SBA TeamMate PIA

SMALL BUSINESS ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

Name of Project: TeamMate Automated Audit Documentation System
Program Office: Office of Inspector General
Project's Unique ID:

A. CONTACT INFORMATION:

1. Who is the person completing this document?

Richard Harai
TeamMate System Manager
Office of Inspector General for Auditing, 202-205-7414.

2. Who is the System Owner?

Debra S. Ritt
Assistant Inspector General for Audit
Office of Inspector General, 202-205-7390

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

Richard K. Harai
Senior IT Auditor,
SBA Office of Inspector General 202-205-7414

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

Richard K. Harai
TeamMate System Security Officer,
SBA Office of Inspector General, 202-205-7414

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. Members of the public can have their information within the system.

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

Yes. Depending upon the objectives of the audit, individual members of the public can have information contained within the system.

c. Is the information about employees?

Yes. Depending upon the objectives of the audit, employee information may be contained within the system.

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

The TeamMate Application supports the Office of Inspector General (OIG) Auditing Division. The OIG uses the application to manage, support and store information for all audit projects and related work papers and audit reports. The system is essential for the day-to-day activities of the OIG Auditing Division. The TeamMate Application supports the OIG Auditing Division. The application stores and maintains electronic audit working papers.

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

13 CFR 101.300 grants the Inspector General's authority to conduct audits, investigations, and inspections. The Inspector General Act of 1978, as amended (5 U.S.C. App. 3) 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.

13 CFR Sec. 101.301 grants that the Office of Inspector General should receive all information or allegations of waste, fraud, or abuse regarding SBA programs and operations.

13 CFR Section 101.302 identifies the scope of the Inspector Generals authority. To obtain the necessary information and evidence, the Inspector General (and designees) have 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.

The Government Accountability Office (GAO) prescribes Government Auditing Standards (GAS) GAO-03-673G which all SBA OIG audits must comply with. To maintain adequate documentation within the scope of the Inspector Generals authority and GAS, TeamMate has been procured as an automated workpaper documentation package for the storage and retention of audit evidence.

The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems." OMB Circular A-130 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 TeamMate.

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 on all aspects of SBA operations. Such information would be determined based upon the objectives of the SBA audit or review. This information may include, but is not limited to:

- Lending and loan guarantees for individuals which includes social security numbers, home addresses, employment, assets, income, expenses, taxes, credit history, property, and disaster damage is collected and used in the system in making loan and lending decisions.
- Business information including employer ID numbers, trade secrets, operational practices for obtaining business direct loans (during emergencies) and business loan guarantees.

- Contracting and grant information also including trade secrets.
- Operational memoranda, management and operational decisions on ongoing SBA operations.
- Financial information on SBA vendors and creditors for paying bills and receiving remittances.
- SBA employee information including evaluations, personal email, payroll information, personally identifiable information.
- 8a minority and HUBZone information on business size and trade secrets.
- And, documentation of SBA's current information technology (IT) status including weaknesses and strengths within SBA's IT systems.

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

b. 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 can be obtained from individuals including SBA employees and SBA borrowers or through interview or inspection of SBA documentary evidence. Information can also be downloaded from SBA's 19 major IT systems in forms or formats as desired.

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

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

d. **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 data sharing agreements.

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

Any individual or business for which SBA OIG may have a business need to obtain data or review data to accomplish our mission of reviewing SBA operations and activities.

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

Information on all aspects of SBA operations. Such information would be determined based upon the objectives of the SBA audit or review. This information may include, but is not limited to:

- Lending and loan guarantees for individuals which includes social security numbers, home addresses, employment, assets, income, expenses, taxes, credit history, property, and disaster damage is collected and used in the system in making loan and lending decisions.
- Business information including employer ID numbers, trade secrets, operational practices for obtaining business direct loans (during emergencies) and business loan guarantees.
- Contracting and grant information also including trade secrets.
- Operational memoranda, management and operational decisions on ongoing SBA operations.
- Financial information on SBA vendors and creditors for paying bills and receiving remittances.
- SBA employee information including evaluations, personal email, payroll information, personally identifiable information.
- 8a minority and HUBZone information on business size and trade secrets.
- And, documentation of SBA's current information technology (IT) status including weaknesses and strengths within SBA's IT systems.

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 subject to regulation and identified by name, address and SSN or EIN. Data is compared between source documents and ancillary information in SBA's 19 major systems.

b. How will data be checked for completeness?

Audit evidence is analyzed, compared and reconciled with any third party data received. Government Auditing Standards require that audit evidence adequately reviewed by supervisory personnel as part of an audit or review.

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).**

Government Auditing Standards (GAO-03-673G) require that audit evidence is timely and reflects current Agency operations so that audit reports and memoranda are timely reported to Agency decision makers.

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

Data elements are not described in detail or documented. Due to the nature of the different types of audits, it is not possible to foresee all the different types of data elements which maybe encountered.

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 objectives of each audit or review performed by the SBA OIG Auditing Division.

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?**

Yes. Certain information may be derived from audits or reviews of individuals as necessary through the scope or objectives of the audit or review. TeamMate data is maintained and filed in a historical record of SBA OIG audits and reviews performed. SBA OIG is mandated to hold and maintain its audits and reviews as prescribed by the National Archives and Records Administration (NARA) under 44 U.S.C. 2904, 3101, 3102, 3105, and 3303.

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

Depending upon to scope and objectives of the review or audit, audit information may be the basis for personnel determinations and those determinations placed in employees Official Personnel File.

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

Yes. Audit analyzes and conclusions can for the basis of new conclusions about employees and the public relating to SBA operations.

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

Analyses and conclusions based upon new data is subject to supervisory review, peer review and referencing review by SBA OIG internal control mechanisms.

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

TeamMate may consolidate data previously housed in different agency systems as the result of analyses and conclusions about SBA operations.

TeamMate's primary files are accessed through the SBA's LAN and OIG users are subject to SBA's LAN access controls. Moreover, TeamMate utilizes Windows Active Directory to ensure that only authorized SBA OIG Audit personnel access the different projects for which they are assigned. All SBA OIG audits within TeamMate are set to accept Windows Active Director for verifying Identification and Authentication for audit team members who may be assigned to the different audits and reviews.

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. Not applicable.

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 SBA OIG auditors through access permissions to other major agency systems. OIG auditors have sufficient privileges by ID and password to access those systems. If the information is relevant to OIG audit objectives, the resulting information will be placed in TeamMate to document agency actions and operations.

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

TeamMate does not generate reports specific to individuals, their loans, grants, personnel or payroll data. Reports are produced to present the results of analyses or review of SBA operations. SBA OIG may produce specific reports and inquiries to comply with FOIA and Privacy Act requirements. Access to OIG audits or are restricted to auditors with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines.

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?**

Audits or reviews of SBA Agency operations generally have objectives of preventing waste, fraud and abuse as well as making recommendations to improve economy and efficiency of Agency operations. Audits and reviews do not include allegations of specific wrong doing by SBA borrowers, grantors, program participants or Agency employees.

13 CFR Section 101.302 identifies the scope of the Inspector Generals authority. To obtain the necessary information and evidence, the Inspector General (and designees) have 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?

SBA OIG Audit Staff Memorandum No. 04 00 03 "Audit Policy and Guidance for Using TeamMate Electronic Audit Documentation Files" mandate consistent use of TeamMate for all SBA OIG audit offices including Washington DC, Atlanta GA, Fort Worth TX, Glendale CA and Chicago IL.

The system is installed on each auditor's desktop and laptop computer. Audit master files are maintained on SBA agency file servers across the nation. Data is backed up to separate desktops and servers on a periodic basis.

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

Data retention will be consistent with SOP 00 41 2 which is currently being developed. All SBA audits and reviews performed using TeamMate are stored indefinitely to preserve audit evidence.
TeamMate data is maintained and filed in a historical record of SBA OIG audits and reviews performed. SBA OIG is mandated to hold and maintain its audits and reviews as prescribed by the National Archives and Records Administration (NARA) under 44 U.S.C. 2904, 3101, 3102, 3105, and 3303.

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?

SBA's current process for the archival of agency data along with long-term disposition of electronic records is in planning. Documentation of the archival process including procedures for disposition of data and report retention standards are partially completed, with an anticipated completion date in 2007.

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)?

SBA is actively pursuing the implementation of Homeland Security Presidential Directive 12 (HSPD). When HSPD 12 is implemented, TeamMate with its capability to set user authentication according to Windows Active Directory settings will have the capability to identify and

validate authorized users who successfully logged into SBA's network system using the SBA HSPD 12 mechanism.

Currently, TeamMate utilizes Windows Active Directory for ID's and passwords.

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.**

N/A

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

N/A.

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 is limited to SBA OIG personnel acting in their official capacity, with a need to know. No other individuals have access to TeamMate files unless at

the express permission of the Assistant Inspector General for Audit.

The TeamMate software package is owned by PriceWaterhouseCoopers (PWC) LLP. Changes to application software are by PWC. PWC has no access to SBA OIG data files.

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

Access is granted per Audit Staff Memorandum No. 04 00-03 "Audit Policy and Guidance for Using TeamMate Electronic Audit Documentation Files"

The audit project is initiated by the Audit Manager or Supervisory Auditor. Each auditor assigned to the project is given the ID from their Windows Alias. They are also given an initial password which they must change. The password is for replication of files to take off-site during tele-work. The auditor is also set so that their ID is recognized by Windows Active Directory for automatic access to the projects for which they are assigned.

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

Users have access capabilities given their roles.
Entry level auditors are given the role "preparers." They can create audit evidence, but not review and approve it.

Auditors-In-Charge and Audit Mangers are given the role "Preparer/Review" which allows them to both prepare and review audit evidence.

Audit Managers are given the role "Administrators" which allow them to reset passwords and reset audit settings as needed.

The TeamMate Champion is also given the role of Administrator incase something happens to the Audit Manager during the review.

Audit Directors are given the role "Preparer/Reviewer" to prepare and review audit evidence from their subordinates.

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

There are no software controls which prevent the misuse or unauthorized browsing of data by those who have access. All SBA personnel including 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?**

The TeamMate software package is owned by PriceWaterhouseCoopers (PWC) LLP. Changes to application software are by PWC who distribute the software changes via CD-Rom to OIG. OIG installs the updated versions of the software on audit desktop and laptop computers. PWC has no access to SBA OIG data files.

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?**

N/A

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

APPENDIX A
DECLARATION OF PRIVACY PRINCIPLES

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the Small Business Administration to the public and are the responsibility of all SBA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the SBA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of SBA data systems, processes and facilities.

All SBA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected. To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the SBA, the SBA will be guided by the following Privacy Principles:

Principle 1:	Protecting citizen, client, partner, and employee privacy and safeguarding confidential citizen, client and partner information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens, clients, employees or partners that is not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Information will be collected, to the greatest extent practicable, directly from the citizen, client, partner or employee to who it relates when necessary.
Principle 4:	Information about citizens, clients, partners or employees collected from third parties will be verified to the greatest extent practicable with the citizens, clients, partners or employees themselves before action is taken against them.
Principle 5:	Personally identifiable citizen, client, partner, or employee information will be used only for the purpose for which it was collected, unless other uses are specifically authorized by law.
Principle 6:	Personally identifiable citizen, client, partner, or employee information will be disposed of at the end of the retention period required by law or regulation.
Principle 7:	Citizen, client, partner, or employee information will be kept confidential

	and will not be discussed with, nor disclosed to, any person within or outside the SBA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing or any unauthorized access of citizen, client, partner, or employee information by any SBA OIG employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client, partner, or employee information will be such to ensure fair treatment of all individuals.
Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the SBA OIG and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

APPENDIX B

POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

The SBA OIG is fully committed to protecting the privacy rights of all citizens, clients, partners and employees. Many of these rights are stated in law. However, the SBA OIG recognizes that compliance with legal requirements alone is not enough. The SBA OIG also recognizes its social responsibility which is implicit in the ethical relationship between the SBA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, partners or employees' privacy rights is an expectation that the SBA OIG will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the SBA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The SBA will safeguard the integrity and availability of citizens, clients, partners and employees' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients, partners and employees. SBA OIG personnel will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the SBA OIG will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the SBA OIG takes very seriously its social responsibility to citizens, clients, partners and employees to limit and control information usage as well as to protect public and official access. In light of this responsibility, the SBA OIG is equally concerned with the ethical treatment of citizens, clients, partners and employees as well as their legal and administrative rights.

The following officials have approved this document:

(1) System Owner

Debra S. Ritt

Name: Debra S. Ritt
Title: Assistant Inspector General for Audit

(2) System IT Security Manager

for Rich Harai

Name: Richard K. Harai
Title: TeamMate Security Officer

(3) SBA Privacy Official

Christine H. Liu

Name: Christine Liu
Title: Chief Privacy Officer