

# **Privacy Impact Assessment (PIA)**

## **(Public Version)**

**EXIM Salesforce**



**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:** Salesforce

### **System Description:**

The Export-Import Bank of the United States (EXIM) uses Salesforce, a secure, cloud-based, FedRAMP-certified Software as a Service (SaaS) Customer Relationship Management (CRM) platform, hosted in the Salesforce Government Cloud Plus, to support its mission of facilitating U.S. exports and supporting American jobs. Salesforce enables EXIM staff to manage and track interactions with customers, partners, and stakeholders involved in financing transactions. Additionally, the platform supports relationship management with agencies, brokers, and lenders. EXIM also utilizes Salesforce’s Partner Relationship Management (PRM) module to operate the EXIM Partner Portal, where registered insurance brokers can access referrals, marketing materials, and collaborate with EXIM staff.

### **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:**

Individual names are used to facilitate and track interactions with them as representatives of companies/organizations. We have limited the PII we collect only to individual names—all other information is business information.

- From whom will the information be collected?**

Information is collected in a variety of ways:

- It is collected through interactions with EXIM staff by phone, email, or in person at trade shows or other events.

- It is also collected through individuals filling out EXIM web forms hosted by HubSpot and sent to Salesforce through the Salesforce-HubSpot integration.
- It is also collected through partner organizations who refer companies to EXIM (either entered into Salesforce by an EXIM staff member or received through our Salesforce-to-Salesforce connection with MBDA).
- Additionally, company information (no PII) is collected through our integration with D&B Connect which appends company information (DUNS Number, NAICS Code, number of employees, etc.) to company records.
- **What specific data will the system collect?**  
 The only PII collection is individual name (first & last name). The race/ethnicity of a company's owner is collected as part of the company's record, not the individual contact record. Additionally, we collect job titles, business emails, and business phone numbers. The majority of the information in Salesforce is company information including company name, address, Unique Entity Identifier (UEI), Dun & Bradstreet (D&B) Data Universal Numbering System (DUNS) identifier number, website, and North American Industry Classification System (NAICS) code. We also capture information and note about a company's potential, current, or former transactions with EXIM including which EXIM product(s), status, amount, and EXIM transaction number. A comprehensive list of data fields collected is documented in a Salesforce Objects worksheet which can be made available upon request.
- **With whom will the information be shared, both within EXIM and externally?**  
 Internal users are only those EXIM employees or contractors who need access to fulfill one or more of their job duties. This includes both regular users and admins/developers. The level of access they are given is based on their position, the documented separation of duties, and in accordance with the principle of "Least Privilege" where the user will be granted only the access they need and no more.  
  
 External users are specific staff members at EXIM partners who have access to specific records shared with them. They can see a limited number of data fields on those records. Data in the system may be shared with other partner organizations outside the system if EXIM is referring a company to that organization for assistance.

#### **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] *If so, explain below:***
- **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:**

Data in this system falls under records schedule GRS 6.5 Item 020, DAA-GRS2017-0002-0002. These records are temporary, and disposition is 'Delete when superseded, obsolete, or when customer requests the agency to remove the records.

**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  No**

Information is retrieve using Individual name (First Name, Last Name, or both First and Last Name).

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

The SORN is listed in the Federal Register as 86 FR 30933

**To contact the EXIM Bank Senior Agency Official for Privacy (SAOP) use:**

[fismasaop@exim.gov](mailto:fismasaop@exim.gov)