Privacy Impact Assessment (PIA)
(Public Version)

EXIM Financial Management System – Next Generation (FMS-NG)

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: Financial Management System – Next Generation (FMS-NG)

System Description:
Financial Management System – Next Generation (FMS NG) is the Export Import Bank of the United States (EXIM)'s modern internal financial management platform. It integrates administrative services—such as budget execution and procurement—with client-facing functions including preauthorization, interest accrual, billing, claims management, and rescheduling. Built as a commercial off-the-shelf (COTS) Fiscal Intermediary Services Organization (FISO) product that is compliant with credit reform, FMS NG leverages Oracle Federal Financials and Oracle Loans.

Legal Authority:
Authority of the Export-Import Bank Act of 1945, as amended (12 U.S.C. 635 et seq.), Executive Order 9397 as amended by Executive Order 13478 signed by President George W. Bush on November 18, 2008, relating to Federal agency use of Social Security Numbers.

Characterization of the Information Collected:

- **Describe all uses of the PII:**
  FMS-NG data is used by Treasury for payment processing and legally required Federal Reporting. FMS-NG tracks credits from obligation through maturity and termination. FMS-NG processes loan, guarantees, and insurance policies from obligation through final disbursement/payment, write-off, or Claim/Rescheduled Debt Servicing System application creation. It includes EXIM's cash control system and standard general ledger. As described above, the data contained in this application may be extracted and summarized in statistical and textual summaries and reports that do not identify the individuals or the Company's business confidential information. Additionally, summarized extracts of the data will be shared for search and display on the Federal Funding Accountability and Transparency Act (FFATA)web portal, at which point the

summary data will not contain any PII.

- **From whom will the information be collected?**

  Primarily data is sourced from interconnected EXIM financial business systems i.e., EXIM Online, ELMS, APS & Comprizon. The accuracy of the individual and business records is verified by the individuals at the time of data entry. The entries may be subsequently updated as needed. Specifically, PII information is voluntarily disclosed by EXIM employees seeking reimbursement of the authorized expenses by entering it in the 'Authorization for Direct Deposit' form. It is the employees' responsibility to ensure that the financial information they provide is accurate and up to date. The same applies to invitational travelers who are seeking reimbursements for the pre-authorized expenses incurred while speaking at or attending a function at the request of EXIM. It is the individual's responsibility to ensure that the financial information they provide for the purpose of receiving a direct deposit reimbursement is accurate.

- **What specific data will the system collect?**

  FMS-NG contains customer information related to the financial obligations of the Bank to and from individuals and corporate entities, starting from the point of obligation through final disbursement. It provides complete loans and guarantees servicing throughout the entire life of a credit. The FMS-NG system stores Personally Identifiable Information (PII) about Ex-Im Bank employees, public individuals with pre-authorized reimbursable expenses, Ex-Im product applicants, contracted suppliers, and other business partners.

  1. Administrative and Employee-Related Records

     These records relate to employees and individuals who receive payments, reimbursements, or other financial actions through FMS-NG:

     - Employee Name
     - Employee Address
     - Employee email address
     - Employee Phone Number
     - Employee Bank Account Number (for payroll or reimbursements)
     - Travel reimbursement and expense records linked to an identifiable individual

  2. Vendor / Payee Records (Individuals and Sole Proprietors Only)

The following records are included only when the vendor or payee is an individual or sole proprietor, and the record is retrieved using an individual identifier:

- Individual Vendor Name
- Vendor ID assigned to an individual
- Tax Identification Number (individual or sole proprietor)
- Bank Account Holder Name (individual only)
- Bank Account Number
- Bank Routing/SWIFT Code

3. Individual Beneficiary or Applicant Records

   - Records related to individuals who receive or apply for EXIM financial services, disbursements, or program benefits:
   - Name
   - Address
   - Contact Information
   - Payment or disbursement information
   - Records necessary to determine eligibility or process financial transaction

- **With whom will the information be shared, both within EXIM and externally?** Following EXIM business category roles: Budget (Manager Role and User Role); Payables (Manager Role and User Role); Purchasing (Manager Role and User Role); General Ledger (Manager Role and User Role); CRM Resource Manager Role; Credit Administration User Role; Functional Manager Role; HRMS Manager Role; Loan Guarantee Servicing User Role; Portfolio Manager Role; and Receivables User Role Business roles with the approval from Office of Chief Financial Officer (OCFO) are granted to OCFO staffs to perform their assigned duties in the system. The System Administrator role is assumed by Application Database Administrator to perform operational and maintenance tasks.

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 [x] No [ ]** ***If so, explain below*****:**
  FMS-NG data may be extracted and summarized in statistical and textual summaries and reports that do not identify the individuals or the Company's business confidential information. Additionally, summarized extracts of the data will be shared for search and display on the Federal Funding Accountability and Transparency Act (FFATA)web

portal, at which point the summary data will not contain any PII.

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

  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:**
  Retention policies of the EXIM Bank govern records. Therefore, regardless of whether these records are managed and retained in an information system as structured or unstructured data, on magnetic disks as flat files, or on paper, the same retention policies apply to the same kinds of records. Under normal circumstances, Transaction Records, including those in Docusign, are eligible for destruction seven (7) years after transaction termination per Records Schedule DAA-0275-2015-0001. FMS-NG data is considered a temporary Federal Record with the retention period subject to the applicable Record Schedules. FMS-NG is designed to mark records inactive when no longer required for EXIM business, whereupon these records become subject to the retention period as defined by the applicable Records Schedule. Records that are at the end of the specified legal retention period will be deleted by following the procedures documented in Oracle Financials Application Guides, based on the built-in criteria categories:
  • Invoice Purge Criteria
  • Payment Purge Criteria
  • Supplier Purge Criteria
  • Requisition Purge Criteria
  • Purchase Order Purge Criteria
  • Supplier Schedules Purge Criteria

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 [ ]**

  Primary access to FMS-NG data is via FMS-NG forms and reports. FMS-NG users that have been granted access can retrieve data by personal identifiers (e.g., Customer's EIN). The identifiers used are:
  • Name: Used as the unique identifier.
  • Banking Information: Employee and supplier bank account numbers are stored in a hashed/masked format (e.g., "XXXXXX9913").
  • Employee work email address: Work email address used for all employee records

- **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 85 FR 3372

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