Privacy Impact Assessment (PIA)
(Public Version)

EXIM NICE inContact

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: NICE inContact

System Description:
NICE inContact is a multi-tenant, public-cloud SaaS solution hosted on the FedRAMP-authorized NICE CXone platform, employing a moderate baseline of security controls, and providing a comprehensive suite of contact center capabilities such as Automated Call Distribution (ACD), Interactive Voice Response (IVR), Computer Telephony Integration (CTI), and the Personal Connection Dialer (PCD). The EXIM Contact Center, part of EXIM's Office of Small Business, relies on NICE inContact to manage inbound and outbound calls, email responses, and website chat support. With its all-in-one, vendor-hosted model, NICE inContact enables EXIM to operate a robust contact center without significant upfront investment or ongoing maintenance, while still delivering advanced features to meet operational needs. Additionally, EXIM has seamlessly integrated NICE inContact with its Salesforce CRM using the platform's built-in integration tools, ensuring smooth connectivity and streamlined workflows.

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:**
  Information is collected on individuals for the purpose of creating, tracking, and researching their service requests. These individuals are people interested in learning more about EXIM's products including EXIM staff, potential or current customers, partners, and or other organizations and agencies involved in EXIM deals or whom

EXIM works with in supporting U.S. exporters.

- **From whom will the information be collected?**
  The information is collected directly from the caller/individual. The agent will obtain the information when the caller/individual contacts the Contact Center via phone or email.

- **What specific data will the system collect?**
  The agent will collect the caller/individual's Name, Phone, Email, Company Name, Company Address, Customer Type, Customer Status, Call Topic, Summary and Call Resolution

- **With whom will the information be shared, both within EXIM and externally?**
  Internally, information collected is shared with Administrators, Managers, Supervisors, Team Leads, and Agents. There will be no information shared externally.

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*:**

- **<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:**
  Records retention follows EXIM's agency-wide policies. Data in NICE inContact is

covered by the General Records Schedules (GRS) 6.5 Item 020 and DAA-GRS2017-0002-0002 records disposition authorities. Records are temporary and are deleted 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 [x] No [ ]**

  Information is retrieved using the caller/individual's Contact ID (Phone number).

- **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 86 FR 30933.

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