6690 – 01 – P]

EXPORT-IMPORT BANK

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 Emergency Notification System. 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 Emergency Notification System using OnSolve Platform for Critical Event Management (PCEM), will collect information for current employees and contractors of the Bank for emergency notification, information technology alerting, and disaster recovery to support effective communication and management of critical alerts, and to keep EXIM employees and contractors safe, informed, assured, and productive during an event/incident or crisis.

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 202-329-2052, or by going to EXIM Bank Privacy Act System of Records Notice. You may also contact Selma Hamilton, Director, Security Services at Selma.Hamilton@exim.gov or 202-565-3313.

SUPPLEMENTARY INFORMATION: The new system of records described in this notice, EXIM Emergency Notification System, will store certain information about employees and contractors of the Bank for emergency notification, information technology alerting, and disaster recovery to support effective communication and management of critical alerts, and to keep EXIM employees and contractors safe, informed, assured, and productive during an

event/incident or crisis.

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 Emergency Notification System

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) US East/West cloud services facility at 410 Terry Ave N, Seattle, WA 98109-5210.

SYSTEM MANAGER(S):

Selma Hamilton, Director, Security Services, EXIM Bank, 811 Vermont Avenue NW, Washington, DC 20571, Selma.Hamilton@exim.gov, 202-565-3313.

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 and enable EXIM to communicate with its employees and contractors ("Contacts") in a quick and efficient manner in critical events. EXIM utilizes EXIM Emergency Notification System to ensure employee safety and business continuity, as well as swift disaster recovery during critical events. EXIM uses contact information of its employees and contractors (typically name, telephone number, email addresses and/or physical address, which is stored within OnSolve Platform for Critical Event Management (PCEM)) and use the system to communicate alerts using multiple modalities (including SMS, email, and voice collectively referred to herein as "alerts") to the Contacts at scale.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The EXIM Emergency Notification System will contain information on EXIM current employees and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:

The EXIM Emergency Notification System will contain Personally Identifiable Information (PII) of EXIM current employees and contractors typically including, but not limited to name, telephone number, email addresses and/or physical address/location, and travel data such as dates and locations of travel

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

captured through manual entry or an API (Application Programming Interface) from EXIM Travel Reservation Management system (Concur). This information will be necessary to enable EXIM to identify and communicate with EXIM staff and other persons having connections with EXIM ("Contacts" or "Recipients") in a quick and efficient manner to ensure employee safety and business continuity, as well as swift recovery during critical events.

RECORD SOURCE CATEGORIES:

The information in the system is obtained using one of three methods: (1) Active Directory (AD) user data will be used as the initial source of information for the database to create users, (2) additional user information will be entered by the user via the user account "opt-in" portal, and (3) data captured through manual entry or an API (Application Programming Interface) from EXIM Travel Reservation Management system (Concur). User accounts are created individually within the OnSolve portal or uploaded via SFTP from an Active Directory export using System Center Orchestrator (SCOrch).

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. Congressional offices in response to an inquiry made at the request of the individual to whom the record pertains.
4. 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.
5. 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.
6. 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.
7. 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 OnSolve PCEM Amazon Web Services (AWS) FedRAMP authorized cloud environment. OnSolve PCEM encrypts EXIM's sensitive information (such

as current employee or contractor first name, last name, and email address) at rest and stores it in the databases leveraging native AWS encryption including Database (DB) clusters, snapshots, underlying structure for DB clusters. Automated database backups are in place along with read replica. Native AWS encryption on storage level with an encrypted Elastic Block Storage (EBS) volume using Advanced Encryption Standard (AES)-256). For live data (not in a backup file) Elastic File System (EFS) is used. EXIM Emergency Notification System complies with EXIM policy which stipulates that sensitive data (such as routine reports) generated from EXIM Emergency Notification System must be stored on EXIM's storage system that is 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 the system administrator using Contact's (EXIM employee and contractor) first name, last name, work email address, as well as non-key attributes such as location (e.g., Headquarters or Regional Offices), to identify lists of potentially impacted contacts with a nexus to a critical event. Information may additionally be retrieved by other personal identifiers by user account maintenance programs within the application. The administrator runs routine reports and reviews analytics that include user unique identifiers such as name and phone number, etc. Reports can be filtered using a personal identifier (i.e., reports can be generated to indicate who responded to a notification message).

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 OnSolve PCEM Cloud Service Provider (CSP) Amazon Web Service (AWS). EXIM Emergency Notification System has configurable, layered user accounts and permissions features to ensure users have only the amount of access necessary to perform their duties. Access to EXIM Emergency Notification System is restricted to EXIM current employees

and contractors for emergency notification, information technology alerting, and disaster recovery to support effective communication. OnSolve PCEM users use HTTPS through CloudFlare DNS to access the application using an Internet Browser. EXIM AD Data daily sync is performed using SFTP one direction initiated from EXIM only.

OnSolve PCEM personnel access the AWS US East/West OnSolve Platform CEM environment via VPN to meet FIPS 140-2 Cryptographic Module Validation Program requirements at https://csrc.nist.gov/projects/cryptographic-module-validation-program. Multi-factor authentication is implemented on personal mobile devices (only) for CSP administrators to authenticate. VPN Authentication occurs at the VPN located in the public subnet in the authorization boundary. After establishing the VPN connection, the administrator establishes an SSH connection to remote desktop into a Jump Host, within the Jump Host subnet. Personnel must supply their username and password provided by a dedicated Active Directory, specifically used for this AWS environment (i.e., not the corporate Active Directory). If someone were to leave the organization or no longer require access, that individual's jump host can be deleted. Jump Hosts authenticate against Vault (within a management services subnet in the OnSolve AWS cloud environment) to establish access. Vault checks Active Directory to validate the login information that has been provided by the user and returns an SSH-signed certificate token/key that expires after 12 hours. Vault also stores "secrets" to the environment. For example, all the database passwords for database users are stored in Vault. The Jump Host is allowed access into all other subnets for administrative purposes just as if the 12-hours token has not expired.

OnSolve PCEM, 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.

OnSolve PCEM CSP is compliant with the Federal Risk and Authorization Management Program (FedRAMP). The PII information EXIM Emergency Notification System is encrypted and stored in AWS, and the Hypertext Transfer Protocol Secure (HTTPS) protocol and Security Assertion Markup Language (SAML) authentication is used to access EXIM Emergency Notification System.

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:

- 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,

IT Specialist.

Billing Code 6690-01

[FR Doc. 2024-03908 Filed: 2/26/2024 8:45 am; Publication Date: 2/27/2024]