PRIVACY IMPACT ASSESSMENT TEMPLATE

Name of System/Application: TeamMate Automated Audit Documentation System

Program Office: Office of Inspector General

Once the Privacy Impact Assessment is completed and the signature approval page is signed, please submit an electronic copy and hardcopy with original signatures of the PIA to the SBA Senior Advisor to the Chief Privacy Officer in the Information Privacy Office of the OCIO.

A. CONTACT INFORMATION

1) Who is the person completing this document?

Audrey B. Delaney
Auditor
Office of Inspector General for Auditing
801 -524-3226
Audrey.delaney@sba.gov

2) Who is the system owner?

Debra S. Ritt
Assistant Inspector General for Audit
Office of Inspector General
202-205-7390
debra.ritt@sba.gov

3) Who is the system manager for this system or application?

Audrey B. Delaney
Auditor
Office of Inspector General
801-524-3226
Audrey.delaney@sba.gov

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

Lawrence Gottlieb
Acting Chief Information Security Officer
Office of the Chief Information Officer
202-205-6032
Lawrence.Gottlieb@sba.gov

5) Who is the Senior Advisor who reviewed this document?

Ethel Matthews
Senior Advisor to the Chief Information Officer
Office of the Chief Information Officer
202-205-7173
Ethel.matthews@sba.gov

6) Who is the Reviewing Official?

Paul T. Christy
Acting Chief Information Officer
Office of the Chief Information Officer
202-205-6708
Paul.christy@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

1)*Does this system contain any information about individuals? If yes, explain.*

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

a. 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.

b. 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) Is the system in the development process?

No.

4) How will the technology investment (new or updated) affect existing privacy processes?

It will not be affected.

5) What legal authority authorizes the purchase or development of this system/application?

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 General's 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. To maintain adequate documentation within the scope of the Inspector General's 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" 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.

6) **Privacy Impact Analysis: What privacy risks were identified and describe how they were mitigated for security and access controls?**

The system has effective security controls in place in accordance with NIST special publication 800-53 and FISMA requirements. Access to the system requires user ID and password.

C. **SYSTEM DATA**

1) **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?**

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?**

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 20 major IT

systems (under the standards categorized by FIPS 199) in forms or formats as desired.

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

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

c. What Tribal, State, and local agencies are providing data for use in the system?

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

d. 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.

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

Information on all aspects of SBA operations will be collected. 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 is data collected from sources other than SBA records 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 20 major systems.

b. **How is data checked for completeness?**

Audit evidence is analyzed, compared and reconciled with any third party data received. Government Auditing Standards require that audit evidence be 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 reported to Agency decision makers in a timely fashion.

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 may be encountered.

4) **Privacy Impact Analysis:** Discuss what privacy risks were identified and how they were mitigated for the types of information collected?

The system has effective security controls in place in accordance with NIST special publication 800-53 and FISMA requirements. Access to the system requires user ID and password.

D. DATA ATTRIBUTES

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

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 the 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 or members of the public that would not be possible without the new data?**

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

5) **How is the new data verified for relevance, timeliness and accuracy?**

Analyses and conclusions based upon new data are 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 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 Directory 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? If process are not be consolidated please state, "N/A".**

No processes are being consolidated. N/A.

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 the 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 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 Generals (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.

11) Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used as intended.

Auditors are provided extensive training in auditing, the application and how to protect PII. As members of the of the IG and auditing community, we are also held to additional ethical standards that require our auditors to hold our work and ourselves to a high standards. As a result, any member in our audit division that is found to be in violation of a Government Auditing Standard and/or one of our internal guidance policies may receive disciplinary action depending on the severity of the offence. Actions may include, having their TeamMate accessed denied, limiting their TeamMate access to certain projects or servers, or temporary removal from the auditing division.

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?

SBA OIG Audit Staff Memorandum No. 04 00 03 "Audit Policy and Guidance for Using TeamMate Electronic Audit Documentation Files" mandates 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 this system?

Data retention will be consistent with SOP 00 41 2 which are 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 the planning stage. Documentation of the archival process including procedures for disposition of data and report retention standards are partially completed.

4) **Is the system 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 IDs and passwords.

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.**

No.

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?**

TeamMate can be accessed only when the user has authorized access to a computer (i.e. Windows authentication), and rights to the TeamMate files. TeamMate files are also individually password protected as passwords are required by SBA policy.

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

N/A

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

N/A

F. DATA ACCESS

1) **Who will have access to the data in the system?** (e.g., contractors, users, 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 the company CCH, a tax and accounting software provider. Changes to application software are by CCH. CCH 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 Managers are given the role "Preparer/Review" which allows them to both prepare and review audit evidence.

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

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

Audit directors are the given 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? (Please list processes and training materials)**

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 Automated Information Security Systems 5 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 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?**

The TeamMate software package is owned by the company CCH, a tax and accounting software provider. Changes to application software are by CCH who distributes the software changes via CD-Rom to OIG. OIG installs the updated versions of the software on audit desktop and laptop computers. CCH 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?**

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

8) **Will other agencies share data or have access to the data in this system via transferred or transmitted (Federal, State, and Local, Other (e.g., Tribal))?**

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

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

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

10) What procedures are in place for assuring proper use of the shared data?

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

11) Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for information shared internal and external.

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

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) **System Owner**

Debra S. Ritt (Signature) 7-26-10 (Date)

Name: Debra S. Ritt

Title: Assistant Inspector General for Audit

---

2) **Project Manager**

(Signature) 7.26.10 (Date)

Name: Audrey B. Delaney

Title: Auditor

---

3) **IT Security Manager**

(Signature) 8/13/2010 (Date)

Name: *Lawrence Gottlieb*

Title: Chief Information Security Officer

---

4) **Chief Privacy Officer**

(Signature) 9/3/2010 (Date)

Name: Paul *T. Christy*

Title: Acting Chief Privacy Officer