

SBA Investigations Management Information System PIA

SMALL BUSINESS ADMINISTRATION PRIVACY IMPACT ASSESSMENT

Name of Project: Investigations Management Information System (IMIS)

Program Office: Office of Inspector General

Project's Unique ID:

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Rose Madden
IMIS System Manager
Office of Inspector General for Investigations, (202) 205-6393

2) Who is the System Owner?

Daniel J. O'Rourke
Assistant Inspector General for Investigations
Office of Inspector General, (202) 205-6648

3) Who is the System Manager for this system or application?

Rose Madden
Investigative Analyst
Office of Inspector General for Investigations, (202) 205-6393

4) Who is the IT Security Manager who reviewed this document?

David McCauley
Chief Information Security Officer
(202) 205-7173

5) Who is the Bureau/Office Privacy Act Officer who reviewed this document?

Ethel Matthews

6) Who is the Reviewing Official?

Christine Liu

B. PIA PROCESS APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes

a. Is this information identifiable to the individual?

Yes. The information is identifiable to the individual.

b. Is the information about individual members of the public?

Yes. Individual members of the public may have information contained within the system.

c. Is the information about employees?

Yes. Depending upon the details of the case, employee information may be contained within the system.

2) What is the purpose of the system/application?

The IMIS application is the official case management system for the Office of Inspector General (OIG) Investigative Division (ID). The system is designed to allow investigators to initiate, maintain, manage, and close their investigations and allegations. The system also supports uploading of electronic copies of case documents. This feature allows real-time supervisory approval of documents from remote locations. The system is essential for the day-to-day operations of the OIG ID.

3) What legal authority authorizes the purchase or development of this PIA Process?

The legal authority for the development of IMIS, the electronic case management system for the storage; retention; and retrieval of investigative information, is authorized as follows:

- The Inspector General Act of 1978, as amended, 5 U.S.C. Appendix 3 (IG Act) authorizes SBA's Inspector General to provide policy direction for, and to conduct, supervise, and coordinate such audits, investigations, and inspections relating to the programs and operations of SBA, as appears necessary or desirable.
- 44 U.S.C. Chapter 31 authorizes the head of each Federal agency to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights

of the Government and of persons directly affected by the agency's activities.

- The President's Council on Integrity and Efficiency (PCIE) publication, Quality Standards for Investigations (QSI), requires that investigative data be stored in a manner allowing effective retrieval, referencing, and analysis.
- The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems" implements a number of Federal laws relating to information resources management (for example, the Paperwork Reduction Act, and the Clinger-Cohen Act).
- The Federal Information Security Management Act of 2002 (FISMA) prescribes security measures for non-major IT systems such as IMIS.

C. DATA in the PROCESS:

1) Generally describe the type of information to be used in the system and what categories of individuals are covered in the System?

Information gathered or created during preparation for, conduct of, and follow-up on investigations conducted by SBA OIG or other Federal, state, local, or foreign regulatory or law enforcement agencies. The type of information would be determined by the allegations being investigated. This information may include, but is not limited to:

- Information on individuals applying for SBA loans or otherwise involved in SBA lending decisions (e.g. name, social security number, date of birth, home address, employment, assets, income, expenses, taxes, credit history, property, disaster damage, etc.).
- Business information including employer ID numbers and business loan guarantees.
- Information about allegations, decisions, investigative assignments, and special techniques.
- Reports and results of investigations.
- Contracting information.
- Operational memoranda--management and operational decisions on ongoing SBA operations.
- Financial information on SBA borrowers and lenders.
- SBA employee information including evaluations, personal email, payroll information, personally identifiable information.
- HUBZone and 8a minority information on business size.
- Time spent by investigators on individual cases.

2) What are the sources of the information in the System?

- a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual source, then what other source?**

Information may be obtained directly from the individual source (SBA employees, SBA borrowers, and other individuals with pertinent information relating to the case). Information may also be obtained from third-party witness interviews, subpoenas, other law enforcement agencies, or SBA documentary evidence. Information can also be downloaded from SBA's IT systems in forms or formats, as desired.

- b. What Federal agencies are providing data for use in the process?**

SBA OIG may obtain data from other Inspector Generals or other Federal agencies on an infrequent basis. However there are no specific ongoing data sharing agreements.

- c. What State and local agencies are providing data for use in the process?**

State or local agencies may share data with SBA OIG from time to time. However, there are no specific ongoing data sharing agreements.

- d. From what other third party sources will data be collected?**

Data may be collected from any individual or business for which SBA OIG may have a need to obtain data to accomplish its mission of investigating fraud, waste, and abuse.

- e. What information will be collected from the employee and the public?**

The type of information collected from employees and the public is determined by the allegations being investigated. This information may include, but is not limited to:

- Information on individuals applying for SBA loans or otherwise involved in SBA lending decisions (e.g. name, social security number, date of birth, home address, employment, assets, income, expenses, taxes, credit history, property, disaster damage, etc.).
- Business information including employer ID numbers and business loan guarantees.
- Information about allegations, decisions, investigative assignments, and special techniques.
- Reports and results of investigations.

- Contracting information.
- Operational memoranda--management and operational decisions on ongoing SBA operations.
- Financial information on SBA borrowers and lenders.
- SBA employee information, including personally identifiable information; evaluations; personal email; payroll information, etc.
- HUBZone and 8a minority information on business size.
- Time spent by investigators on individual cases.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than SBA records be verified for accuracy?

- Data from Federal agency records is identified by name, address, and/or SSN and is subject to Privacy Act regulation and documented practices for accuracy.
- Data from commercial entities is identified by name, address, and SSN or EIN and is also subject to regulation.
- Data is compared between source documents and ancillary information in SBA's major IT systems.
- Supervisors perform case reviews every 90-days. These reviews include a quality assurance check of the IMIS case file for accuracy.
- The Investigation Division complies with the PCIE QSI, which requires that investigations be conducted in a timely, efficient, thorough, and legal manner. This compliance is verified through periodic peer reviews (similar to audits, but conducted by another OIG's Investigations Division). This safeguard also applies to questions b., c., and d, below.

b. How will data be checked for completeness?

- Supervisors perform case reviews every 90-days. These reviews include a quality assurance check of the IMIS case file for completeness.
- Headquarters staff access IMIS on a daily basis and notify supervisors if additional information is needed.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Agents are required by SBA OIG Chapter 340, Report Writing for Investigations, to upload their reports to IMIS within required timeframes.

- d. **Are the data elements described in detail and documented? If Yes, what is the name of the document?**

Yes, the data elements are documented and described in detail in the IMIS User Manual and SBA OIG Chapter 344, Case Management and Investigative Files.

D. ATTRIBUTES OF THE DATA

- 1) **Is the use of the data both relevant and necessary to the purpose for which the process is being designed?**

Yes. The information is based upon the allegations and findings of each investigation performed by the SBA OIG ID.

- 2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

No. The system will not derive new data or create previously unavailable data from information collected.

- 3) **Will the new data be placed in the individual's record?**

N/A

- 4) **Can the system make determinations about employees/public that would not be possible without the new data?**

N/A

- 5) **How will the new data be verified for relevance and accuracy?**

N/A

- 6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

IMIS does contain legacy data that was previously housed in an Access database. IMIS access is controlled by entering a GLS user name and password and by user permissions granted by the IMIS Security Manager.

- 7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access through the process? Explain.**

No processes are being consolidated.

- 8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Data on individuals can be retrieved by personal identifiers (first, middle, and last name and social security number) or by case identifiers (case number, case name, agent's name, etc.).

- 9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

IMIS does not routinely generate reports specific to individuals, their loans, grants, personnel or payroll data. SBA OIG may produce specific reports to comply with FOIA and Privacy Act requirements. Access to OIG investigative information is restricted to investigative staff with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines. Reports are produced to present the investigative statistics for the Semiannual Report to Congress, the PCIE Annual Report, and Agency internal reports

- 10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?**

Investigations are based on allegations of specific wrong doing by SBA borrowers, grantors, program participants or Agency employees. Providing information is required as noted below.

The IG Act and 13 C.F.R. Section 101.302 identify the scope of Inspector General's authority. To obtain the necessary information and evidence, the Inspector General (or designee) has the right to:

- (a) Have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to SBA and relating to SBA's programs and operations;
- (b) Require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence;
- (c) Administer oaths and affirmations or take affidavits; and
- (d) Request information or assistance from any Federal, state, or local government agency or unit.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

- 1) If the information in the process is operated in more than one site, how will consistent use of the data be maintained in all sites?**

The IMIS User Manual and the Case Management and Investigative Files chapter explain in detail the policies and procedures for consistent use of the data.

- 2) What are the retention periods of data in the system?**

Hard-copy investigative files are retained for 20 years after the end of the fiscal year in which the case was closed. A records retention schedule for the electronic investigative records in IMIS has not yet been determined.

- 3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

N/A

- 4) Are the systems in the process using technologies in ways that the SBA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No

- 5) How does the use of this technology affect public/employee privacy?**

N/A

- 6) Will this system in the processes provided have the capability to identify, locate, and monitor individuals? If yes, explain.**

N/A

- 7) What kinds of information are collected as a function of the monitoring of individuals?**

N/A

- 8) What controls will be used to prevent unauthorized monitoring?**

N/A

- 9) **Under which Privacy Act Systems of Records Notice does the system operate? Provide number and name.**

The system operates under Investigations Division Management Information System--SBA 17.

- 10) **If the system is being modified, will the Privacy Act Systems of Records notice require amendment or revision? Explain.**

No

F. ACCESS TO DATA:

- 1) **Who will have access to the data in the System? (e.g., system users, contractors, managers, system administrators, developers, tribes, other)**

Access to and use of this data is limited to those SBA OIG staff members with a "need to know" and staff assigned to the Office of the Chief Information Officer whose official duties require such access.

- 2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

The AIGI is the approval authority for IMIS access. Once the AIGI has granted verbal approval, the user requests a GLS Logon ID and then through GLS requests IMIS Access. Access to IMIS is controlled by both IT Security and the ID Program Office. The IMIS Program Manager enters the user into the Staff table of IMIS and assigns a user role and case supervisor. Currently, a document entitled, "IMIS User Account Creation, Management and Maintenance" is being written.

- 3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Users will be able to view all case data on the system except grand jury information. Only those users who are on the grand jury list for a particular case are able to view the grand jury information for that case. In addition, users are assigned roles which determine their system capabilities.

- Special Agents and ID administrative staff are given the "Create" role. They can create cases and enter information into cases that they have created.
- Special Agents in Charge and Senior Special Agents are given the "Admin" role. This role allows them to create cases, run supervisory reports, and approve documents for those cases for which they are set up as the supervisor.

- The System Manager is given the “Superuser” role. This role allows that person to update staff access and roles, change case supervisors, and change case data in fields not accessible to other users.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

SBA OIG personnel sign a “Rules of Behavior” statement for accessing government owned computers. Additionally, SBA Standard Operating Procedure on Computer Security SOP 90-47.2 prohibits unauthorized browsing of data by those who have access.

5) Are contractors involved with the design and development of the system? Are they also involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes, contractors were involved with the original design and development of the system and continue to be involved with enhancements to the system. Contractors are also routinely involved with maintenance of the system. Privacy Act contract clauses were inserted in all their contracts as is standard SBA practice.

6) Do other systems share data or have access to the data in the system? If yes, explain.

No other system has access to the data or system.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

There is no interface with other systems.

8) Will other agencies share data or have access to the data in this system?

No other agency shares data or has access to the system.

9) How will the data be used by the other agency?

N/A

10) Who is responsible for assuring proper use of the data?

N/A

SBA OIG IMIS PIA

The following officials have approved this document:

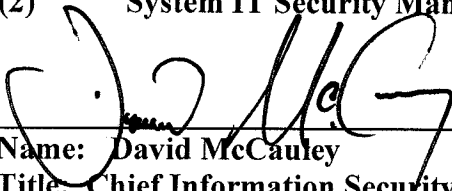
(1) System Owner



Name: Daniel J. O'Rourke

Title: Assistant Inspector General for Investigations

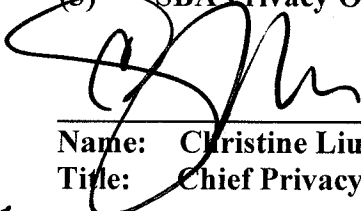
(2) System IT Security Manager



Name: David McCauley

Title: Chief Information Security Officer

(3) SBA Privacy Official



8/16/07

Name: Christine Liu

Title: Chief Privacy Officer

