



EXPORT IMPORT BANK OF THE UNITED STATES

Privacy Act of 1974; New 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”) is proposing a new system of records notice (“SORN”). EXIM Bank is proposing a new system of records – EXIM AgilQuest. This new SORN will include the authorities for maintenance of the system, the purposes of the system, and the categories of entities and individuals covered by the system. The new system of records described in this notice, EXIM AgilQuest, will collect information for current employees and contractors of the Bank to support a hybrid (onsite & telework) working environment.

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 eRulemaking 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 Ave. 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 Ave. NW, Washington, DC 20571.

FOR FURTHER INFORMATION CONTACT: The Office of the General Counsel, Administrative Law Group at OGCAdminlaw@exim.gov, or by calling 202-565-3168, or by going to <https://www.exim.gov/about/freedom-information-act/privacy-act-requests/pia-notice-assessments>.

SUPPLEMENTARY INFORMATION:

The new system of records described in this notice, EXIM AgilQuest, will store certain information of current employees and contractors of the Bank to support a hybrid (onsite & telework) working environment. 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 AgilQuest, System Number: N/A

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: This electronic system will be used via a web interface and mobile application by the Export Import Bank of the United States, 811 Vermont Avenue NW,

Washington, DC 20571. The physical location and technical operation of the system is at the FedRAMP Authorized Amazon Web Services (AWS) cloud services facility at 410 Terry Ave N, Seattle, WA 98109-5210.

SYSTEM MANAGER(S): Tomeka Wray, Vice President of Operations, EXIM Bank, 811 Vermont Avenue NW, Washington, DC 20571, tomeka.wray@exim.gov, 202-565-3996.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Export-Import Bank Act of 1945, as amended (12 U.S.C. 635 et seq.).¹ 5 U.S.C. 301.

PURPOSE(S) OF THE SYSTEM: The purpose of this system of records is to facilitate the hybrid workforce environment by allowing EXIM employees and contractors to reserve agency workspaces such as “Touchdown Spaces”, “Collaboration Spaces/Meeting Rooms”, and Information Technology (IT) assets. The system will provide employees with increased flexibility and access to workspaces while providing the agency with space utilization information to make data-driven decisions for facilities operations and capital planning.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The EXIM AgilQuest system will contain information on EXIM current employees and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM: The EXIM AgilQuest system will contain Personally Identifiable Information (PII) of EXIM current employees and contractors, necessary to obtain an account and reserve workspaces relevant to their division and job functions. Records maintained in this system may contain employee and contractor information including, but not limited to, name, agency email address, agency phone number, location (e.g., EXIM Headquarters or satellite location), and organization/division/office of assignment. Individuals may voluntarily provide additional contact information through the EXIM AgilQuest online portal such as picture, preferred name, additional phone numbers, and EXIM work groups.

RECORD SOURCE CATEGORIES: Information in this system is obtained using one of three methods: manual entry by an administrator user, direct database connection to supply the

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

required information, and through employee or contractor entry of optional data to their individual profile.

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:

1. Appropriate agencies, entities, and persons when (a) the Bank suspects or has confirmed that there has been a breach of the system of records; (b) the Bank has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Bank (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Bank's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
2. Another Federal agency or Federal entity, when the Bank 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.
3. The Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf.

4. Congressional offices in response to an inquiry made at the request of the individual to whom the record pertains.
5. Contractors or other authorized individuals performing work on a contract, service, cooperative agreement, job, or other activity on behalf of the Bank or Federal Government and who have a need to access the information in the performance of their duties or activities.
6. The U.S. Department of Justice (DOJ) for its use in providing legal advice to the Bank or in representing the Bank in a proceeding before a court, adjudicative body, or other administrative body, where the use of such information by the DOJ is deemed by the Bank to be relevant and necessary to the advice or proceeding, and in the case of a proceeding, such proceeding names as a party in interest: (a) The Bank; (b) Any employee of the Bank in his or her official capacity; (c) Any employee of the Bank in his or her individual capacity where DOJ has agreed to represent the employee; or (d) The United States, where the Bank determines that litigation is likely to affect the Bank or any of its components.
7. 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.
8. Appropriate Federal, State, local, foreign, tribal, or self-regulatory organizations or agencies responsible for investigating, prosecuting, enforcing, implementing, issuing, or carrying out a statute, rule, regulation, order, policy, or license if the record indicates a violation or a potential violation of civil or criminal law, rule, regulation, order, policy, or license.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: The records are stored digitally in encrypted format in the AgilQuest Amazon Web Services (AWS) FedRAMP authorized cloud environment. AgilQuest 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. AgilQuest also leverages AWS Key Management Service (KMS) to encrypt data and restrict access based on user roles and job functions. AgilQuest complies with EXIM policy which stipulates that sensitive data generated from AgilQuest must be stored on EXIM’s Microsoft OneDrive and SharePoint site that are managed and protected by EXIM’s Infrastructure General Support System administrative, technical, and physical controls.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by other users by using the employee’s name. Records may be retrieved by administrator/superusers by the following: first or preferred name, last name, email address, Location (e.g., Headquarters or satellite location), and user role. Information may additionally be retrieved by other personal identifiers by user account maintenance programs within the application.

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.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Information will be stored in electronic format within the AgilQuest Cloud Service Provider (CSP) Amazon Web Service (AWS). EXIM AgilQuest has configurable, layered user accounts and permissions features to ensure users have only the proper access necessary to perform their duties. Access to

EXIM AgilQuest 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. AgilQuest uses AWS Key Management Service (KMS), a managed service for AgilQuest 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 (<https://csrc.nist.gov/projects/cryptographic-module-validation-program>) to implement cryptography for data at rest. AWS KMS enables AgilQuest to maintain control over who can use AgilQuest 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 AgilQuest 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.

AgilQuest CSP, is compliant with the Federal Risk and Authorization Management Program (FedRAMP). The PII information in EXIM AgilQuest is encrypted and stored in AWS, and the Hypertext Transfer Protocol Secure (HTTPS) protocol is used to access EXIM AgilQuest.

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 Ave. 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 Ave. 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 Ave. 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
4. Signature

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

EXPORT-IMPORT BANK OF THE U.S.

Christopher Sutton,

Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO),

IT Security Systems & Assurance Unit.

[FR Doc. 2023-22384 Filed: 10/6/2023 8:45 am; Publication Date: 10/10/2023]