



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 Federal Personnel Payroll System (FPPS) enables EXIM’s Security Office staff to process EXIM’s personnel, payroll, and time and labor data to facilitate payments, benefits, and pensions. FPPS also provides personnel and payroll data to the FPPS Datamart application which EXIM uses to perform queries and report on FPPS information. FPPS is an online personnel and payroll system providing support to Federal agency customers through interagency agreement with the IBC. FPPS is customized to meet customer needs for creating and generating the full life cycle of personnel transactions. FPPS allows for immediate updates and edits of personnel and payroll data. FPPS also handles regulatory requirements such as specialized pay, garnishments, and special appointment programs. FPPS also operates in batch mode for performing close of business, payroll calculation, and other processes. FPPS customers can use a web-enabled interface, WebFPPS, to access FPPS through a web browser to perform personnel and payroll tasks. FPPS is a major application that consists of several minor applications to include time and attendance applications, a system for creating retirement cards and updating retirement records, a system for converting client data for integration into FPPS. The purpose of this system is to ensure proper payment of salary and benefits to EXIM personnel, and to track time worked, leave, or other absences for reporting and compliance purposes. Use of this system will streamline EXIM Bank’s personnel, payroll and other human resources functions into a unified,

secure system, thereby improving employee input into these systems while enhancing data integrity and security and improving operational efficiency.

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: EXIM FPPS processes EXIM's personnel, payroll, and time and labor data to facilitate payments, benefits, and pensions. FPPS also provides personnel and payroll data to the FPPS Datamart application which EXIM uses to perform queries and report on FPPS information.

The report of this update to this 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 Federal Personnel Payroll System (FPPS)

System Number: N/A

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: This electronic system will be 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, through an electronic database managed by the DOI IBC in Denver, Colorado. FPPS customers will use a web-enabled interface, WebFPPS, to access FPPS through a web browser to perform personnel and payroll tasks. The FPPS functionality of certain

applications are only accessible via the IBC or EXIM Bank intranets, and interconnections with the FPPS are outlined in the Interconnection Security Agreement and/or Memorandum of Understanding between EXIM Bank and IBC. The system is located and managed at U.S. Department of the Interior, Interior Business Center, Human Resources and Payroll Services, 7301 W Mansfield Ave. MS D-2000 Denver, CO 80235.

SYSTEM MANAGER(S): Nakia Burton, Deputy Chief Human Capital Officer (DCHCO)
Export-Import Bank of the United States, 811 Vermont Avenue NW, Washington, DC 20571
Email: Nakia.Burton@exim.gov

Telephone number: (202)565-3335

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: EXIM requests the information in this application under the following authorization: The Export-Import Bank Act of 1945, as amended (12 U.S.C. 635 et seq.); 5 U.S.C. 5101, et seq., 5501 et seq., 5525 et seq., and 6301 et seq.; 31 U.S.C. 3512; Executive Order 9397 as amended by Executive Order 13478, relating to Federal agency use of Social Security numbers. 31 U.S.C. 3512 et seq.; and 5 C.F.R. Part 293; and Executive Order (EO) 14249, Protecting America's Bank Account Against Fraud, Waste, and Abuse.

PURPOSE(S) OF THE SYSTEM: EXIM Federal Personnel Payroll System (FPPS) processes EXIM's personnel, payroll, and time and labor data to facilitate payments, benefits, and pensions. FPPS also provides personnel and payroll data to the FPPS Datamart application which EXIM uses to perform queries and report on FPPS information.

FPPS is an online personnel and payroll system providing support to Federal agency customers through interagency agreement with the IBC. FPPS is customized to meet customer needs for creating and generating the full life cycle of personnel transactions. FPPS allows for immediate updates and edits of personnel and payroll data. FPPS also handles regulatory requirements such as specialized pay, garnishments, and special appointment programs. FPPS also operates in batch mode for performing close of business, payroll calculation, and other processes. FPPS customers

can use a web-enabled interface, WebFPPS, to access FPPS through a web browser to perform personnel and payroll tasks. FPPS is a major application that consists of several minor applications to include time and attendance applications, a system for creating retirement cards and updating retirement records, a system for converting client data for integration into FPPS. The purpose of this system is to ensure proper payment of salary and benefits to EXIM personnel, and to track time worked, leave, or other absences for reporting and compliance purposes. Use of this system will streamline EXIM Bank's personnel, payroll and other human resources functions into a unified, secure system, thereby improving employee input into these systems while enhancing data integrity and security and improving operational efficiency.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The FPPS system data contains Personally Identifiable Information (PII) on current and former EXIM Bank employees, including volunteers and emergency employees, and limited information regarding employee spouses, dependents, emergency contact, or in the case of an estate, a trustee.

CATEGORIES OF RECORDS IN THE SYSTEM: Categories of Records in the FPPS

System include:

- Name,
- Citizenship
- Sex
- Birth Date
- Marital Status
- Other Names Used
- Truncated SSN
- Legal Status
- Place of Birth
- Security Clearance
- Spouse Information

- Financial Information
- Medical Information
- Disability Information
- Education Information
- Emergency Contact
- Race/Ethnicity
- Social Security Number (SSN)
- Personal Cell Telephone Number
- Personal Email Address
- Home Telephone Number
- Employment Information
- Military Status/Service
- Mailing/Home Address
- Taxpayer Identification Number
- Bank Account Information such as Routing and Account Numbers
- Beneficiary Information
- Savings Bond Co-Owner Name(S) and Information
- Family Member and Dependents Information
- Professional Licensing and Credentials
- Family Relationships
- Age
- Involuntary Debt (Garnishments or Child Support Payments)
- Court Order Information
- Back Pay Information
- User ID

- Time and Attendance Data
- Leave Time Information
- Employee Common Identifier (ECI)
- Volunteer Emergency Contact Information
- Person Number which is a unique number that identifies a person within FPPS
- Person Number-Emergency which is a unique number identifying an individual within FPPS for a Leave Share Occurrence
- Person Number-Volunteer which is a unique number identifying an individual within the FPPS Volunteer Database.

RECORD SOURCE CATEGORIES: The source of the information maintained in EXIM FPPS is the Individual/employee, HR staff personnel and other: state courts for garnishments.

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: Data maintained in FPPS will be stored electronically by IBC. Data is protected by the following electronic security systems: Password, Firewall, Encryption, User ID, Intrusion Detection System, Virtual Private Network (VPN), Public Key Infrastructure (PKI) Certificates, Personal Identity Verification (PIV) Card.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: FPPS authorized users, including EXIM authorized Human Capital personnel, may retrieve information on an individual using full name, SSN and Employee Common Identifier (ECI).

Certain personnel within EXIM and IBC, involved in operations and maintenance of FPPS payroll operations, can retrieve information on an individual using:

- ECI - unique number identifying employees across Federal automated systems
- SSN and full name
- Person Number - unique number which identifies a person within FPPS
- Person Number-Emergency - unique number identifying an individual within FPPS for a leave share occurrence
- Person Number-Volunteer - unique number identifying an individual within the FPPS volunteer database
- Taxpayer Identification Number (TIN) - unique number identifying a trustee for the estate of a deceased employee

Additionally, reports can be produced on an individual containing many of the data elements in FPPS. FPPS also routinely generates a variety of reports related to employment that are required by law, such as Internal Revenue Service (IRS) forms (1099- MISC and W-2); reports of withholdings and contributions for benefits and union dues; and reports on individuals who are delinquent on child-support payments. Access to the reports is limited to employees who process or file the reports and individuals who are granted access on a need-to-know basis. Copies of the reports may also be provided to government entities as required by law, such as tax forms to the IRS.

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.

EXIM Bank is responsible for purging employee data according to the records schedule after an employee's access authority is terminated or the employee retires, changes jobs, or dies. The IBC may purge or delete any customer payroll or personnel records if it is agreed upon in the Inter-Agency Agreement with the IBC.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

- Information about individuals whose data is in FPPS cannot be retrieved without knowing specific information about the employee. FPPS supports a full suite of human resources functions, including calculating payroll. The data in FPPS is necessary to perform those functions and to comply with related Federal laws and regulations. To prevent misuse, (e.g., unauthorized browsing) EXIM Bank signed a Service Level Agreement (SLA) with the IBC to clearly establish and document IBC and client security roles and responsibilities. Most of the employee data in FPPS is collected from individuals and entered into FPPS by an authorized Federal human resource professional with access to the system.
- Access to FPPS related records is restricted to HR personnel. Access to the records is restricted to those with specific roles in the Personal Identity Verification (PIV) process, requires access to background investigation forms to perform their duties, and who have been given a password and PIV card to access applicable files within the system.
- The FPPS system has undergone a formal Security Authorization and Accreditation and has been granted an authority to operate by DOI in accordance with FISMA and NIST standards. FPPS is rated as FISMA moderate based upon the type of data, and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system.
- The security of the information being stored and transmitted in FPPS is protected through the use of FIPS 140-2 approved encryption mechanisms.

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: 82 FR 20878 (May 4, 2017).

Lin Zhou,

Information System Security Manager (ISSM).

Billing Code 6690-01

