Privacy Impact Assessment (PIA)
(Public Version)

EXIM PERSEC IQ

Version 1.0

December 2025

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: PERSEC IQ

System Description:

PerSec IQ Built on the Tyler Technologies Application Platform powered by Entellitrak, PERSEC-IQ 1.0 allows users to execute all core workflows involved in the personnel security lifecycle from Intake Initiation to Adjudication Decision with full visibility. The streamlined collection of candidate information ensures smooth onboarding experience and reduced administrative burden. Users will be able to track case status, record changes, monitor workflow transitions with ease, compile information and/or documents, and route cases through the appropriate business processes. PERSEC-IQ 1.0's dynamic reporting feature also allows users to effortlessly extract essential data and insights.

Legal Authority:

EXIM maintains the information in this application under the following authorization: Export-Import Bank Act of 1945, as amended (12 U.S.C. 635 et seq.). 5 U.S.C. 301. Relative to the purpose of your investigation, the U.S. government is authorized to request this information under Executive Orders: 10865, 12333, 12356, and 13764. Sections 3301 and 9101, of title 5, U.S. Code; section 2165 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 21, 2004. Forms: SF-85, SF-85P, SF-86, SF-87. Amending the civil service rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch governance structure and processes for security clearances, suitability and fitness for employment, and credentialing and related matters.

Characterization of the Information Collected:

- **Describe all uses of the PII:**
  The PII is intended solely for processing and monitoring background investigations of Federal employees and contractor.

- **From whom will the information be collected?**
  The information will be manually entered into the PerSec IQ case management system by EXIM Security Office personnel. The information is derived from the forms submitted by the subject for the background investigation. Human Capital provides OF306 for all federal employees, the form contains PII. Once an individual's background investigation has closed, the closed case file will be added to the individual's case file.

- **What specific data will the system collect?**
  The PERSEC IQ collects the following data:
    - Full Name
    - Former names
    - Date of Birth
    - Birth of Place
    - Social Security Number
    - Home Address
    - Phone Numbers
    - Employment History
    - Residential History
    - Education and Degrees earned
    - Names of Associate
    - References and their contact information
    - Citizenship
    - Names of Relatives
    - Birthdates and Birth Places of Relatives
    - Citizenship of Relative
    - Names of relatives who work for the Federal government
    - Criminal History
    - Mental Health History
    - History of Drug Use
    - Financial Information
    - Fingerprints
    - Summary Report of Investigation
    - Results of Suitability Decisions
    - Level of Security Clearance(s) held
    - Date of Issuance of Security Clearance
    - Requests for Appeal
    - Witness Statements
    - Investigator's notes
    - Tax Return Information
    - Credit Reports
    - Security Violations

- Circumstances of Violation, and Agency Action Taken

- **With whom will the information be shared, both within EXIM and externally?** The information will remain within EXIM and can only be accessed by Security Office staff.

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 ☒** ***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>?**

  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 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.

  Comprehensive records are retained and disposed of in accordance with General Records Schedule 5.6 items: 180,181under Disposition Authority DAA-GRS-2017-0006-0025, approved by the National Archives and Records Administration (NARA). Records regarding individuals with security clearances and other clearances for access to

Government facilities or to sensitive data, created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program will be destroyed 5 years after the employee or contractor relationship ends, however longer retention is authorized if required for business use.

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?**
  PerSec IQ, as implemented at EXIM, stores a broad range of personnel-security-related PII and associated case records to support suitability, fitness, and clearance decisions. The list above focuses on the identifiable data elements described in the EXIM PERSEC IQ System of Records Notice (SORN) and related documentation

- **Is this system operated under a System of Records Notice (SORN) either specific to this system, or part of another SORN? Yes ☒ No ☐**
  90 FR 13359

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