6690-01-P]

EXPORT IMPORT BANK OF THE UNITED STATES

Privacy Act of 1974; System of Records

AGENCY: Export Import Bank of the United States.

ACTION: Notice of a new 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 a new system of records notice ("SORN"). The new system of records described in this notice, EXIM PERSEC IQ, will enable EXIM's Security Office staff to store and manage EXIM personnel security information, manage the integrated workflow processes and activities, manage caseloads, and reporting capabilities relative to personnel security investigations. Records in the system are used to document and support decisions regarding the suitability, eligibility, and fitness of applicants for Federal and contract employment to include students, interns, or volunteers to the extent that their duties require access to Federal facilities, information, systems, or applications. Additionally, records may be used to document security violations and supervisory actions taken. Information contained in PERSEC IQ includes but is not limited to: Employment records, education history, credit history, subjects' previous addresses, names of friends, neighbors, and associates, selective service records, military history, citizenship, pre-employment waivers, Background Investigations (BIs), security clearances, Sensitive Compartmented Information (SCI) access, clearance receipts (reciprocity), reinvestigations, completion dates of various security checks, and adjudication status/notes and decisions.

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 record system and 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 new system of records described in this notice, EXIM PERSEC IQ, will enable EXIM's Security Office staff to store and manage EXIM

personnel security information, manage the integrated workflow processes and activities, manage caseloads, and reporting capabilities relative to personnel security investigations.

The report of a new 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).

SYSTEM NAME AND NUMBER: System Name: EXIM PERSEC IQ. System Number: N/A

SECURITY CLASSIFICATION: This System will not house any classified information**.**

SYSTEM LOCATION: Export Import Bank of the United States (EXIM) is the system customer located at 811 Vermont Avenue NW, Washington, DC 20571. The system PERSEC IQ (aka “Entellitrak”) is hosted in the Tyler Federal Product Suite FedRAMP environment at:

- Primary: Equinix Colocation Center 44470 Chilum Place, DC3 bdg3, Ashburn, VA 20147
- Alternate: Amazon AWS US-West-2 FedRAMP hosting environment

SYSTEM MANAGER(S): Selma Hamilton, Director, Security Services, 811 Vermont Avenue NW, Washington, DC 20571, telephone number 202-565-3313.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: EXIM maintains 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. Relative to the purpose of your investigation, the U.S. government is authorized to request this information under Executive Orders: 10865, 12333, 12356, and 13764. Sections 3301 and 9101, of title 5, U.S. Code; section 2165 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 21, 2004.

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

Forms: SF-85, SF-85P, SF-86, SF-87. Amending the civil service rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch governance structure and processes for security clearances, suitability and fitness for employment, and credentialing and related matters.

PURPOSE(S) OF THE SYSTEM: Records in the system are used to document and support decisions regarding the suitability, eligibility, and fitness for services of applicants for Federal employment and contract positions to include students, interns, or volunteers to the extent that their duties require access to federal facilities, information, systems, or applications. Additionally, records may be used to document security violations and supervisory actions taken.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals who require regular, ongoing access to Federal facilities, information technology systems, or information classified in the interest of national security, including applicants for employment or contracts, federal employees, temporary hires, contractors, students, interns (both paid and unpaid), volunteers, affiliates, individuals authorized to perform services provided in EXIM facilities (e.g., building security, office cleaning, building contractors, etc.), and individuals formerly in any of these positions. The system also includes individuals accused of security violations or found in violation.

CATEGORIES OF RECORDS IN THE SYSTEM:

- Full Name,
- Former names,
- Date of birth,
- Birthplace,
- Social Security number,
- Home address,
- Phone numbers,
- Employment history,

- Residential history,
- Education and degrees earned,
- Names of associates,
- References and their contact information,
- Citizenship,
- Names of relatives,
- Birthdates and birth places of relatives,
- Citizenship of relatives,
- Names of relatives who work for the Federal government,
- Criminal history,
- Mental health history,
- History of drug use,
- Financial information,
- Fingerprints,
- Summary report of investigation,
- Results of suitability decisions,
- Level of security clearance(s) held,
- Date of issuance of security clearance,
- Requests for appeal,
- Witness statements,
- Investigator's notes
- Credit reports
- Security violations,
- Circumstances of violation, and agency action taken.
- SF-85, SF-85P

- SF-86, SF-86C
- OF-306

RECORD SOURCE CATEGORIES: The Defense Counterintelligence Security Agency's (DCSA) National Background Investigation System (NBIS) will provide a conduit for applicants to submit a full disclosure of PII (reference list of PII collected under sec. Categories of Records in the System) through the Electronic Application (e-APP). e-APP is an electronic form that is downloaded by the applicant/employee; the applicant/employee populates the form, and the information is transferred to EXIM via an encrypted file transfer. e-APP records an applicant record in PERSEC IQ system upon the applicants' completion. The following Government-created general service forms, and EXIM forms will be used.

- OF-306, Declaration for Federal Employment: This form collects Name, SSN, DOB, POB, Citizenship, Responses to Criminal, Financial, Employment, Military status.
- EXIM Fair Credit Reporting Act: This document collects applicant name, SSN, and signature for acknowledgement to collect Credit information on this form.
- General Services Administration (GSA) USAccess Criminal History Results: This record collects information on applicants' national criminal history.

Information is obtained from a variety of sources including the employee, contractor, or applicant through use of the SF–85, SF–85P, SF–86, or SF–86C and personal interviews; employers' and former employers' records; FBI criminal history records and other databases; financial institutions and credit reports; medical records and health care providers; educational institutions; interviews of witnesses such as neighbors, friends, co-workers, business associates, teachers, landlords, or family members; and other public records. Security violation information is obtained from a variety of sources, such as security inspections, witnesses, supervisor's reports, audit reports.

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 by EXIM 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. 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.

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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: The records are stored digitally in encrypted format in PERSEC IQ's Amazon Web Services (AWS) FedRAMP authorized cloud environment. PERSEC IQ encrypts EXIM's sensitive information (such as employee or contractor first name, last name, and email address) at rest and stores it in Amazon

Relational Database Service (RDS) AWS databases. Data in transit is encrypted via TLS. PERSEC IQ also leverages AWS Key Management Service (KMS) to encrypt data and restrict access based on user roles and job functions.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Comprehensive electronic records are maintained by the Security Office and stored in the PERSEC IQ electronic database. Access to the records is restricted to those with specific roles in the Single Sign-On process. Retrieval of electronic records will require an individual name or social security number query to produce records of an employee, contractor, student, intern, or volunteer.

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.

Comprehensive records are retained and disposed of in accordance with General Records Schedule 5.6 items: 180,181under Disposition Authority DAA-GRS-2017-0006-0025, approved by the National Archives and Records Administration (NARA). Records regarding individuals with security clearances and other clearances for access to Government facilities or to sensitive data, created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program will be destroyed 5 years after the employee or contractor relationship ends, however longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

- For Paper Records: Comprehensive paper records are kept in locked metal file cabinets in locked rooms in EXIM's Headquarters, in the Security Services Unit which is the office responsible for suitability determinations. Access to the records is limited to Security Services Unit employees who need them in performing their official duties.

- For Electronic Records: Comprehensive electronic records are kept in the Personnel Security Division. 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 including background investigation records. An electronic audit trail is maintained within the system and reviewed periodically to identify and track authorized/unauthorized access. Persons given roles in the PIV process must complete training specific to their roles to ensure they are knowledgeable about handling and safeguarding individually identifiable information.
- For Electronic Records (cloud based): Information will be stored in electronic format within the PERSEC IQ Cloud Service Provider (CSP) Amazon Web Service (AWS). EXIM PERSEC IQ has configurable, layered user accounts and permissions features to ensure users have only the proper access necessary to perform their duties. Access to EXIM PERSEC IQ is restricted to EXIM employees and contractors who need it for their job functions. Authorized users have access only to the data and functions required to perform their job functions. PERSEC IQ uses AWS Key Management Service (KMS), a managed service for PERSEC IQ to create and control the cryptographic keys that are used to protect EXIM data. AWS KMS uses hardware security modules (HSM) to protect and validate AWS KMS keys under the FIPS 140-2 Cryptographic Module Validation Program to implement cryptography for data at rest. AWS KMS enables PERSEC IQ to maintain control over who can use PERSEC IQ AWS KMS keys and gain access to EXIM encrypted data. Keys distributions are only permitted on the AWS Console Layer. Lost or corrupted keys are managed by AWS KMS. EXIM PERSEC IQ which is hosted in AWS as a Software-as-a-Service application inherits all the administrative, technical, and physical controls offered by AWS and the EXIM Infrastructure General Support System. PERSEC IQ is compliant with the Federal Risk and Authorization Management

Program (FedRAMP). The PII information in EXIM PERSEC IQ is encrypted and stored in AWS, and the Hypertext Transfer Protocol Secure (HTTPS) protocol is used to access EXIM PERSEC IQ.

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:

- Name.
- Type of information requested.
- Address to which the information should be sent; and
- Signature.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

Lin Zhou,

Information System Security Manager.

Billing Code 6690-01

[FR Doc. 2025-04894 Filed: 3/20/2025 8:45 am; Publication Date: 3/21/2025]