Name of Project: Auditing Management Information System (AMIS)
Program Office: Office of Inspector General, Auditing Division

A. CONTACT INFORMATION:

1. **Who is the person completing this document?** (Name, title, office and contact information).

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

2. **Who is the system owner?** (Name, title, office and contact information).

   Debra Ritt
   Assistant Inspector General for Auditing
   Office of Inspector General
   409 3rd Street S.W.
   Washington, DC 20416
   (202) 205-7390
   Debra.ritt@sba.gov

3. **Who is the system manager for this system or application?** (Name, title, office, and contact information).

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

   Richard Benton
   4300 Amon Carter Blvd
   Suite 116
   Fort Worth, TX
   76155
   (817) 684-5340
   Richard.benton@sba.gov

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

David McCauley
Chief Information Security Officer
409 3rd Street, SW
Washington, DC 20416
(202) 205-7103
David.McCauley@sba.gov

6. Did the Agency's Senior Office for Privacy review this document? (

Ethel Matthews
Chief Information Security Officer
409 3rd Street, SW
Washington, DC 20416
(202) 205-7173
Ethel.Matthews@sba.gov

7. Who is the Reviewing Official? (According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).

Christine Liu
Chief Information Officer
409 3rd Street, SW
Washington, DC 20416
(202) 205-6708
Christine.Liu@sba.gov

B. SYSTEM 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 system/application?**

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

3. **What legal authority authorizes the purchase or development of this system/application?**

The Inspector General Act

C. DATA IN THE SYSTEM

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

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

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, then what other source?

Human Resource Records- From Individual

(b) What Federal agencies are providing data for use in the system?

None

(c) What State and local agencies are providing data for use in the system?

None

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

None

(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 from sources other than SBA records be verified for accuracy?

None collected

(b) How will data be checked for completeness?

Employees may check the information for accuracy

(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?

A word document developed by the system administrator explains the data elements.
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 system 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?**

   N/A

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?** 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 (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
   Reports 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 system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

   Only operated at OIG HQ.

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

   Indefinite

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?**

   Indefinite

4. **Is the system 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 provide 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?**

   By limiting access to people who are authorized and understand the data's intended use. Access requested in writing and approved by the system's owner.

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 system 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)

   System Administrators and managers. No others have access to the system.

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

   Written request
   Permission is granted by the system owner on an as needed basis.

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 and is able to edit the data.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

   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, are 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?**

   Richard Benton
   Audrey Delaney
   Debra Ritt

8. **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?**

   No

9. **How will the data be used by the other agency?**

   N/A

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

    Debra Ritt

G. PRIVACY IMPACT ANALYSIS

1. **Discuss what privacy risks were identified and how they were mitigated for types of information collected.**

   Potential privacy risk is that an employee's name could be matched with part of their social security number. This risk is mitigated by limiting access to the database, placing the database on an isolated server, and masking the available information (i.e. limiting the social security number to only the last four digits).

2. **Describe any types of controls that may be in place to ensure that information is used as intent.**

   We ensure that the information is used as intended by limiting access to authorized officials. These select officials understand the information and its intended use. Additionally, all users have taken Computer Awareness Training and are aware of the consequences of abusing government equipment and information.

3. **Discuss what privacy risks were identified and how they were mitigated for information shared internal and external?**

   We have identified that an unauthorized official could review reports that contain an employees name and partial social security number. To mitigate this risk we do not share this information externally, it is only used for management to perform their required duties and for employees to review the information for accuracy. Employees receive data reports explaining the information contained in the database (i.e. timesheets) and are permitted to make changes in writing through their manager. Employees do not directly interface with the system.

4. **What privacy risks were identified and describe how they were mitigated for security and access controls?**

   An unauthorized official could access the server where the information is stored. We mitigated that risk by keeping the server in a locked and controlled environment. Another identified risk is an unauthorized user gaining logical access to the data. The access path to the data has been controlled by implementing logical controls limiting access to less than five persons.

Privacy Assessment for AIMS

Responsible Officials - Approval Signature Page

The Following Officials Have Approved This Document

1) System Owner

Debra Ritt (Signature) 12/3/08 (Date)

Name: Debra Ritt
Title: Assistant Inspector General for Auditing

2) System Program/Project Manager

(Signature) 12/3/08 (Date)

Name: Audrey Delaney
Title: System Administrator

3) System Program/Project Manager

Richard C. Benton (Signature) 12-2-08 (Date)

Name: Richard Benton
Title: System Administrator

4) System IT Security Manager

(Signature) 12/17/08 (Date)

Name: David McCauley
Title: Chief Information Security Officer

5) Privacy Official

Christine H. Liu (Signature) 1/2/09 (Date)

Name: Christine H. Liu
Title: Chief Information Officer and Chief Privacy Officer