Privacy Impact Statement

Office of the Inspector General (OIG)
Export-Import Bank of the United States

A. General System/Application Information

System Owner:

Inspector General
Office of Inspector General
Export-Import Bank of the United States
811 Vermont Avenue, NW
Washington, DC 20571
202-565-3908

Project Manager:

Assistant Inspector General for Investigations
Office of Inspector General
Export-Import Bank of the United States
811 Vermont Avenue, NW
Washington, DC 20571
202-565-3908

System Name (Acronym)

Ex-Im Bank Office of Inspector General Information System (IGIS)

Description

The Ex-Im Bank Office of Inspector General Information System (IGIS) is a law enforcement sensitive but unclassified database that allows the Office of the Inspector General (OIG) for the Export-Import Bank of the United States (Ex-Im) to receive, process, and manage allegations of violations of criminal, civil, or administrative laws and regulations relating to Ex-Im employees, contractors, and other individuals and entities associated with the Bank. IGIS also allows the OIG to manage information generated during the course of audits, inspections, and evaluations of Ex-Im program and operations.

Purpose of System

IGIS is established under the Inspector General Act of 1978, as amended, to maintain information and document OIG work related to investigations of criminal, civil, or administrative matters.

System of Records Notice (SORN) Number – EIB-35 Office of the Inspector General Investigative Records

Privacy Impact Statement

Office of the Inspector General (OIG)
Export-Import Bank of the United States

Authorities

5 U.S.C. App. 3 (Inspector General Act of 1978, as amended)

Section I - Data

a. What data is collected about individuals?

IGIS includes personally identifiable information concerning complainants, witnesses, Ex-Im Bank employees, contractors, and other persons involved in Ex-Im Bank programs and operations who may be under investigation related to wrongdoing related to Ex-Im Bank's programs and operations. Data elements include:

Personal Information
Name, including known aliases Information about spouses or partners can also be collected
Address (Street, City, State, Zip, Country)
Telephone (Office, Cell, Fax, Other)
Email
Date of Birth
Social Security Number (SSN)
Driver's License Number
Passport Number and Issuing Country
Resident Alien Card Number
Border Crossing Card Number
Personal Characteristics (Height, Weight, Hair Color, Eye Color)
Passport Number and Issuing Country

b. Data Sources

Data is collected from various sources including, but not limited to, divisions of Ex-Im Bank, other federal agencies, suspects, co-conspirators, witnesses, informants, and other investigative sources.

c. Why is data being collected?

The records and information collected and maintained in this system are for the purpose of conducting investigations of Ex-Im Bank's programs and operations under the Inspector General Act of 1978, as amended. In particular, the data is collected and maintained for the purpose of receiving and processing allegations of violations of law, rules, or regulations relating to Ex-Im Bank programs and operations, managing investigations and information provided during the course of investigations, issuing investigative and statistical reports, referring cases for criminal, civil, or administrative prosecution, and managing and tracking any actions related to the investigation program.

d. What technologies are used to collect data?

Data is collected from paper based systems (files, subpoena documents, etc.) and from law enforcement databases. Data is entered into IGIS manually. IGIS does not communicate electronically with other data collection systems within Ex-Im Bank or other federal agencies.

e. Does a personal identifier retrieve the data?

Yes, data can be retrieved by a variety of personal identifiers (name, SSN, etc.). Data can also be retrieved by case number, agent assigned, etc.

Section II – Use of the Data

How is data being used?

The data is used to conduct investigations relating to Ex-Im Bank programs and operations. In addition, data is used to perform a variety of tasks, which have been identified in the Notice of System of Records of "EIB-35- Office of Inspector General Investigative Records." Below is an excerpt from this Notice on the routine uses and sharing of records maintained in the system:

(A) To an appropriate Federal, State, territorial, tribal, local, or foreign law enforcement agency, licensing entity, or other appropriate authority charged with investigating, enforcing, prosecuting, or implementing a law (criminal, civil, administrative, or regulatory), where Ex-Im Bank OIG becomes aware of an

indication of a violation or potential violation of such law or where required in response to compulsory legal process.

(B) To Federal intelligence community agencies and other Federal agencies to further the mission of those agencies relating to persons who may pose a risk to homeland security.

(C) To international governmental authorities in accordance with law and formal or informal international agreement;

(D) To any individual or entity when necessary to elicit information that will assist an OIG investigation, inspection, or audit.

(E) To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil or criminal discovery or proceedings, litigation, and settlement negotiations.

(F) To Federal, State, local, or foreign government entities or professional licensing authorities responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, or where Ex-Im Bank OIG becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation, or where Ex-Im Bank OIG has received a request for information that is relevant or necessary to the requesting entity's hiring or retention of an employee, or the issuance of a security clearance, license, contract, grant, or other benefit.

(G) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

(H) To the United States Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) Ex-Im Bank; (b) any employee of Ex-Im Bank in his/her official capacity; (c) any employee of Ex-Im Bank in his/her individual capacity where the Department of Justice or Ex-Im Bank has agreed to represent the employee; or, (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation.

(I) To third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation.

(J) To a Member of Congress, or staff acting upon the Member's behalf, when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(K) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(L) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the

context of a particular case would constitute an unwarranted invasion of personal privacy.

(M) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(N) To appropriate agencies, entities, and persons when (1) the OIG suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the OIG has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the OIG or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the OIG's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(O) To the National Archives and Records Administration or other Federal Government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

(P) To appropriate persons engaged in conducting and reviewing internal and external peer reviews of the Ex-Im Bank OIG to ensure adequate internal safeguards and management procedures exist or to ensure that auditing standards applicable to Government audits are applied and followed.

(Q) To the Council of Inspectors General on Integrity and Efficiency ("CIGIE") and other Offices of Inspectors General, as necessary, if the records respond to an audit, investigation, or review which is conducted pursuant to an authorizing law, rule or regulation, and in particular those conducted at the request of the CIGIE pursuant to5 U.S.C. App. 3, § 11.

(R) In an appropriate proceeding before a court, grand jury, or an administrative or adjudicative body, when the OIG determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(S) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an individual; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance or revocation of a grant or other benefit.

(T) To federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(U) To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

Section III – Sharing Practices

Data will be shared as described in Section II –Use of Data.

Section IV – Notice to Individual to Decline/Consent Use

As this information is collected as part of an investigation, allegation, or complaint, individuals have neither the opportunity nor a right to decline to provide information. Exceptions to this general rule include information collected directly from individuals afforded rights under the Fifth Amendment and from individuals who may lawfully assert a privilege (e.g., attorney-client or spousal privilege). Individuals from whom the OIG requests information for this system may decline to provide information.

Individuals have no opportunity to consent to particular uses of the information provided by the individual or about that individual or affiliated business.

Section V - Access to Data

STORAGE: The records in this system are maintained in a variety of media, including paper, digital media (hard drives and magnetic tapes or discs), and an automated database. The records are maintained in limited access areas during duty hours and in locked offices at all other times.

RETRIEVABILITY: Paper media are retrieved numerically by investigation number. Electronic media are retrieved numerically by investigation number, by the name or identifying number for a complainant, subject, victim, or witness; by case number; by special agent, or other personal identifier.

PERSONNEL ACCESS: All paper and electronic records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. Ex-im Bank facilities are protected from the outside by security personnel. Direct access to investigative records is restricted to authorized staff members of the OIG. Paper records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Manual records are in locked cabinets or in safes and can be accessed by key or combination formula only. Electronic records are protected by computer-logon identifications and password protection.

RETENTION AND DISPOSAL: OIG is in the process of developing a records retention schedule in conjunction with the National Archives and Records Administration (NARA). Closed files relating to a specific investigation are destroyed after ten years. Closed files containing information of an investigative

nature but not relating to a specific investigation are destroyed after five years. Records existing on computer storage media are destroyed according to applicable OIG media sanitization practice.

SYSTEM MANAGER(S) AND ADDRESSES: The System Manager is the Ex-Im Bank OIG Inspector General, 811 Vermont Avenue, NW, Rm. 976, Washington, DC 20571.

NOTIFICATION PROCEDURES: Pursuant to a concurrent notice of proposed rulemaking by Ex-Im Bank, this system of records will be generally exempt from the notice, access, and contest requirements of the Privacy Act. However, the Ex-Im Bank OIG will entertain written requests to the systems manager on a case-by-case basis for notification regarding whether this system of records contains information about an individual. Individuals seeking notification of any record contained in this system of records may submit a request in writing to the System Manager identified above. Individuals requesting notification must comply with the Ex-Im Bank Privacy Act regulations (12 CFR § 404.4).

RECORD ACCESS PROCEDURES: Same as "Notification Procedures'" above.

Section VI – How Will the Information Be Secured

IGIS is secured with management, operational, and technical controls. The system is maintained on servers that are segregated from other computer equipment maintained by Ex-Im and access is limited to approved OIG employees and contractors. OIG employees and contractors must log-on to a computer to access IGIS. No components outside of the OIG have direct access to the system. Access to the building where the system is housed is protected by physical building security including security guards and access badges. If case information is provided to outside agencies or other entities in the course of routine access, that information is in hard-copy form and distribution is limited to a need-to-know basis. In case information is provided to outside agencies or entities in electronic form, such information is encrypted. Recipients are sworn law enforcement agents or federal attorneys working on or prosecuting the case. These recipients have accepted rules of behavior for the proper handling of PII.

In summary, the potential risk for unauthorized disclosure of personal information is mitigated by:

- limiting the number of authorized users to OIG employees and contractors (on a need-to-know basis)
- building security procedures
- segregation of OIG servers from Ex-Im Bank servers
- providing hard copy case information to sworn law enforcement agents or federal attorneys on a need-to-know basis only or electronic information in encrypted form.

Section VI- System of Records

IGIS operates under the Privacy Act System of Records Notice entitled "EIB-35- Office of Inspector General Investigative Records." Please refer to __FR___ for more information.

Privacy Impact Statement

Office of the Inspector General (OIG)
Export-Import Bank of the United States

SIGNATURE OF INDIVIDUAL(S) COMPLETING THIS FORM

System Owner/Date Osvaldo L. Gratacós Inspector General	7-2-12
Project Manager/Date Lawrence K. Valett Assistant Inspector General for Investigations	7-2-12

ENDORSEMENT

Senior Agency Official for Privacy/Date Fernanda Young Chief Information Officer	
Chief Information Security Officer/Date John Lowry Director, IT Security and Systems Assurance	

APPROVAL

Chief Informational Officer/Date Fernanda Young	