know basis. In addition, EXIM officials told us they would communicate, and have communicated, general fraud risk trends they may experience or be aware of, such as trends on cybersecurity risk, identity theft risk, and wire fraud risk, through newsletters.

Communication about changes to fraud controls based on evaluative activities could enhance external stakeholders' due diligence responsibilities and EXIM's perception to outside actors, as EXIM officials told us they believe there is an external perception that EXIM has strong antifraud controls. Stakeholders also told us it would be helpful to receive more communication from EXIM on managing fraud. One stakeholder told us that increased communication from EXIM tailored to fraud prevention would be helpful and that they would be receptive to EXIM sharing best practices, recommendations, or areas of concern. Another stakeholder mentioned that, as lenders and advisors, it would be helpful to be aware of issues identified by EXIM as part of lessons learned to improve fraud risk management.

By communicating the results of monitoring activities and evaluations to internal and external stakeholders, EXIM could promote cross-organizational collaboration. Moreover, publicizing the results of evaluations of fraud controls, such as lessons learned or corrective actions, both internally and externally, can aid EXIM in fraud prevention throughout the organization.

Excluded Parties Were Not Identified in Participant Transaction Data

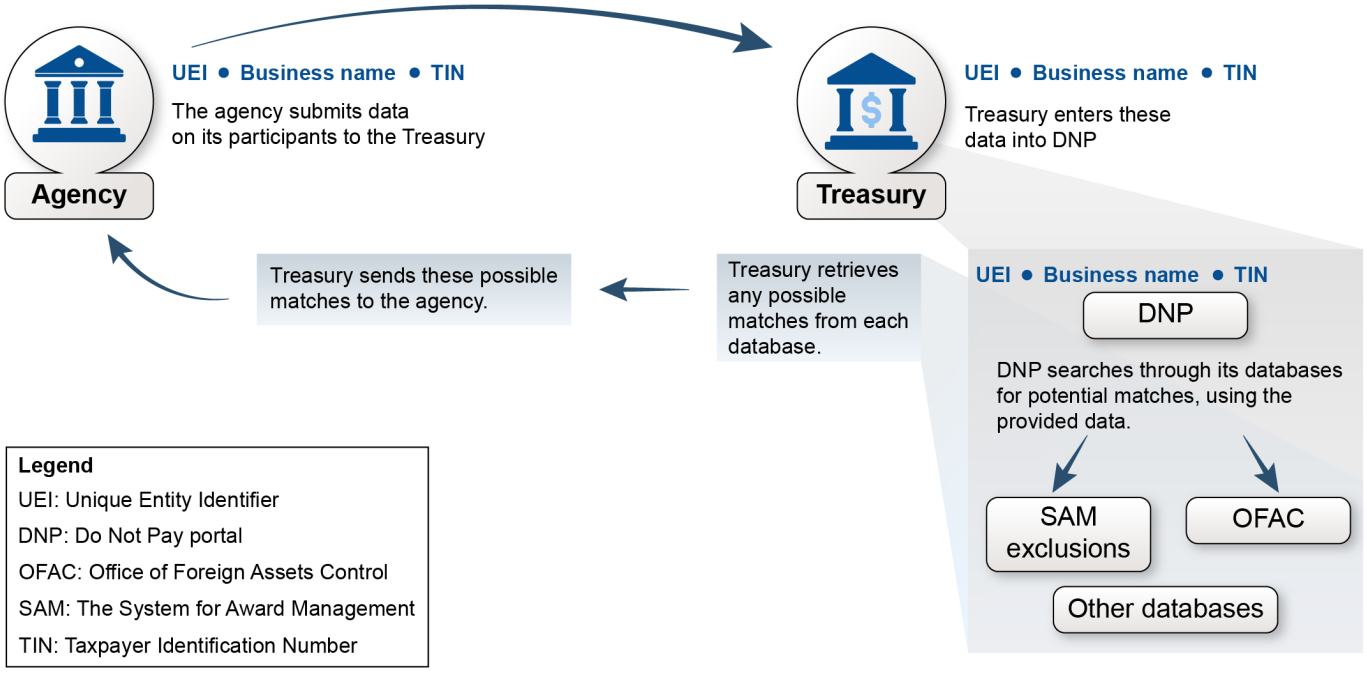
We did not identify any excluded parties within EXIM's transaction data from January 1, 2022, to June 30, 2025.[40] We submitted 78,812 individual participants to DNP and reviewed whether transaction participants appeared in databases searched by DNP, specifically Treasury's Office of Foreign Assets Control (OFAC) sanctions list and the General Services Administration's System for Award Management (SAM) exclusion list.[41]

DNP is a data search system, hosted and administered by Treasury, that, among other things, compares the data submitted by an agency with several federal debarment lists. This includes those lists managed by Treasury, the U.S. Department of Defense, and the General Services Administration. See figure 7 for an illustration of the process for an agency to submit information to DNP.

[40]For this report, we define excluded parties as any entity listed on the Treasury's OFAC sanctions list and the SAM exclusion list. The entities on these lists are generally prohibited from doing business with U.S. persons or are excluded from receiving federal financial and nonfinancial assistance and benefits.

[41]The same company could appear multiple times as different participants, and they would be evaluated separately in each application.

Figure 7: The Process for an Agency to Submit Information to the U.S. Department of the Treasury's Bureau of the Fiscal Service's Do Not Pay Portal



Sources: GAO analysis of the U.S. Department of the Treasury and Export-Import Bank of the United States data; Icons-Studio/stock.adobe.com (icons). | GAO-26-108469

DNP uses data points, such as the company's business name, the Unique Entity Identifier (UEI), and the Taxpayer Identification Number to check whether a company appears in each database.[42] Databases may use different sets of data to return a match. For example, OFAC uses the business name, while SAM uses either UEI or a combination of the Taxpayer Identification Number and business name.

An August 20, 2025, memo from the Office of Management and Budget provided guidance for federal agencies on using DNP to comprehensively screen for improper payments to protect against waste, fraud, and abuse to meet existing DNP usage requirements.[43] EXIM officials told us in

[42]A Taxpayer Identification Number is an identification number used by the Internal Revenue Service in the administration of tax laws. It is issued either by the Social Security Administration or by the Internal Revenue Service.

[43]Office of Management and Budget, *Memorandum to Heads of Executive Departments and Agencies: Preventing Improper Payments and Protecting Privacy Through Do Not Pay,* M-25-32 (Washington, D.C.: Aug. 20, 2025).

December 2025 that EXIM is subject to this memo and is currently taking steps to ensure compliance. For example, officials told us that they are using DNP as a part of its applicant review process. EXIM also complies with the DNP initiative through its CRTI procedures, according to EXIM's fiscal year 2025 report.[44]

EXIM also maintains a convicted parties list.[45] We reported in 2022 that EXIM created the convicted parties list, which has two parts.[46] Part 1 lists those individuals and companies that meet the Section 406 definition of having been convicted "in connection with an application made in the preceding 5 years." EXIM designed a broader scope for Part 2 of the convicted parties list based on what it believed was the intent of the Section 406 antifraud requirement. Part 2 lists those individuals, and companies known to be owned or controlled by such individuals, convicted in the preceding 5 years in connection with any EXIM matter, including the fraudulent use of EXIM's name.

According to EXIM, parties on Part 2 of the list are not necessarily excluded from EXIM transactions, but they must get EXIM's express written permission before proceeding with an EXIM-supported transaction in which any individual or company listed on Part 2 is a buyer, borrower, end-user, lender, or exporter. Both parts of the convicted parties list are

[44]Export-Import Bank of the United States, *Annual Management Report, A Subsection of the Annual Report for the Year Ended September 30, 2025*.

[45]The legislation reauthorizing EXIM, in December 2019, added an antifraud requirement to EXIM's consideration of applications for assistance. Specifically, Section 406 of this legislation stated that EXIM shall deny an application for assistance if the end-user, borrower, lender, or exporter has been convicted of an act of fraud or corruption in connection with an application for support from EXIM made in the preceding 5 years. The legislation further states that EXIM may proceed with an application if an end-user, borrower, lender, or exporter who might be subject to the antifraud requirement can be fully excluded from the transaction. GAO-22-105340. The Further Consolidated Appropriations Act, 2020 (P.L. 116-94, Div. I, title IV, 133 Stat. 2534, 3021-26, enacted December 20, 2019), extended EXIM's general statutory authority for 7 years, through December 31, 2026.

[46]GAO-22-105340.

publicly available at EXIM's website.[47] As of January 2026, there were no entities on Part 1 of the convicted parties list.[48]

Conclusions

For more than 90 years, EXIM has served as a financier of last resort for U.S. companies that seek to sell and export their goods or services to foreign buyers that cannot obtain private financing for their deals. In this role, EXIM assumes credit and country risks that the private sector is unable or unwilling to accept, including the risk of losses due to fraud. Since 2018, EXIM has taken a variety of actions to better manage the fraud risks it faces. For instance, by implementing our recommendations, EXIM's ability to identify vulnerabilities facing the organization and to strategically describe EXIM's approach for preventing, detecting, and responding to fraud has improved.

Further, EXIM has made efforts to monitor and evaluate the effectiveness of its fraud prevention activities. This evaluative effort positions EXIM to respond appropriately to a changing risk environment and effectively manage fraud risks. EXIM also has procedures during the applicant review process to ensure that entities banned from receiving federal assistance are appropriately denied.

However, EXIM's fraud risk management activities can benefit by engaging its external stakeholders in the monitoring and evaluation of its activities. EXIM does not engage external stakeholders in its fraud risk assessment evaluative activities or within its regular fraud risk assessment process. By engaging external stakeholders within these efforts, EXIM can identify emerging risks faced by the organization, improve stakeholder partnership to effectively manage fraud risks, and make better informed decisions when reviewing the effectiveness of its fraud controls. In addition, EXIM does not collect and use information

[47]The website that contains the current convicted parties list is available at https://www.exim.gov/policies/convicted-parties-list-section-406.

[48]EXIM has compiled a convicted parties list pursuant to the procedures implementing Section 406 of the Export-Import Bank Reauthorization Act of 2019. Section 406 has been incorporated into the EXIM Charter under Section 2(f) (12 U.S.C. § 635(f)) and directs EXIM to deny applications for transactions in which certain parties have been convicted of fraud or corruption in connection with EXIM transactions. We reported in 2022 that EXIM created the convicted parties list, which has two parts. Part 1 lists those individuals and companies that meet the Section 406 definition of having been convicted "in connection with an application made in the preceding 5 years." EXIM designed a broader scope for Part 2 of the convicted parties list based on what it believed was the intent of the Section 406 antifraud requirement. See GAO-22-105340. As of January 5, 2026, there were four entities on Part 2 of the convicted parties list. However, we did not include Part 2 entities in our review because they are not necessarily excluded from doing business with EXIM.

about potential fraud from external stakeholders for its monitoring activities. By collecting and using instances of potential fraud from external stakeholders, EXIM could be better assured that its development of fraud indicators is based on recent experiences and reduces the reliance on adjudicated fraud. Further, EXIM does not communicate monitoring results to external stakeholders. Communicating the results of its monitoring activities could inform and enhance external stakeholders' preventative activities, further promote collaboration internal and external to the organization, and deter fraud.

Within the overall context of maturing its capacity to manage fraud risks, enhanced engagement with external stakeholders could help EXIM to further align its efforts with the fourth component of the Fraud Risk Framework and to take a risk-based approach to improving its fraud risk management activities within a resource-constrained environment, thus reinforcing EXIM's antifraud culture.

Recommendations for Executive Action

We are making the following four recommendations to EXIM:

EXIM's Chair and President should engage EXIM's external stakeholders responsible for specific fraud risk management activities within its monitoring and evaluation of preventative activities by including Delegated Authority Lenders (DAL) and Export Credit Insurer (ECI) stakeholders in its fraud risk survey. (Recommendation 1)

EXIM's Chair and President should involve external stakeholders responsible for the design and implementation of fraud controls, such as its DAL and ECI stakeholders, in its fraud risk assessment process. (Recommendation 2)

EXIM's Chair and President should collect and use information on instances of potential fraud from DAL and ECI stakeholders for the refinement of its "red flags," or fraud indicators. (Recommendation 3)

EXIM's Chair and President should communicate the results of its monitoring and evaluations, including corrective actions taken, to its DAL and ECI stakeholders, such as deficiencies identified, lessons learned, or recommendations made as a result of EXIM's fraud risk management activities. (Recommendation 4)

Agency Comments

We provided a draft of this report to EXIM for review and comment. In its comments, reproduced in appendix IV, EXIM agreed with our recommendations, stating that it sees value in the input provided by DAL

and ECI stakeholders, and described planned actions to address the recommendations. EXIM also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees and EXIM's Chair and President, and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at BagdoyanS@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

//SIGNED//

Seto J. Bagdoyan
Director, Forensic Audits and Investigative Service

List of Committees

The Honorable Tim Scott
Chairman
The Honorable Elizabeth Warren
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Lindsey Graham
Chair
The Honorable Brian Schatz
Ranking Member
Subcommittee on State, Foreign Operations, and Related Programs
Committee on Appropriations
United States Senate

The Honorable French Hill
Chairman
The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable Mario Diaz-Balart
Chairman
The Honorable Lois Frankel
Ranking Member
Subcommittee on National Security, Department of State, and Related Programs
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report assesses the extent to which (1) the Export-Import Bank of the United States (EXIM) has monitored and evaluated its fraud risk management activities and engaged its stakeholders in the monitoring process and (2) excluded parties can be identified in EXIM's transaction data from January 1, 2022, to June 30, 2025.[1]

To assess the extent to which EXIM has monitored and evaluated its fraud risk management activities and engaged its stakeholders in the monitoring process, we analyzed EXIM documentation related to its antifraud efforts and interviewed EXIM officials responsible for their development. Specifically, we reviewed EXIM's fiscal year 2023 and fiscal year 2025 fraud risk assessments, its fraud risk profiles, and fiscal year 2025 Antifraud Strategy. In addition, we interviewed 10 selected EXIM external stakeholders, Delegated Authority Lenders (DAL) and Export Credit Insurers (ECI), to obtain their views on EXIM's efforts to engage and communicate with stakeholders responsible for fraud risk management during its monitoring and evaluation process. Although the findings of these interviews are not generalizable to all stakeholders, they provide illustrative examples of fraud risk management activities at EXIM and insight about EXIM's efforts to engage with, and communicate to, stakeholders in its monitoring and evaluation process. To obtain a range of external stakeholder types and perspectives, we selected DAL and ECI stakeholders based on a variety of considerations. These considerations included the geographic location of the stakeholder; the stakeholder's classification, as assigned by the Federal Deposit Insurance Corporation; the stakeholder's asset size; tier rating; the length of time the stakeholder was associated with EXIM; and the number of active loans or policies held by the stakeholder.

We analyzed the extent to which these activities and EXIM's efforts aligned with leading practices in the fourth component of GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework).[2] The Fraud Risk Framework's fourth component describes 10 leading practices for evaluating outcomes using a risk-based approach and adapting activities to improve fraud risk management. We assessed

[1]For this report, we define excluded parties as any entity listed on the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctions list and the General Services Administration's System for Award Management (SAM) exclusion list. The entities on these lists are generally prohibited from doing business with U.S. persons or are excluded from receiving federal financial and nonfinancial assistance and benefits.

[2]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

these activities and EXIM's efforts against all 10 leading practices from the fourth component. We discuss five leading practices that are relevant to this objective:

1. Monitor and evaluate the effectiveness of preventive activities, including fraud risk assessments and the antifraud strategy, as well as controls to detect fraud and response efforts;

2. Collect and analyze data, including data from reporting mechanisms and instances of detected fraud, for real-time monitoring of fraud trends and identification of potential control deficiencies;

3. Engage stakeholders responsible for specific fraud risk management activities in the monitoring and evaluation process;

4. Use the results of monitoring and evaluations to improve the design and implementation of fraud risk management activities; and

5. Communicate the results of monitoring and evaluations, including corrective actions taken, if any, to relevant stakeholders.

Based on our findings related to EXIM's efforts to monitor and evaluate the effectiveness of its fraud preventative activities, including its fraud risk assessments, we evaluated EXIM's involvement of its external stakeholders in the development of its fraud risk assessment. For this, we analyzed the extent to which this effort aligned with a relevant leading practice in the second component of GAO's Fraud Risk Framework.[3] This leading practice states that program managers should involve relevant stakeholders in the assessment process, including individuals responsible for the design and implementation of fraud controls.

To assess the extent to which excluded parties can be identified in EXIM's transaction data from January 1, 2022, to June 30, 2025, we compared EXIM transaction participants to the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctions list and the General Services Administration's System for Award Management (SAM) exclusion list for excluded parties. As part of this work, we submitted a list of EXIM transaction participants from January 1, 2022, to June 30, 2025, to the U.S. Department of the Treasury's Bureau of the Fiscal Service's

[3]GAO-15-593SP.

Do Not Pay portal (DNP).[4] Next, we independently verified the accuracy of any matches from DNP, using the SAM exclusion list database.

As a part of this work, we also obtained information from the SAM exclusion list database from the time of our submission to DNP on September 22, 2025, as a method of verifying the accuracy of the returns from DNP.[5] This database includes the records of excluded parties from several federal databases, including OFAC and SAM, in addition to the dates in which the excluded parties were restricted. We counted DNP returns as confirmed matches to excluded parties if the participant was present in the SAM exclusion list database and was also excluded at the time of the EXIM transaction in which they participated.

In addition, we reviewed EXIM and DNP documentation to confirm that our use of EXIM transaction data and DNP was accurate. We also met with EXIM data managers to confirm this understanding.

We did not review the extent to which participants within EXIM's convicted parties list were present in EXIM's participant transaction data

[4]DNP is a data search system, hosted and administered by the U.S. Department of the Treasury, Bureau of the Fiscal Service. It compares the data submitted by an agency with several federal debarment lists. Agencies can use DNP to review program participants for potential improper payments. DNP consolidates data on entities ineligible to receive payments. DNP is also a data-matching service for agencies to use in preventing payments to ineligible individuals, such as those who are deceased.

[5]DNP uses data points, like a company's business name, Unique Entity identifier, and Taxpayer Identification Number, to check whether an entity appears within a set of federal exclusion databases.

because, as of January 2026, there were no entities on Part 1 of the convicted parties list.[6]

We assessed the reliability of EXIM's participant transaction data by performing electronic testing on specific data elements, reviewing related documentation, and interviewing knowledgeable officials responsible for the data and related information systems. We determined that the data we used in our analysis were sufficiently reliable for the purposes of our reporting objective.

We conducted this performance audit from May 2025 to May 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[6]EXIM has compiled a convicted parties list pursuant to the procedures implementing Section 406 of the Export-Import Bank Reauthorization Act of 2019. Section 406 has been incorporated into the EXIM Charter under Section 2(f) (12 U.S.C. § 635(f)) and directs EXIM to deny applications for transactions in which certain parties have been convicted of fraud or corruption in connection with EXIM transactions. We reported in 2022 that EXIM created the convicted parties list, which has two parts. Part 1 lists those individuals and companies that meet the Section 406 definition of having been convicted "in connection with an application made in the preceding 5 years." EXIM designed a broader scope for Part 2 of the convicted parties list based on what it believed was the intent of the Section 406 antifraud requirement. GAO, *Export-Import Bank: Additional Documentation about Stakeholder Roles and Clarity about Fraud Risks Would Strengthen Antifraud Efforts*, GAO-22-105340 (Washington, D.C.: Sept. 27, 2022). As of January 5, 2026, there were four entities on Part 2 of the convicted parties list. However, we did not include Part 2 entities in our review because they are not necessarily excluded from doing business with EXIM. According to EXIM, parties on Part 2 of the list are not necessarily excluded from EXIM transactions, but they must get EXIM's express written permission before proceeding with an EXIM-supported transaction in which any individual or company listed on Part 2 is a buyer, borrower, end-user, lender, or exporter.

Appendix II: The Export-Import Bank of the United States' Total Exposure in Fiscal Year 2025

The Export-Import Bank of the United States (EXIM) releases an annual report on its market activity, including a breakdown of its support by country for that fiscal year. Table 1 displays the top five countries in which EXIM had the most exposure in fiscal year 2025.[1] In fiscal year 2025, EXIM had a total exposure of $34.8 billion.

Table 1: Top Five Countries That Received Support from the Export-Import Bank of the United States in Fiscal Year 2025

Rank	Country	Total exposure in fiscal year 2025
1	Mozambique	$4.7 billion
2	Saudi Arabia	$3.5 billion
3	Angola	$3.2 billion
4	Turkey	$2.9 billion
5	Kazakhstan	$1.0 billion
	Other countries	$19.5 billion

Source: Export-Import Bank of the United States information. I GAO-26-108469

[1]According to EXIM, exposure is the total outstanding and undisbursed principal balance of loans, guarantees, and insurance, along with any unrecovered balances of payments made on claims submitted and approved by EXIM. This does not include the accrued interest or transactions pending final approval, according to EXIM. The claims payments are made by EXIM while acting as guarantor or insurer under the export guarantee and insurance programs, according to EXIM. Export-Import Bank of the United States, A*nnual Management Report, A Subsection of the Annual Report for the Year Ended September 30, 2025* (Washington, D.C: Jan. 2026).

Appendix III: Status of Fraud Risk Management Recommendations

Table 2 lists the 11 recommendations from three prior GAO reports on the Export-Import Bank of the United States' (EXIM) fraud risk management activities.[1] EXIM has implemented all 11 recommendations.

Table 2: Prior GAO Recommendations to Enhance Fraud Risk Management at the Export-Import Bank of the United States (EXIM)

Number	Report number	Recommendation
1	*Export-Import Bank: The Bank Needs to Continue to Improve Fraud Risk Management* (GAO-18-492)	The acting Bank President and Board Chairman should ensure that the Bank evaluates and implements methods to further promote and sustain an antifraud tone that permeates the Bank's organizational culture, as described in GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework).[a] This should include consideration of requiring training on fraud risks relevant to Bank programs, for new employees and all employees on an ongoing basis, with the training to include identifying roles and responsibilities in fraud risk management activities across the Bank.
2	GAO-18-492	As the agency begins efforts to plan and conduct regular fraud risk assessments and to determine a fraud risk profile, the acting Bank President and Board Chairman should ensure that the Bank's risk assessments and profile address not only known methods of fraud, including those that are absent from its current risk register, but other inherent fraud risks, as well.
3	GAO-18-492	As the agency begins efforts to plan and conduct regular fraud risk assessments and to determine a fraud risk profile, the acting Bank President and Board Chairman should ensure that the risk profile includes risk tolerances that are specific and measurable.
4	GAO-18-492	The acting Bank President and Board Chairman should ensure that the Bank develops and implements an antifraud strategy with specific control activities, based upon the results of fraud risk assessments and a corresponding fraud risk profile, as provided in GAO's Fraud Risk Framework.[b]
5	GAO-18-492	The acting Bank President and Board Chairman should ensure that the Bank identifies, and then implements, the best options for sharing more fraud-related information—including details of fraud case referrals and outcomes—among Bank staff, to help build fraud awareness, as described in GAO's Fraud Risk Framework.[c]

[1]GAO, *Export-Import Bank: The Bank Needs to Continue to Improve Fraud Risk Management,* GAO-18-492 (Washington, D.C.: July 19, 2018); *Export-Import Bank: EXIM Should Explore Using Available Data to Identify Applicants with Delinquent Federal Debt,* GAO-19-337 (Washington, D.C.: May 23, 2019); and *Export-Import Bank: Additional Documentation about Stakeholder Roles and Clarity about Fraud Risks Would Strengthen Antifraud Efforts*, GAO-22-105340 (Washington, D.C.: Sept. 27, 2022).

Number	Report number	Recommendation
6	GAO-18-492	The acting Bank President and Board Chairman should lead efforts to collaborate with the Bank's Office of Inspector General (OIG) to identify a feasible, cost-effective means to systematically track outcomes of fraud referrals from the Bank to the OIG, including creating a means to link the OIG's proven cases of fraud to the specific Bank transactions from which the OIG's actions arose. If any such means are found to be feasible and cost-effective, the acting Bank President and Board Chairman should direct appropriate staff to implement them, with such information to be used for purposes consistent with GAO's Fraud Risk Framework, such as data analytics.[d]
7	GAO-18-492	The acting Bank President and Board Chairman should ensure that the Bank monitors and evaluates outcomes of fraud risk management activities, using a risk-based approach and outcome-oriented metrics, and that it subsequently adapts antifraud activities or implements new ones, as determined to be appropriate and consistent with GAO's Fraud Risk Framework.
8	*Export-Import Bank: EXIM Should Explore Using Available Data to Identify Applicants with Delinquent Federal Debt* (GAO-19-337)	EXIM's Chief Operating Officer should direct EXIM's Credit Review and Compliance Division to assess and document the practicality of incorporating into its preauthorization character, reputational, and transaction integrity (CRTI) reviews searches of data elements in the General Services Administration's System for Award Management (SAM) that indicate delinquent federal debts owed by applicants and, if practical, implement relevant approaches—such as manual searches or batch matching.
9	GAO-19-337	EXIM's Chief Operating Officer should direct EXIM's Credit Review and Compliance Division to assess and document the practicality of incorporating into its postauthorization CRTI reviews searches of data elements in SAM that indicate delinquent federal debts owed by applicants and participants and, if practical, implement relevant approaches—such as manual searches or batch matching.
10	*Export-Import Bank: Additional Documentation about Stakeholder Roles and Clarity about Fraud Risks Would Strengthen Antifraud Efforts* (GAO-22-105340)	EXIM's Chair and President should update its antifraud strategy to demonstrate links to its highest internal and external residual fraud risks outlined in its fraud risk profile to its antifraud strategy.
11	GAO-22-105340	EXIM's Chair and President should update its antifraud strategy to document the roles and responsibilities of the external parties, specifically Delegated Authority Lending (DAL) and Export Credit Insurance (ECI) partners, responsible for fraud controls.

Source: GAO analysis of recommendations from prior GAO reports on the Export-Import Bank of the United States' fraud risk management activities. I GAO-26-108469

[a]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

[b]GAO-15-593SP.

[c]GAO-15-593SP.

[d]GAO-15-593SP.

Appendix IV: Comments from the Export-Import Bank of the United States

May 1, 2026

Government Accountability Office

441 G Street, N.W.

Washington, D.C. 20548-0001

Regarding: EXIM Management Response to the GAO Draft Report: Improved External Stakeholder Engagement Could Enhance Fraud Risk Management. (GAO -26-108469)

Dear Mr. Bagdoyan:

The Export-Import Bank of the United States (EXIM) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report, **"Improved External Stakeholder Engagement Could Enhance Fraud Risk Management" (GAO-26-108469).**

EXIM leadership fully supports the GAO's work and values our cooperative relationship. We share a mutual commitment to continuously improving EXIM's policies, procedures, and operations. Specifically, we appreciate the GAO's thorough evaluation of our: (1) fraud risk assessment process, (2) assessment evaluations, and (3) the collection and use of information for fraud risk monitoring.

This report aligns with our strategic commitment to optimizing risk management through enhanced stakeholder engagement. By refining our framework in coordination with these key partners, EXIM will further strengthen its risk assessment integrity. These improvements are vital to fostering the institutional trust necessary to expand our programs, drive U.S. job creation, and deliver maximum value to the taxpayer.

Sincerely,

Kenneth Tinsley

KENNETH TINSLEY Digitally signed by KENNETH TINSLEY Date: 2026.04.30 19:42:19 -04'00'

Senior Vice President and Chief Risk Officer (CRO)

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

Recommendation 1: EXIM's Chair and President should engage EXIM's external stakeholders responsible for specific fraud risk management activities within its monitoring and evaluation of preventative activities by including Delegated Authority Lenders (DAL) and Export Credit Insurer (ECI) stakeholders in its fraud risk survey.

Management Response: EXIM agrees with this recommendation. EXIM sees value in input provided by DAL and ECI stakeholders to serve as a source for identifying new fraud risk factors, potential fraud schemes, and fraud risk controls. The Bank will request this information within criteria that exempts the need for an official form per the Paperwork Reduction Act. EXIM will codify the use of this information in its Anti-Fraud Strategy.

Recommendation 2: EXIM Chair and President should involve external stakeholders responsible for the design and implementation of fraud controls, such as its DAL and ECI stakeholders in its fraud risk assessment process.

Management Response: EXIM agrees with this recommendation. EXIM sees value in input provided by DAL and ECI stakeholders to serve as a source for identifying new fraud risk factors, potential fraud schemes, and fraud risk controls. The Bank will request this information within criteria that exempts the need for an official form per the Paperwork Reduction Act. EXIM will codify the use of this information in its Anti-Fraud Strategy.

Recommendation 3: EXIM Chair and President should collect and use information on instances of potential fraud from DAL and ECI stakeholders for the refinement of its "red flags" or fraud indicators.

Management Response: EXIM agrees with this recommendation. EXIM sees value in information provided by DAL and ECI stakeholders on instances of potential fraud for use in further refining its fraud risk indicators. EXIM will codify this in its Anti-Fraud Strategy.

Recommendation 4: EXIM's Chair and President should communicate the results of its monitoring and evaluations including corrective actions taken to its DAL and ECI stakeholders, such as deficiencies identified, lessons learned, or recommendations made as a result of EXIM's fraud risk management activities.

Management Response: EXIM agrees with this recommendation. At present, EXIM periodically communicates to DAL and ECI stakeholders through existing outreach. EXIM agrees, at appropriate intervals, to include in such communications lessons learned from its fraud risk management monitoring and evaluation activities. EXIM will codify this in its Anti-Fraud Strategy.

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

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Seto J. Bagdoyan at BagdoyanS@gao.gov

Staff Acknowledgments

In addition to the contact named above, Nicholas Weeks (Assistant Director), Paulissa Earl (Analyst in Charge), Sean Dedmon, Michael Doerge, Colin Fallon, Gina Hoover, Joseph Rini, and Sabrina Streagle made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us