6690-01-P]

EXPORT IMPORT BANK

Privacy Act of 1974; System of Records

AGENCY: Export Import Bank of the United States.

ACTION: Notice of a Modified System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974, the Export Import Bank of the United States ("EXIM", "EXIM Bank", or "The Bank") proposes to update a system of records notice ("SORN"). The updated system of records described in this notice, EXIM Financial Management System- Next Generation, supports flexible financial accounting, control and disbursement of funds, management accounting, loan and guarantee servicing, and financial report processes. Information contained in Financial Management System- Next Generation include but is not limited to: Customer name, the name of the "Care Of" entity, U.S. address, foreign address, and foreign contact name, bank account information, Corporate Name, Corporate Address, Phone Number, Employer Identification Number (EIN), and banking account and banking routing number. The purpose of this notice is to update the routine uses of this system to comport to the requirements of M-25-32 – Preventing Improper Payments and Protecting Privacy through the Do Not Pay -- issued by OMB on August 20, 2025.

DATES: The system of records described herein will become effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The deadline to submit comments on this system of records, as well as the date on which the below routine uses will become effective, will be 30 days after Federal Register publication.

ADDRESSES: You may submit written comments to EXIM Bank by any of the following methods:

- Federal e-Rulemaking Portal: https://www.regulations.gov. Follow the website instructions for submitting comments.
- E-mail: SORN.Comments@exim.gov. Refer to SORN in the subject line.
- Mail or Hand Delivery: Address letters to the Freedom of Information Act Office and the Office of Information Management and Technology, Export Import Bank of the United States, 811 Vermont Avenue NW, Washington, DC 20571.

Commenters are strongly encouraged to submit public comments electronically. EXIM Bank expects to have limited personnel available to process public comments that are submitted on paper through mail. Until further notice, any comments submitted on paper will be considered to the extent practicable.

All submissions must include the agency's name (Export Import Bank of the United States, or EXIM Bank) and reference this notice. Comments received will be posted without change to EXIM Bank's website. Do not submit comments that include any Personally Identifiable Information (PII) or confidential business information. Copies of comments may also be obtained by writing to the Freedom of Information Act Office and the Office of Information Management and Technology, Export Import Bank of the United States, 811 Vermont Avenue, NW, Washington, DC 20571.

FOR FURTHER INFORMATION CONTACT: For further information, contact Michael Soybel, Acting Assistant General Counsel for Administration, at michael.soybel@exim.gov or (202) 565-3475 or by going to the website: https://exim.gov/about/freedom-information-act/privacy-act-requests/pia-notices-assessments

SUPPLEMENTARY INFORMATION:

The update to system of records described in this notice, EXIM Financial Management System-Next Generation, to support flexible financial accounting, control and disbursement of funds, management accounting, loan and guarantee servicing, and financial report processes. The report of this update to a system of records has been submitted to the Committee on Oversight and Government Reform of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Office of Management and Budget, pursuant to OMB Circular A–108, ''Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act'' (Dec. 2016) and the Privacy Act, 5 U.S.C. 552a(r).

The purpose of this notice is to update the routine uses of this system to comport to the requirements of M-25-32 – Preventing Improper Payments and Protecting Privacy through the Do Not Pay -- issued by OMB on August 20, 2025.

SYSTEM NAME AND NUMBER:

System Name: EXIM Financial Management System-Next Generation (FMS-NG)

System Number: N/A

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

This electronic system is used via a web interface by EXIM staff from the HQ of the Export Import Bank of the United States, 811 Vermont Avenue NW, Washington, DC 20571.

SYSTEM MANAGER(S):

Dae Sung Batoff, IT Program Manager,

Export Import Bank of the United States, 811 Vermont Avenue NW, Washington, DC 20571

Email: daesung.batoff@exim.gov

Telephone number: (202)860-5870

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

EXIM requests the information in this application under the following authorization: Export-Import Bank Act of 1945, as amended (12 U.S.C. 635 et seq.).[1] 5 U.S.C. 301. Executive Order 9397 as amended by Executive Order 13478 signed by President George W. Bush on November 18, 2008, relating to Federal agency use of Social Security Numbers.

PURPOSE(S) OF THE SYSTEM:

Financial Management System- Next Generation (FMS-NG) is a custom configured COTS solution, which supports flexible financial accounting, control and disbursement of funds, management accounting, loan and guarantee servicing, and financial report processes. More specifically, FMS-NG maintains EXIM's spending budget, supports buying of goods and services, vendor payments, records general ledger entries, reports to Department of Treasury, Office of Management and Budget, other agencies, and external parties, is used to verify data accuracy, properly clears and closes ledgers and journals, and provides complete loan and guarantee servicing over the entire life of a credit.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The FMS–NG system holds information on EXIM customers, employees, contractors, vendors, and invitational travelers who have been asked to speak at or attend a function at the request of EXIM and who are seeking reimbursements for expenses incurred.

CATEGORIES OF RECORDS IN THE SYSTEM:

FMS-NG contains customer information related to the financial obligations of the Bank to and from individuals and corporate entities, starting from the point of obligation through final

[1] More specifically, sections 635(a)(1) and 635a(j)(1)(C) of the Export-Import Bank Act of 1945, as amended.

disbursement. It provides complete loans and guarantees servicing throughout the entire life of a credit. The FMS-NG system stores Personally Identifiable Information (PII) about Ex-Im Bank employees, public individuals with pre-authorized reimbursable expenses, Ex-Im product applicants, contracted suppliers, and other business partners.

(1) Administrative and Employee-Related Records

These records relate to employees and individuals who receive payments, reimbursements, or other financial actions through FMS-NG:

- Employee Name
- Employee Address
- Employee email address
- Employee Phone Number
- Employee Bank Account Number (for payroll or reimbursements)
- Travel reimbursement and expense records linked to an identifiable individual

(2) Vendor / Payee Records (Individuals and Sole Proprietors Only)

The following records are included only when the vendor or payee is an individual or sole proprietor, and the record is retrieved using an individual identifier:

- Individual Vendor Name
- Vendor ID assigned to an individual
- Tax Identification Number (individual or sole proprietor)
- Bank Account Holder Name (individual only)
- Bank Account Number
- Bank Routing/SWIFT Code

(3) Individual Beneficiary or Applicant Records

- Records related to individuals who receive or apply for EXIM financial services, disbursements, or program benefits:
- Name
- Address
- Contact Information
- Payment or disbursement information
- Records necessary to determine eligibility or process financial transaction

RECORD SOURCE CATEGORIES:

The source of the record information in EXIM FMS-NG system is coming from interconnected EXIM financial business applications. The record information contained in the FMS–NG is obtained using one of two methods: Manual entry, and through data consumption from source flat files imported after validating data with business rules using PLSQL procedural upload to the FMS–NG database.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures that are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside EXIM as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To the Department of Justice (DOJ) when:

(1) EXIM, or

(2) Any employee of EXIM in his or her official capacity, or

(3) Any employee of EXIM in his or her individual capacity when the DOJ has been asked, or has agreed, to represent the employee, or

(4) The United States, when EXIM determines that litigation is likely to affect the agency, is a party to litigation, or has an interest in such litigation, and the use of such records by the DOJ is deemed by EXIM to be relevant and necessary to the litigation.

b. To a court or adjudicative body in a proceeding, when:

(1) EXIM, or

(2) Any employee of EXIM in his or her official capacity,

(3) Any employee of EXIM in his or her individual capacity when the EXIM has agreed to represent the employee, or

(4) The United States, when EXIM determines that litigation is likely to affect EXIM, is a party to litigation or has an interest in such litigation, and the use of such records by the DOJ is deemed by EXIM to be relevant and necessary to the litigation.

c. Except as noted on Standard Forms SF 85, 85–P, 86, and 86–C, when a record, alone or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant to such a statute, to the appropriate public authority, whether federal, state, local, foreign, tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant to the statute, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

d. To a congressional office in response to an inquiry from that office made at the written request of the constituent about whom the record is maintained.

e. To the National Archives and Records Administration (NARA) for records management functions authorized by laws, regulations, and policies governing NARA operations and agency records management responsibilities.

f. To contractors or other authorized individuals performing work on a contract, service, cooperative agreement, job, or other activity on behalf of the EXIM Bank who have a need to access the information in the performance of their duties or activities.

g. To a court, magistrate, or administrative tribunal during an administrative proceeding or judicial proceeding, including disclosures to opposing counsel or witnesses (including expert witnesses) during discovery or other pre-hearing exchanges of information, litigation, or settlement negotiations, where relevant and necessary to a proceeding, or in connection with criminal law proceedings.

h. To any source or potential source from which information is requested in the course of an investigation concerning the retention of an employee or other personnel action (other than hiring), or the retention of a security clearance, contract, grant, license, or other benefit, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

i. To a Federal, State, local, foreign, or Tribal or other public authority to the extent that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another federal agency for criminal, civil, administrative personnel or regulatory action.

j. To the news media or the general public, factual information the disclosure of which would be in the public interest, and which would not constitute an unwarranted invasion of personal privacy, consistent with Freedom of Information Act standards.

k. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the

CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders.

l. To appropriate agencies, entities, and persons when: (1) EXIM suspects or has confirmed that there has been a breach of the system of records; (2) EXIM has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, EXIM (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with EXIM's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

m. To Another Federal agency or Federal entity, when EXIM determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

n. To the U.S. Department of the Treasury when disclosure of the information is relevant to review payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state (meaning a state of the United States, the District of Columbia, a territory or possession of the United States, or a federally recognized Indian tribe) in a state-administered, federally funded program.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The records are stored digitally in encrypted format in FMS-NG Amazon Web Services (AWS) FedRAMP authorized cloud environment. The storage records for FMS-NG production database resides on a virtual server running Redhat Linux on AWS US East hosted in Northern Virginia.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Comprehensive electronic records are maintained by EXIM Office Of Chief Financial Officer stored in the FMS-NG database. Access to the records is restricted to those with specific roles. To access FMS-NG data multifactor authentication is required. Primary access to FMS-NG data is via FMS-NG forms and reports. FMS-NG users that have been granted access can retrieve data by personal identifiers (e.g., Customer's EIN). The identifiers used are:

- Name: Used as the unique identifier.
- Banking Information: Employee and supplier bank account numbers are stored in a hashed/masked format (e.g., "XXXXXX9913").
- Employee work email address: Work email address used for all employee records.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are archived/disposed of during the routine data sync for individuals who are no longer employees or contractors of EXIM. Otherwise, records are maintained and destroyed in accordance with the National Archives and Record Administration's ("NARA") Basic Laws and Authorities (44 U.S.C. 3301, et seq.) or an EXIM Bank records disposition schedule approved by NARA.

FMS-NG data is considered a temporary Federal Record with the retention period subject to the applicable Record Schedules. FMS-NG is designed to mark records inactive when no longer required for EXIM business, whereupon these records become subject to the retention period as defined by the applicable Records Schedule. Records that are at the end of the specified legal retention period will be deleted by following the procedures documented in Oracle Financials Application Guides, based on the built-in criteria categories:

• Invoice Purge Criteria
• Payment Purge Criteria
• Supplier Purge Criteria
• Requisition Purge Criteria
• Purchase Order Purge Criteria
• Supplier Schedules Purge Criteria

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information will be stored in electronic format within the FMS–NG. FMS–NG has configurable responsibilities-based (processes and data) user access rules. User access is granted only to the authorized internal users. The authorized FMS–NG users will have restricted access only to the data subset necessary to perform their job function. This access is managed via Oracle Application System Administration, User and Responsibility security functions. The infrastructure that FMS-NG is installed on, AWS, is compliant with the Federal Risk and Authorization Management Program (FedRAMP). The PII information in FMS–NG is stored encrypted in place. HTTPS protocol is employed in accessing FMS–NG.

RECORD ACCESS PROCEDURES:

Requests to access records under the Privacy Act must be submitted in writing and must be

signed by the requestor. Requests should be addressed to the Freedom of Information Act Office and the Office of Information Management and Technology, Export Import Bank of the United States, 811 Vermont Avenue NW, Washington, DC 20571. The request must comply with the requirements of 12 CFR 404.14.

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest and/or amend records under the Privacy Act must submit a request in writing. The request must be signed by the requestor and should be addressed to the Freedom of Information Act Office and the Office of Information Management and Technology, Export Import Bank of the United States, 811 Vermont Avenue NW, Washington, DC 20571. The request must comply with the requirements of 12 CFR 404.14.

NOTIFICATION PROCEDURES:

Individuals wishing to determine whether this system of records contains information about them may do so by submitting a written request to the Freedom of Information Act Office and the Office of Information Management and Technology, Export Import Bank of the United States, 811 Vermont Avenue, NW, Washington, DC 20571. The written request must include the following:

1. Name.
2. Type of information requested.
3. Address to which the information should be sent; and
4. Signature.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

(85 FR 3372)

Lin Zhou

Information System Security Manager

Billing Code 6690-01

[FR Doc. 2026-05932 Filed: 3/26/2026 8:45 am; Publication Date: 3/27/2026]