SMALL BUSINESS ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

Name of Project: Auditing Informational Management System

Project's Unique ID: AIMS

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- SBA IT Security Manager
- SBA OCIO IT Portfolio Division
- SBA Privacy Act Officer

A. **CONTACT INFORMATION**:

   1) **Who is the person completing this document?**

   Audrey Delaney
   System Administrator
   409 3rd Street S.W.
   Washington, DC 20416
   (202) 205-7647
   audrey.delaney@sba.gov

   2) **Who is the System Owner?**

   Debra Ritt, Assistant Inspector General for Auditing, Office of Inspector General

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

   Audrey Delaney, OIG

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

   David McCauley

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

   Ethel Matthews

   6) **Who is the Reviewing Official?** (According to OMB, this the agency IO or other agency head designee who is other than the official

procuring the system or the official who conducts the PIA).

Christine Liu

B. PIA PROCESS APPLICATION GENERAL INFORMATION:

1. **Does this system contain any information about individuals?**

    a. Is this information identifiable to the individual?

    Yes

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

    No

    c. Is the information about employees?

    Yes

2. **What is the purpose of the PIA Process?**

    AMIS tracks OIG audit project origination and progress, auditor time and audit outcomes.

3. **What: legal authority authorizes the purchase or development of this PIA Process?**

    The Inspector General Act

C. Data in the PROCESS:

1. **What categories of individuals are covered in the PIA Process?**

    Employees (Auditors)

2. **What are the sources of the information in the PIA Process?**

    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?

    Human Resource Records- From Individual

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

    None

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

None

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

Auditees & SBA Program Offices

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

The name and last four digits of SSN will be collected from the employee.

3. Accuracy, Timeliness, and Reliability

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

None collected

b. How will data be checked for completeness?

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)

PIA data is current unless an employee changes their name. In the case of a name change the employee submits the new name and it is changed in AMIS. The SSN derived identifier does not change.

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

Personal Word Document on Specifics
Access Data Base

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, it is needed to identify auditor time spent on projects

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

3. Will the new data be placed in the individual's record?

No

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

No

5. How will the new data be verified for relevance and accuracy?

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

Data is not consolidated.

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.

Processes are not 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 is retrieved by queries and displayed in reports. The only identifier used is the employee ID (first letter of last name plus last four digits of SSN).

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

- Employee working on specific projects
- Timekeeping
- Repots are used by audit management to track audit progress.

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 individuals can grant consent?

None

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1. If the information in the process operated in more that one site, how will consistent use of the date be maintained in all sites?

Only operated at OIG HQ.

2. What are the retention periods of data in the system?

Forever

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?

Forever

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?

6. Will this system in the process provided the capability to identify, locates, and monitor individuals? If yes, explain

Monitor Time (15 min) each employee
Charges to each project

7. What kinds of information are collected as a function of the monitoring of individuals?

Time charged to individual project codes.

8. What controls will be used to prevent unauthorized monitoring?

Restricted access

9. Under which Privacy Act systems of records notice does the system operate? Provide number and name

None

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. contractors, users, managers, system administrators, developers, tribes, other)

3 users
1 owner

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

Written request
Permission by owner

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

Yes. Users have access to all data

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

Users are public trust employees

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

No

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

No

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

Audrey Delaney
Debra Ritt

8. Will other agencies share data or have access to the data in this:

The Following Officials Have Approved this Document

1) System Owner

Signature: _Debra Ritt_   Date: _8/1/07_

Name: Debra Ritt
Title: Assistant Inspector General for Auditing

2) System Program/Project Manager

Signature: _Audrey Delaney_   Date: _8/1/07_

Name: Audrey Delaney
Title: System Administrator

3) System IT Security Manager

Signature: _David McCauley_   Date: _8/3/07_

Name: David McCauley
Title: Chief Information Security Officer

4) System Privacy Official

Signature: _Christine Liu_   Date: _8/3/07_

Name: Christine Liu
Title: Chief Privacy Officer