Privacy Impact Assessment (PIA)
Public Version

EXIM Emergency Notification System (EENS)

Version 1.0

January 2026

Introduction

The Export-Import Bank of the United States (EXIM) requires PIAs to be created and maintained on all IT systems that collect, store, process or transfer personally identifiable information (PII).

The system owner has completed this assessment in compliance with Section 208 of the E-Government Act of 2002 ("E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget (OMB) Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

Name of the system: EXIM Emergency Notification System (EENS)

System Description:
EXIM Emergency Notification System (EENS) uses the OnSolve Critical Event Management (CEM) platform, a cloud-based Software as a Service (SaaS) solution hosted within the Amazon Web Services (AWS) US East/West cloud environment, compliant with the FedRAMP Moderate baseline for security. EENS enables EXIM to quickly and efficiently communicate with employees and contractors via multiple channels, including SMS, email, and voice alerts to connected devices. By utilizing the OnSolve CEM platform, EXIM enhances employee safety, ensures business continuity, and supports rapid disaster recovery during critical events.

Legal Authority:
FISMA ACT of 2014 (Public Law No: 113-283 (12/18/2014), and OMB A-130.

Export-Import Bank Act of 1945, as amended (12 U.S.C. 635 et seq.).1 5 U.S.C. 301.

Characterization of the Information Collected:

- **Describe all uses of the PII:**
  The contact information is used to communicate alerts using multiple modalities (including SMS, email, and voice) to the employees and contractors in case of an emergency. EXIM employees and contractors provide EENS with their respective contact information (typically including name, telephone number, email addresses and/or physical address, which is stored within EENS.

- **From whom will the information be collected?**
  EXIM Active Directory user data will be used as the initial source of information for the database to create users.

Additional user information will be entered by user via user account portal. EXIM will provide a file (in CSV format) daily via SFTP EENS to update the user database. Note that personal non-bank information will be provided by the user. It will be not synced from AD.

- **What specific data will the system collect?**
  Some information used in the EENS will come from EXIM Active Directory (AD) and consist of First Name, Last Name, Unique ID, Job Title, Company Name, Division, Work Phone, Work Mobile, Email, Work Address, Work City, Work State, Work Zip Code, Employee Type, Office, and Desktop alert.

  Additional information will be provided by user through the User Account Management Portal as part of the Opt-in process or via an automated process and future integration with EXIM Travel Reservation Management system. The additional information includes user home physical address, user personal email address, user personal home and cell phone numbers, company number, company name, data type, and record locator. Other information from hotel reservation includes start date & time, stop date & time, hotel name, hotel address, hotel city, hotel postal code, hotel state/province (if applicable), and hotel country code; Air Travel Reservation information includes flight number, carrier, start date & time UTC, stop date & time UTC, stop location code, and start location code; Rail Travel Reservation information includes operator, train number, start location code, stop location code, start date & time UTC, and stop date & time UTC. The above information will be used to transmit official notification to EXIM staff and contractors

- **With whom will the information be shared, both within EXIM and externally?**
  Internally: Access to data is determined by an individual's role. All users have access to their respective "optin" data via the portal and all other are provided by AD synced daily. Role-based access is implemented throughout the environment so that everyone has access to data necessary to complete their job functions. Access Control procedures are documented in the EENS Access Control Standard Operating Procedure. Access for roles with elevated viewing rights requires manager approval. A user defined as a "contact" cannot initiate any communication to other contacts, a "Contact" simply responds when contacted, an "initiator" initiates messaging alerts to assigned "contact" user/s. The administrator can perform the role of "initiator" and receives messaging alerts. In addition, the administrator has all the privileges required to manage the system.

  Externally: No external user can access the data stored in EENS.

Privacy Risks and Mitigation Strategies:

- **Does the system derive new data or create previously unavailable data about individuals through aggregating or consolidating this data with data from other**

sources? Yes [ ] No [x]

- **<u>For data that is collected other than directly from the user, how is the integrity and accuracy of the data collection assured</u>?**

  N/A - This system has been assessed and authorized in accordance with applicable federal information security requirements. All security controls have been implemented, tested, and evaluated in alignment with the NIST Risk Management Framework (RMF) as defined in NIST Special Publications 800-37, 800-53, and associated guidance. The organization has completed a comprehensive Security Assessment Report (SAR) and Plan of Action and Milestones (POA&M) in accordance with NIST SP 800-53A and maintains continuous monitoring activities consistent with NIST SP 800-137.

  The Assessment and Authorization process complies with OMB Circular A-130, OMB Memorandum M-17-25, and all relevant federal policies governing the management of federal information systems. An Authorizing Official (AO) has reviewed the security posture and risk determination and has issued an Authorization to Operate (ATO) contingent upon ongoing adherence to federal cybersecurity requirements. The system is subject to continuous monitoring, annual assessments, and periodic updates, ensuring ongoing compliance with NIST and OMB standards.

- **Describe the retention periods for data in this system:**
  During the term of the service agreement, absent any changes or instructions from the data controller, OnSolve will retain all personal data provided by the data controller. Upon termination of the service agreement with the data controller, all personal data associated with the account will be deleted within 90 days. The contents of the alerts sent via the OnSolve Platform system are not regularly deleted. Upon termination of the service agreement with the data controller, any metadata containing personal information associated with alerts retained by OnSolve is permanently obfuscated within 90 days.

Privacy Act Applicability; System of Records Notice (SORN) Requirement:

- **Is information retrieved from the system by using a name or a "unique identifier", or other PII linked to an individual? Yes [x] No [ ]**

  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.

- **Is this system operated under a System of Records Notice (SORN) either specific to this system, or part of another SORN? Yes [x] No [ ]**

  The SORN is listed in the Federal Register as 89 FR 14487

To contact the EXIM Bank Senior Agency Official for Privacy (SAOP) use:
fismasaop@exim.gov