

**United States Small Business Administration
Privacy Impact Assessments
Official Guidance**



February 2009

**Office of the Chief Information Officer
Office of the Chief Privacy Officer**

**The U.S. Small Business Administration
Privacy Impact Assessment
And Guidance**

Table of Contents

<i>EXECUTIVE SUMMARY</i> _____	<i>iii</i>
<i>OVERVIEW</i> _____	<i>1</i>
What is the Privacy Impact Assessment (PIA)? _____	<i>1</i>
When is a PIA Required? _____	<i>2</i>
How are PIAs Submitted? _____	<i>3</i>
1) With OMB Budget Submissions in Exhibit 300s _____	<i>3</i>
2) With Paperwork Reduction Act Submissions _____	<i>3</i>
3) With the SBA IT Security Certification and Accreditation Process _____	<i>3</i>
What if the System Maintains No Information on Individuals in Identifiable Form? _____	<i>4</i>
Who Contributes to a PIA? _____	<i>5</i>
Understanding the PIA Guide _____	<i>6</i>
PII Samples _____	<i>6</i>
Document Breakdown _____	<i>6</i>
<i>PRIVACY IMPACT ASSESSMENT TEMPLATE</i> _____	<i>8</i>
A. CONTACT INFORMATION _____	<i>8</i>
B. SYSTEM APPLICATION/GENERAL INFORMATION _____	<i>9</i>
C. SYSTEM DATA _____	<i>10</i>
D. DATA ATTRIBUTES _____	<i>12</i>
E. MAINTENANCE AND ADMINISTRATIVE CONTROLS _____	<i>15</i>
F. DATA ACCESS _____	<i>16</i>
<i>Privacy Impact Assessment PIA Approval Page</i> _____	<i>20</i>
<i>APPENDIX A</i> _____	<i>A-1</i>
<i>Sample Completed PIA</i> _____	<i>A-1</i>
<i>APPENDIX B</i> _____	<i>B-1</i>
<i>Privacy Threshold Analysis (PTA)</i> _____	<i>B-1</i>
<i>APPENDIX C</i> _____	<i>C-1</i>
<i>The US SBA PII Survey</i> _____	<i>C-1</i>

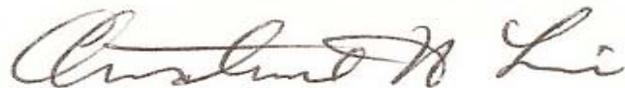
EXECUTIVE SUMMARY

The Privacy Impact Assessment (PIA) is one of the most important instruments through which the SBA establishes public trust in its operations. As the Chief Information Officer/Privacy Officer, I am responsible for ensuring that technologies developed and used by the Small Business Administration (SBA) sustain and do not erode privacy protections. The PIA is a vital tool that evaluates possible privacy risks and the mitigation of those risks throughout the development life cycle of a program or system. The transparency and analysis of privacy issues provided by a PIA demonstrates that the Agency actively engages program managers and system owners on the mitigation of potential privacy risks.

By conducting a PIA, the SBA demonstrates its consideration of privacy during the development of programs and systems and thus upholds the SBA's commitment to maintain public trust and accountability. Without the trust of the public, the SBA's mission is made more difficult. By documenting the procedures and measures through which the Agency protects the privacy of individuals, the Agency can better carry out its mission.

Over the past year, the OCIO has issued a template on the PIAs to the Program Offices to use for programs and systems. OCIO has revised the template to include new requirements from the Office of Management and Budget to address systems under development, risk mitigation and FISMA requirements. These requirements are specifically targeted for both major and minor information systems containing **personally identifiable information (PII)**.

If you have any question regarding this guidance please communicate your questions to Ethel Matthews, Senior Advisor to the Chief Privacy Officer at (202) 205-7173.



Christine H. Liu
Chief Information Officer and
Chief Privacy Officer

The U.S. Small Business Administration Privacy Impact Assessment and Guide

OVERVIEW

What is the Privacy Impact Assessment (PIA)?

A PIA assists U.S. Small Business Administration (SBA) employees in identifying and addressing information privacy when planning, developing, implementing, upgrading and operating agency information management systems that maintain information on individuals. A PIA provides information on how personally identifiable information¹ (PII) is collected, stored, protected, shared and managed within an information system. The Office of Management and Budget's (OMB) Memorandum M-03-22, dated September 26, 2003 defines the PIA as:

“Privacy Impact Assessment (PIA) – is an analysis of how information is handled:
(i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
(ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form¹ in an electronic information system, and
(iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.”

The PIA process helps to identify sensitive systems to ensure that appropriate information assurance measures are in place, such as secured storage media, secured transmission, special handling instructions, and access controls.

The goals accomplished in completing a PIA include:

- Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;
- Accountability for privacy issues;
- Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and
- Providing documentation on the flow of personal information and information requirements within SBA systems.

When developing a PIA, the process requires candid and forthcoming communications between the System Manager or Data Owner and the Privacy Office to ensure appropriate and timely handling of privacy concerns. By publicly addressing the privacy concerns through the use of a PIA it provides a public trust in the operation of the Small Business Administration and its many

¹ “Personally Identifiable Information” - According to the OMB Memo M-06-19, means information about an individual maintained by an agency including, but not limited to education, financial transactions, medical history, and criminal and employment history and information which can be used to distinguish or trace an individuals identity, such as their name, social security number, and place of birth, mothers maiden name, biometrics records etc., including any other personal information which is linked or linkable to an individual.

programs. The PIA helps the public to understand what information is being collected, stored, used, and protected by the SBA. and it will examine how the SBA has incorporated privacy concerns throughout the systems development, design, and deployment of the technology and/or rulemaking.

The PIA will be used to demonstrate that the SBA considers Privacy from the beginning stages of development to the end of the system development lifecycle. It is important that the privacy controls are incorporated into the system from the start, and not after the system has been developed. Implementing the controls from the start shows that system developers and owners have made technology choices that reflect the incorporation of privacy into the systems fundamental architecture.

When is a PIA Required?

According to the OMB guidance (M-03-22), the E-Government Act requires agencies to conduct a PIA before:

1. Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public;
2. Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government); and
3. Where a system change creates new privacy risks. The following are examples where privacy risks may occur:
 - a) Converting paper-based records to electronic systems;
 - b) When functions change anonymous information into information in identifiable form;
 - c) New uses of an existing IT system significantly changes how information in identifiable form is managed in the system;
 - d) Agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;
 - e) User-authenticating technology (password, digital certificate, biometric) is newly applied to an electronic information system assessed by members of the public;
 - f) Agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources;
 - g) Agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives (in such cases the lead agency should prepare the PIA);
 - h) Alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form; or
 - i) New information in identifiable form added to a collection raises the risks to personal privacy.

How are PIAs Submitted?

1) With OMB Budget Submissions in Exhibit 300s

For projects that collect and manage information on **individual members of the public** (vs employees) OMB now requires that a PIA is addressed appropriately in budget requests (see OMB Circular A-11 <http://www.whitehouse.gov/omb/circulars/a11/2002/S300.pdf>). Exhibit 300, discusses identifying and assessing security and privacy risks as a part of the overall risk management effort for each system supporting or part of the investment. The identifying information asks if there is at least one Privacy Impact Assessment which covers the system in question. According to OMB, Security and Privacy Planning must proceed in parallel with the development of the system(s) to ensure IT security and privacy requirements and costs are identified and incorporated in the systems lifecycle. This is also implemented in a number of areas within Exhibit 300 which discusses the contracts and task orders as they relate to the system. This ensures that value is added to any current or planned systems.

2) With Paperwork Reduction Act Submissions

The E-Government Act also requires that the questions below be addressed with a new electronic collection of information when collected from 10 or more persons (does not include agencies, organizations, or employees of the federal government). See OMB Memorandum, M-03-22 dated September 26, 2003, Attachment A, II, D for more information on the E-Government Act and Paperwork Reduction Act interface.

The following information should be included with the OMB 83-I Supporting Statement (request to OMB to approve a new agency information collection) when being submitted to OMB:

- a) A description of the information to be collected in the response to Item 1 of the Supporting Statement;
- b) A description of how the information will be shared and for what purpose in Item 2 of the Supporting Statement;
- c) A statement detailing the impact the proposed collection will have on privacy in Item 2 of the Supporting Statement;
- d) A discussion in Item 10 of the Supporting Statement of:
 1. Whether individuals are informed that providing the information is mandatory or voluntary;
 2. Opportunities to consent, if any, to sharing and submission of information;
 3. How the information will be secured; and
 4. Whether a system of records is being created under the Privacy Act.

3) With the SBA IT Security Certification and Accreditation Process

For all systems that maintain information on individuals (both employees and members of the public), the SBA requires that a PIA be completed for a SBA Information Technology (IT) Security Certification and Accreditation (C&A). The SBA IT Security Plan outlines the policies and procedures for the C&A process. This ensures that systems including information on employees are also compliant with Privacy Act requirements.

What if the System Maintains No Information on Individuals in Identifiable Form?

The Office of the Chief Information Officer requests that a Privacy Threshold Analysis (PTA), in Appendix B, be completed to ensure that a thorough review is made of an IT system without information on individuals in identifiable form. The CIO, or a designee, will determine if a complete PIA is needed based on the PTA.

This “preliminary PIA” will be maintained with the Chief Privacy Officer, to verify that a review for information on individuals was already done for the system.

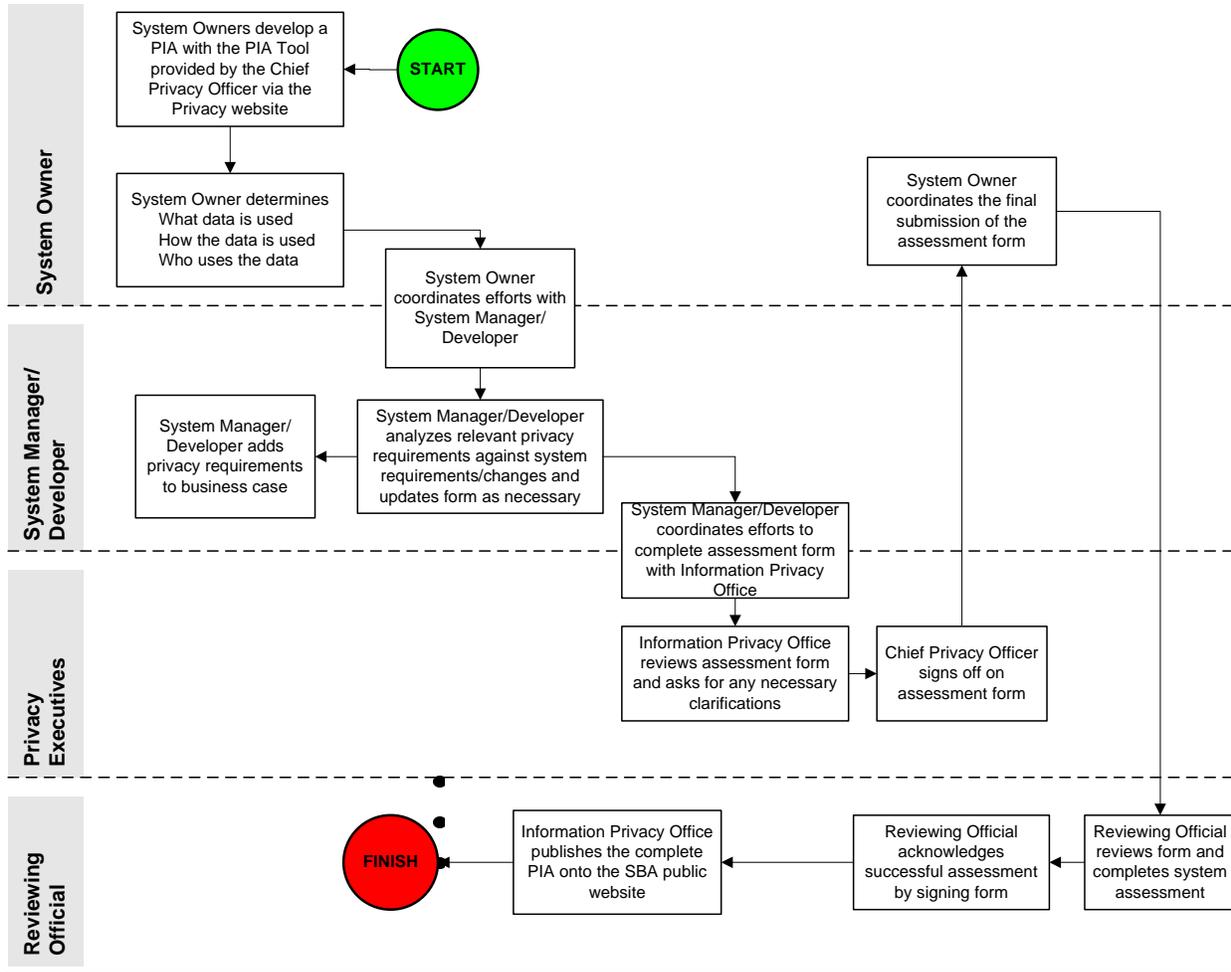
The lack of a system’s information on individual members of the public must be reported if an OMB Exhibit 300 is required for the system. System owners should indicate in Section E, Table 8(d)(f) that a PTA established that no personally identifiable information on individual members of the public was present and there was no reason to complete the PIA. This will make it clear to OMB that SBA performed an analysis and provides the reason why a PIA was not completed. (See Exhibit 300 sections E.8.).

For OMB guidance on when a PIA is not required, refer to OMB Memorandum M-03-22, Attachment A, Section II.B.3.

Who Contributes to a PIA?

SBA Privacy Impact Assessment Roles and Responsibilities

PIA Chart



Note: System Owners should allow time to coordinate information collection approvals if necessary through the FOI/PA Office, the approved document (SORN) must then be published in the Federal Register. The Office of Management and Budget must be given 30 days notice prior to the altering of any system of record notice on file. The Records Disposition Schedules will be coordinated with your Records Management Officer.

Understanding the PIA Guide

This guidance provides explanations and references for completing questions in the Privacy Impact Assessment template. The template suggests possible ways to complete answers of the designated questions. It also provides the necessary guidance to ensure that the writer of the document has the necessary resources to provide a complete answer. The document also suggests tips on what to look for when researching questions to provide as much detail as possible.

In the development of the information systems Privacy Impact Assessment (PIA), it is very important to understand how the information will be handled. The PIA is an analysis, which provides the public with the knowledge of how their personal information will be protected when provided to the Small Business Administration. This PIA Guide will include questions and guidance to completing the full assessment of your information system.

The document allows the writer to coordinate with staff and others regarding the makeup of their system architecture. It provides the tools needed to ensure that the needed privacy controls are integrated into the information systems architecture.

It is important to understand that a PIA is to be documented for every IT system which collects, stores, protects, shares and manages PII. The document is a living document, which is updated as the system develops and changes occur with the system and its handling of the data. Samples of PII data include, but are not limited to the following:

PII Samples

Name	Mailing Addresses
Social Security Number (SSN)	Telephone Numbers
Checking or Savings Account Number	Driver's License Numbers
Data of Birth	Biometric Identifiers
Electronic Identification Numbers (EIN)	Email Address

Document Breakdown

The Privacy Impact Assessment Guide contains four appendices including: 1) a sample completed PIA; 2) a Privacy Threshold Analysis (PTA); and 3) a copy of the SBA PII Survey, which will assist the Information Privacy Office in gathering information to make a complete assessment of the SBA's PII holdings. The sample PIA and the PTA are described below:

Sample PIA

This document contains a sample completed PIA to provide guidance as to what type of information should be entailed within your completed document. This fictitious system is only used as a guide to assist you in answering your questions. It provides a look at the formulation of answers, as well as provides a general idea of what type of information to provide when completing the Privacy Impact Assessment. The completed PIA allows the user to get an idea of how information should be provided without providing intellectual property of the information system and its security controls.

Privacy Threshold Analysis

This document will assist the information owner and Information Privacy Office in ensuring that a document is on file with an analysis of the system describing if it is used to store, manage, or utilize PII. This analysis will break down the data and provide the Information Privacy Office with the tool to determine if a complete Privacy Impact Assessment will be required for the information system/application. It is our goal to establish a one to one relationship for every system to have a Privacy Threshold Analysis for each system within the organization. This will ensure that every system has been analyzed to determine if PII exists on the system or application.

For assistance and to obtain an electronic version of this document, please contact the Chief Privacy Officer, the Senior Advisor to the Chief Privacy Officer, or visit the SBA Website at <http://www.sba.gov/aboutsba/sbaprograms/OCIO/pia/index.html>.

PRIVACY IMPACT ASSESSMENT TEMPLATE

Name of System/Application:

Program Office:

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

Guidance: Each listing should include the full name, title, SBA Office and program, SBA phone number and SBA e-mail.

1) Who is the person completing this document? (Name, title, SBA Office, phone number, and SBA e-mail)

2) Who is the system owner? (Name, title, SBA Office, phone number and SBA e-mail)

Guidance: This is the official responsible for this system that will implement the legal information resources management requirements (privacy, security, Freedom of Information Act, system of records, data administration, etc).

3) Who is the system manager for this system or application? (Name, title, SBA Office, phone number, and SBA e-mail)

Guidance: The manager who manages the day-to-day operations of an existing system, including having responsibility for the timely, accurate and relevant collection of individual's information and the information's lifecycle throughout the SBA. The term "System Developer" may also be used for those systems in development, and refers to the manager who develops the business case for procurement and governance purposes.

4) Who is the IT Security Manager who reviewed this document? (Name, title, SBA Office, phone number and SBA e-mail)

Guidance: This is the SBA's Chief Information Security Officer (CISO) or a designated Program Office IT Security Manager..

5) Who is the Privacy Officer who reviewed this document? (Name, title, SBA Office, phone number and SBA e-mail)

Guidance: Provide the name of the Chief Privacy Officer (CPO) or designee, often the Senior Advisor to the Chief Privacy Officer.

6) Who is the Reviewing Official? (Name, title, SBA Office, phone number, and SBA e-mail)

Guidance: This is the SBA's CIO or other agency head designee, other than the official procuring the system or the official who conducts the PIA).

B. SYSTEM APPLICATION/GENERAL INFORMATION

Guidance: This section offers an overview and defines the scope of general system information and pertains to any system that collects, maintains, uses, and disseminates information, and that can be retrieved by the name or other identifier particular to an individual(s). This section also pertains to electronic systems of records (SOR) covered by the Privacy Act. For more information on SORs, refer to the SBA Privacy Act Procedures Manual.

(<http://collab.sba.gov/sops/Documents/4004/SBASOP-40-04-3.pdf>)

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

Guidance: Explain how information is collected (paper form, online application, etc.), and list all types (full name, social security number, birth date, address, account numbers, biometric identifiers etc...) of information collected and stored in the system throughout the information's lifecycle.

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

Guidance: If yes, a PIA must be submitted with the IT Security C&A documentation.

b. Is the information about employees?

Guidance: If yes, and there is no information about members of the public, the PIA is required for the SBA IT Security C&A process.

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

Guidance: Complete answers to questions such as: What will be the primary uses of the system/application? How will this support the program's mission? Please provide a detailed explanation about your system/application.

3) Is the system in the development process?

Guidance: If no, continue with question 4. If yes, please describe:

1. Privacy documentation related to system's development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
2. The impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in question B(1) above, to the extent these elements are known at the initial stages of development;
3. Updates needed before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.

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

Guidance: Consider the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) and explain how information handling changes at each stage may affect individuals' privacy. The analysis for existing or developing systems should include an extensive analysis of the:

1. *Consequences of collection and flow of information, or any changes associated with system updates;*
2. *Alternatives to collection and handling as designed or updated;*
3. *Appropriate measures to mitigate risks identified for each alternative and,*
4. *Rationale for the final design choice or business process.*

Additionally, SBA may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.

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

Guidance: *Describe the statutory provisions or Executive Orders that authorize the maintenance of the information to meet an official program mission or goal. Please review the system documentation and other information related to the design, approval, and implementation of the system/application.*

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

Guidance: *Please discuss the particular security risks presented by the system and how they have been mitigated. Do not discuss in such detail as to compromise security measures, but please discuss how the security measures enable for the system (user access controls, auditing, etc.) help mitigate any potential risk to the security of the system or the privacy of the information it contains. You can reference the system C&A and FISMA documentation.*

C. SYSTEM DATA

1) What categories of individuals are covered in the system?

Guidance: *Explain the customer groups that are served by the system, such as loan applicants, small business owners, lenders, etc.... What type of individuals are utilized within the system?*

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?

Guidance: *List of sources of the information, such as individuals applying for loans, creditors and/or forms individuals completed from an SBA web page. Write a short explanation of each source.*

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

Guidance: *List any federal agencies where the data originates. (E.g., the Social Security Administration, the Internal Revenue Service, Office of Personnel Management etc.) Explain how information is being received by the system.*

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

Guidance: *List all Tribal, State or local agencies that provide information where the data originates.*

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

Guidance: List any third party (usually a **non-Federal** person or **entity**), which may be a source of data/information (i.e., a lender, an internet service provider, a data center host).

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

Guidance: Be as specific as possible and list information on individuals collected from the public such as a social security number, address, debts owed, account numbers, and telephone numbers. Employee information may include badge number, user identifier, telephone number, social security number and health information.

If you are collecting information from the public, contact your Information Collection Clearance Officer to ensure that you have an OMB approval to do so or to determine whether you need to obtain an OMB approval to collect the information. The Paperwork Reduction Act of 1980 establishes requirements for collecting the same information from 10 or more individuals (this does not include employees acting in their official capacity). This information may be helpful in responding to Exhibit 300, Part II, D.3, regarding OMB approval codes for collections of information.

This information is used in preparing the Privacy Act system of records notice. If the system already has a Privacy Act system of records notice, then the information for this question should reflect the information already in the notice.

3) Accuracy, Timeliness, and Reliability

Guidance: The Privacy Act of 1974 requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. These requirements are statutory and the PIA should explain SBA's efforts to comply.

Document how the requirements are enforced while the data is retained in the system, and what data is considered sensitive. Maintaining metadata (documentation on the data) is important so it can be referenced in the future to identify data conditions when making decisions about data from a system (see OMB Circular A-130 8.a.4, SBA Privacy Manual).

Although the following does not apply to information covered by the Privacy Act, information used to make or influence decisions and that is published in the public domain, may be subject to challenge by the public under the Data Quality Act. The need to publish correct and useful information should always be a concern. Third party information or information originating outside of SBA that is adopted by SBA in any decision-making process is subject to the Data Quality Act and efforts to comply should be outlined in the question.

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

Guidance: Explain efforts by business partners (other agencies, lenders or other third-party organizations) to verify data accuracy due to the Privacy Act provisions that require that only relevant and accurate records should be collected and maintained about individuals. Explain whether information in the system is checked against any other source of information outside

your organization before the information is used to make decisions. If not, are rules and procedures in place to reduce data inaccuracies within the system. Discuss these rules and procedures.

Data accuracy and reliability are important requirements in implementing the Privacy Act. The statute requires that each agency that maintains a system of records shall “maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.”

(5 U.S.C. 552a (e) (5)).

b. How is data checked for completeness?

Guidance: *Explain the process to check data before the data is deemed accurate. Are controls in place to ensure completeness of data prior to its processing? Explain.*

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).

Guidance: *Describe the steps or procedures that are taken to ensure the data is current, including, if applicable, the document (e.g., data models).*

If the data is out-of-date, then the relevancy and accuracy of the data are called into question. This is particularly true with data warehousing. A data warehouse may contain data that is not current, which would cause a domino effect throughout the data stores.

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

Guidance: *The data element description should provide information on the legal requirements of the data. Data elements should also be documented in keeping with OMB Circular A-130 requirements for determining the privacy impact at each stage or phase of the information life cycle.*

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

Guidance: *For example, if the Program Manager or System Owner chose to restrict collection of information please include the reasons behind the decreased scope of collection. Further, if specific risks are inherent to the sources or methods of collection, please discuss how those risks were mitigated.*

D. DATA ATTRIBUTES

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

Guidance: *Explain why SBA processes cannot accommodate less specific data. The Privacy Act at 5 U.S.C. 552a(e)(1) requires that “each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to*

accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.”

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?

Guidance: Explain how the system will derive new data and create previously unavailable data about an individual through aggregation from the information collected, and how that will impact information’s lifecycle within the SBA.

What is meant by derived and aggregation?

➤ *Derived data* is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

➤ *Aggregation of data* is the taking of various data elements and then turning it into a composite of all the data to form another type of data. (For example, tables or data arrays).

Refer also to the General Accounting Office (GAO) report on “Data Linkage and Privacy” (GAO-01-126SP) at <http://www.gao.gov/new.items/d01126sp.pdf>.

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

Guidance: Describe how the new data that is created either by deriving or aggregating the data be attached to a person’s record. Will it be placed in a new filing system? Or will it be placed in an existing file system with information on the individual (for example, in the employee’s Official Personnel File or manager’s file)?

4) Can the system make determinations about employees or members of the public that would not be possible without the new data?

Guidance: If No, state “No”. If yes, explain how automated or manual analysis using the new system may produce information about the individual.

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

Guidance: This question only applies if new data is aggregated or derived to make a decision based on question D.4. Refer to the relevance, accuracy and timeliness questions provided for question C.3 above. If the question is not applicable please state N/A.

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

Guidance: Describe efforts to safeguard the consolidated data, if the data is being consolidated, that is, combined or united into one system, application, or process. Explain existing controls, if any, that remain to protect the data and any necessary efforts to strengthen the control(s) to ensure that the data is not accessed inappropriately or by someone unauthorized to access the data. These controls will help to prevent unauthorized use from occurring. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III. Another consideration is the use of

Role Based Access Controls (RBAC). For more information on RBAC go to <http://csrc.nist.gov/rbac/>.

The SBA Security SOPs describe the practice of identification and authentication that is a technical measure that prevents unauthorized people or processes from accessing data. The IT Security C&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.

- 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”.**

Guidance: Refer to the SBA IT Security Risk Assessment Guide processes, deliberately developed to be broad in scope, when describing the technical security aspects and the managerial and operational as well. When processes are consolidated, management must maintain the proper controls minimizing the risk to all systems. The IT Security C&A process requires that a risk assessment be performed regularly on SBA’s major applications, networks, and computer installations.

- 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.**

Guidance: Explain how a personal identifier associated with data retrieval mechanism is used and list each potential identifier. This may be an extensive list, if a database has multiple links between data points, like a name and a zip code or a street number and a first name. A system with data on individuals that is retrieved by a name or personal identifier is a Privacy Act system and will need a published system of records notice in the Federal Register. If you do not have a published system or record notice, contact the SBA’s Privacy Officer.

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

Guidance: Create a table listing every report, its use and who will have access to it. Also, include examples of potential ad-hoc 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 individuals can grant consent.**

Guidance: Explain the process for individuals to decline to provide the information, and the work-around to accommodate these requests within the system. Responses to Information Collection Clearance packages submitted to OMB also request the same information, and a response can be taken from that package. Contact your Office of Administration (OA).

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

Guidance: *For example, is appropriate use of information covered in training for all users of the system? Are disciplinary programs or controls (i.e. denial of access) in place if an individual is found to be inappropriately using this information?*

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?

Guidance: *Describe processes and procedures that allow multiple sites to safeguard accurate, timely and relevant data throughout the data's lifecycle.*

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

Guidance: *Describe how the system complies with the Privacy Act requirements for the retention and disposal of information about individuals in Privacy Act system of records. Do not neglect records that reside in backups. (The information is published in the Federal Register with the Privacy Act system of records notice). Retention also supports the Privacy Act requirement to maintain such records "with such accuracy, relevance, timeliness, and completeness...."*

The retention periods of data/records that the SBA manages are explained in the Records Management Program.

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?

Guidance: *Clarify how records are determined to be unneeded, and how those records are disposed of, including backups. Disposing of the data at the end of the retention period is the last state of life cycle management. Records subject to the Privacy Act have special disposal procedures. Also, refer to SBA SOP 00 41 02, Records Management Program, and National Institute of Standards and Technology special publications on Managing Sensitive Information Systems.*

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

Guidance: *Explain any innovations in technology or process that are new to SBA, including how technology or process was accepted, including any activity logs or backups that may contain individual information. Are there new ways used to monitor activities of the individual in any way? For example, access logs may already be used to track the actions of users of a system, but new software allows keystroke monitoring.*

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

Guidance: *Describe the impact on either public or employee privacy the new technology or process will have on affected individuals. If "N/A," please state so.*

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Guidance: Most systems provide the capability to identify, locate, and monitor individuals (e.g., audit trail systems/applications). Data base administrators or systems engineers for a particular system should be able to address this issue.

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

Guidance: The SBA IT Security Plan describes the audit trail process. In response to this question provide what audit trails are maintained to record system activity and user activity including invalid logon attempts and access to data. The IT Security C&A process require a system security plan outlining the implementation of the technical controls associated with identification and authentication.

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

Guidance: Explain the processes and tools used to avoid and detect unauthorized monitoring, such as business rules, internal instructions, technologies or posted Privacy Warning Notices.

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

Guidance: If a system is a Privacy Act system of records, a Privacy Act system of records notice **must be published** in the Federal Register **before a system can operate** according to the Privacy Act. If you do not know the Privacy Act systems of records (SOR) notice, contact the SBA Privacy Officer. Any officer or employee who knowingly and willfully maintains a SOR without meeting the Privacy Act notice requirements (5 U.S.C. 552a (e)(4)) is guilty of a misdemeanor and may be fined up to \$5,000. Also refer to information for question D. 8 above.

If a name or other personal identifier is not used to retrieve information, it is possible that the system is not a Privacy Act system. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may be protected from disclosure under the Freedom of Information Act.

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

Guidance: The system may already have a Privacy Act system of records notice that applies to it, although the Privacy Act requires that amendments to an existing system must also be addressed in a Federal Register notice (see the SBA Privacy Act Manual). Consult with the SBA's Privacy Officer.

F. DATA ACCESS

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

Guidance: Create a list of all potential users who may have system access, including "other" users who may not be as obvious as those listed above, such as the GAO or the Inspector General. "Other" may include database administrators or IT System Security Managers. Also

include those listed in the Privacy Act system of records notice under the “Routine Use” section when a Privacy Act system of records notice is required. The more comprehensive the list, the better it is.

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

Guidance: Describe the division of users into groups, the roles of potential user groups, as well as the responsibilities of those that require access. Explain how the groups must access the system to fulfill the SBA’s mission. For the most part, access to data by a user within the SBA is determined by the “need-to-know” requirements of the Privacy Act (this means to authorized employees WITHIN the SBA who have a **need for the information to perform their duties**). Care should be taken to ensure that only those employees who need the information have access to that information. Other considerations are the user’s profile based on the user’s job requirements and managerial decisions.

The criteria, procedures, controls and responsibilities regarding access must be documented to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy. What criteria will the manager and system security person use to decide on access to the data, for example?

The SBA Privacy Manual indicates that the system manager is responsible for ensuring that access to information and data is restricted to authorized personnel on a “need-to-know” basis.

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

Guidance: Describe the criteria used to determine access for each group of users. Also see explanation in #2 above. Usually, a user is only given access to certain data on a “need-to-know” basis for information that is needed to perform an official function. Care should be given to avoid “open systems” where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system and/or application. However, restrict access when users may not need to have access to all the data. For more guidelines on this, refer to the Federal Information Processing Standards [FIPS] Publications at <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>

The IT Security Plan describes the practice of applying logical access controls. Logical access controls are system-based means by which the ability is explicitly enabled or restricted.

It is the responsibility of managers of systems to ensure no unauthorized access is occurring.

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)

Guidance: List and describe the business rules, internal instructions, posting Privacy Warning Notices or training efforts that are used to address access controls and violations for unauthorized browsing and access. Outline the processes applied on a day-to-day basis.

According to OMB Circulars A-123 and A-130, every system/application/process that uses data must have some sort of control to prevent the misuse of the data by those having access to the data.

The IT Security Plan describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data. The C&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.

Additionally, all employees, including contractors, have requirements for protecting information in Privacy Act systems (see SBA Privacy Act regulations). Describe the controls in place. This will be helpful in completing Exhibit 300, Part II. C. 2. (D).

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?

Guidance: Explain which contractors have access for development or maintenance, and why, and include the contract number if necessary. Include the Privacy Act contract clauses inserted in their contracts, along with any other relevant regulatory contract language.

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

Guidance: This question deals primarily with interfaces between processes, systems and applications, and any Memorandums of Understanding (MOU) that apply. Describe the connection or method for sharing data (FTP or XML transmission or transferred). The appropriate IT specialist may be able to describe the connection if additional technical information is required.

For further information on interfaces and applicable guidance, refer to FIPS Publication 191, Local Area Networks. The publication contains definitions and explanations that may assist you (see FIPS publications at <http://csrc.nist.gov/publications/fips/fips191/fips191.pdf>).

Review SBA SOP 40 04 3, Privacy Act Procedures to determine whether any information that may come from an existing Privacy Act SOR allows that information to be exchanged and used for these new purposes or uses.

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

Guidance: Outline the roles and responsibilities for safeguarding privacy in the system., Although all employees who have access to information in a Privacy Act system have some responsibility for protecting personal information covered by the Privacy Act (see SBA SOP 40 04 3, Privacy Act Procedures), often the information owner and system manager (identified in the Privacy Act system of records notice) share responsibilities.

For system manager responsibilities identified by the Privacy Act refer to SBA Privacy Act Procedures.

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))?

Guidance: This question deals primarily with agencies outside of the SBA and will include the oversight agencies.

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

Guidance: Describe how each agency will use the data being transferred or transmitted.

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

Guidance: Explain how the SBA and the other agency will safeguard the data use, including logging or tracking access, physical security, destruction, etc. Refer to OMB Circulars A-123: Management Accountability, and A-130: Management of Federal Information Resources.

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

Guidance: For example, if your Program Office has access to the system that your Office controls, discuss how access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing of information. You can discuss interagency memorandum of understanding between your agency and other agencies, to include third party entities.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) System Owner

_____ (Signature) _____ (Date)

Name:

Title:

2) Project Manager

_____ (Signature) _____ (Date)

Name:

Title:

3) IT Security Manager

_____ (Signature) _____ (Date)

Name:

Title:

4) Chief Privacy Officer

_____ (Signature) _____ (Date)

Name:

Title:

APPENDIX A

Sample Completed PIA

The U.S. Small Business Administration Privacy Impact Assessment

Name of Project: Small Business Administration Electronic FOIA Tracking System (EFTS)
Program Office: The Office of the Chief Information Officer (OCIO)

A. CONTACT INFORMATION

(1) Who is the person completing this document?

Alexandra Mallus
Freedom of Information Act (FOIA) Officer,
Office of the Chief Information Officer
(202) 208-5342
Alexandra.Mallus@sba.gov

(2) Who is the system owner (name, organization and contact information)?

Name: Dave Thomas
Title: Director, Office of Freedom of Information Act
Office: Office of Freedom of Information Act
Phone: 202-206-6323
Email: DThomas@sba.gov

(3) Who is the system manager for this system or application (name and contact information)?

Name: Robert Romero
Title: IT Specialist
Office: Office of Freedom of Information Act
Phone: 202-323-2000
Email: RRomero@sba.gov

(4) Who is the IT Security Manager for this system and their contact information?

Name: Troy Thompson
Title: Acting Chief Information Security Officer
Office: Office of the Chief Information Officer
Phone: (202) 205-6351

Email: Troy.Thompson@sba.gov

(5) Who is the Privacy Act Officer who reviewed this document (name and contact information)?

Ethel M. Matthews
Senior Advisor to the Chief Privacy Officer
Office of the Chief Information Officer
(202) 205-7173
Ethel.Matthews@sba.gov

(6) Who is the Reviewing Official?

Christine Liu
Chief Information Officer/Privacy Officer
Office of the Chief Information Officer
(202) 205-6708
Christine.Liu@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

(1) Does the system contain any personal information about individuals? If yes, explain.

The system contains personal information about individuals, e.g., name, home address, home telephone and fax numbers, personal e-mail address, and other pertinent information related to processing and responding to their FOIA and Privacy Act requests.

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

No

b. Is the information about employees?

Yes

(2) What is the purpose of the System/Application?

The primary purpose of this system is to facilitate the manageability and efficiency of the FOIA and Privacy Act (PA) process throughout the U.S. Small Business Administration (SBA). The system will allow the tracking of FOIA/PA requests from receipt to completion, provide valuable information to SBA FOIA Coordinators, identify duplicate requests, ensure consistency in responses, reduce the time in processing requests, support action on FOIA requests, appeals, and litigation, facilitate reporting and reviews, and improve customer service.

(3) Is the system in the development process? No

(4) How will the technology investment (new or updated) affect existing privacy process? N/A

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

5 U.S.C. 552; 5 U.S.C. 552a

(7) Privacy Impact Analysis: What privacy risks were identified and describe how they were mitigated for security and access controls.

The Agency's FOIA Public Liaisons and FOIA Service Center Representatives and Office of the Chief Information Officer employees and contractors with a need to know have access to the system and Privacy Act contract clauses are inserted in contractors' contracts. As these records are subject to the Privacy Act and to eliminate privacy risks such as misuse of the information, the designated employees submit an access request to SBA's security team who submits the request to the FOI/PA Office for approval. Once approved employees can only access the system with their user name, identification and password. The system locks after three failed access attempts. FOIA Public Liaisons and Service Center Representatives can only view their office's data. The System has two levels of security; security roles and access have been designed and assigned based on the roles of the user community. This is detailed in the User's Manual and training video both of which are available from the SBA Yes page.

C. DATA IN THE SYSTEM

(1) What categories of individuals are covered in the system?

Individuals who have submitted FOIA/PA requests and administrative appeals; individuals whose requests or records have been referred to the Department by other agencies; and in some instances attorneys representing individuals submitting such requests, appeals and litigation; individuals who are the subject of such requests, appeals, litigation, and/or the SBA personnel assigned to handle such requests, appeals and litigation.

(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 in this system comes primarily from the individuals who submit FOIA/Privacy Act requests, internally generated documents, and employees processing the requests.

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

None

c. What Tribal, 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?

Information collected will include, but not be limited to: name, home/business address; home/business telephone number; fax and email numbers; organizational affiliation; all FOIA costs incurred including payments; date of request; subject of request; pertinent information associated with office contact information; other information related to processing and responding to requests, e.g., disposition of requests.

(3) Accuracy, Timeliness, and Reliability

All FOIA Officers and Coordinators will be responsible for ensuring that information entered into the system is accurate and complete. Information will be entered in a timely manner and updated in the system as appropriate. There are software controls in place to ensure accuracy of both data fields and cross field relationships.

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

Information is received from individual FOIA/PA requesters and is only as reliable as that provided by the requester.

b. How is data checked for completeness?

The system is designed to require specific information be entered in order to consider the FOIA/PA request complete. If the required information is not entered into the system, the FOIA/PA request will not be accepted by the system.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not dated? (i.e., data models, name documents)

Information is received from individual FOIA/PA requesters and is only as reliable and current as that provided by the requester.

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

The EFTS is comprised of specific data fields. These fields will be described and detailed in a data dictionary as prepared by the contractor. In addition, specific guidance regarding data entry for specific fields is included in the business rules and guidelines for the EFTS.

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

Since these are Privacy Act records, access is limited to SBA employees who are designated as a FOIA Public Liaison or a FOIA Service Center Representative. Privacy risks are minimized since access to the system is obtained through a two-step approval system shared with IT Security and the FOIA/PA Office.

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?

The information collected in the EFTS is necessary and is directly related to the reason for which the system has been designed. The majority of the data elements are required for preparation and submission of the FOIA Annual Report to Congress (5 U.S.C. 552(e)).

(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. The system will allow users to aggregate information about requesters with regard to the number, nature of, and costs associated with FOIA/PA requests they have submitted to the U.S. Small Business Administration.

(3) Will the new data be placed in the individuals' record?

The data will be maintained in the EFTS.

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

Yes, through the use of the system, the Department, as well as the offices, will be able to determine what records have been created and completed by users in the system.

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

Refer to the information provided for question C (3).

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

The system consolidates the information provided by requesters and users for the express purpose of providing computerized reports. No privacy information is consolidated in this system or reports from the system, only general statistical information pertaining to FOIA activities, i.e., dollar amounts, number of days spent processing requests.

(7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain. If process is not consolidated please state, "N/A".

The EFTS is designed to protect data fields once the FOIA/PA request has been completed. Additionally, access to the EFTS will only be granted to those persons within the U.S. Small Business Administration and specifically authorized by the FOIA/PA Officer. Access levels and permission levels have been established and authorized only to those persons who have a need to know the information contained in the system in order to carry out their duties. In accordance with OMB Circulars A-123, and A-130, Appendix III, the electronic FOIA tracking system will have controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of: firewalls and IP addresses, passwords, user identification, database permissions and software controls (see F(4)).

(8) How will the data be retrieved? Can it be retrieved by a personal identifier? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

Data will be retrieved by various fields including, name of requester, date of request, subject of request, FOIA number and/or the organizational affiliation of the requester, 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?

The system will be able to produce reports using various parameters determined by the user but limited to only the information that has been provided by the requester. The reports will enable the user to determine certain information regarding the requests submitted including types of requests, categories of requests, numbers of requests, dates

pertinent to requests, costs associated with the requests, etc. This profile of information will only be accessible to the users of the EFTS.

(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.

Access to the EFTS is voluntary. The data collected via the application form is required for the processing of the data.

The collected employee data which is stored electronically is the same mandatory data required for completion of the information. Where specific data elements on the application and other paperwork are identified to not be required or are listed only 'if applicable,' the individual has the option to not provide this specific information.

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

The system contains set fields that only collect information, which is sufficient to identify and track the course of each specific FOI/PA inquiry. Controls are in place that do not allow the system to derive new data or create data about an individual. The security and disciplinary provisions of the Privacy Act are applicable.

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?

The users manual, operation manual, and business rules and guidelines will ensure consistent use of the data in all sites.

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

The retention periods of data/records in the system are covered by General Records Schedules 14 and 20. Program Offices and officers also follow guidance on permanent and temporary records disposition issued by the National Archives Records Administration.

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

Procedures for eliminating the data at the end of the retention are established in accordance with GRS 14 and 20 or NARA guidance. Disposal of Privacy Act information will also be consistent with the procedures established in SOP 41 2. Eliminating the data at the end of

the retention period is part of the system development lifecycle (SDLC) and is the last stage of the SDLC.

(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?

There is no new use of technology that would affect privacy.

(6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No. In this release of the system, the firewall software will keep track of the IP addresses of those individuals accessing the system. In the next release, the system will generate a log which will show which individuals accessed the system and when.

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

There will be no monitoring of individuals.

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

The system is not used to monitor individuals. Policy prevents monitoring except under certain circumstances. The system is only accessible by those SBA employees who have been assigned user names and passwords.

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

SBA-71, Electronic FOIA Tracking System and FOIA Case Files;

SBA-69, FOIA Appeals; and

SBA-57, Privacy Act Files.

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

Not at this time.

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)

Users of the system will include: FOIA/PA officers and coordinators, system managers, attorneys and other employees of the FOIA/PA office who have a need to know and the information contained in this system in order to carry out their duties. The System Administrator will have access to the data in the system as necessary to carry out his/her responsibilities. In certain instances, the contractor performing work on the FOIA/PA office behalf may have access to records in the system. The routine use section of the Privacy Act system of records notice, SBA-71, identifies those parties that can gain access to the information when the use is compatible with that identified in the notice. Disclosure and access to information in the system is based on SBA FOIA and Privacy Act regulations at 43 CFR Part 2.

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

For the most part, access to the data by a user (i.e., SBA employees who are designated as FOIA/Privacy Act personnel and, as such, require access to the database to administer the laws) is determined by the “need-to-know” requirements of the Privacy Act, the user’s profile based on the users’ job requirements, managerial decisions, etc. and dependent on a compatible purpose for which the data was collected. The criteria, procedures, controls and responsibilities regarding access are documented in the business rules and guidelines and rules of behavior and comply with the intent of the Computer Security Act of 1987 [Public Law 100-235] for standards and guidelines on security and privacy (see F(4)).

(3) Will users have access to all data on the system or is the user’s access restricted? Explain.

Access to records in the system is limited to authorized personnel whose official duties require such access, i.e., on a “need to know” basis. Electronic data is protected through user identification, passwords, database permissions and software controls. Such security measures establish different access levels for different types of users. For example, in the EFTS, system administrators may have access to all of the data for their specific Program Office.

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

In accordance with OMB Circulars A-123, and A-130, Appendix III, the electronic FOIA tracking system will have controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions and software controls. All employees

including contractors must meet the requirements for protecting Privacy Act protected information. Business rules and guidelines as well as rules of behavior, and an access matrix have been established to prevent inadvertent disclosure to individuals not authorized to use the system or those who do not have a direct need to know certain information contained in the system. The system is designed to allow access in a pipeline format and also to provide levels of disclosure through a series of masks depending on the level of sensitivity. All users have a password and ID that is issued by the FOIA Officer. All users will receive training on the new electronic FOIA tracking system. In addition, the contractor has developed: 1) an operations manual to provide guidance to the technical support staff who will maintain the system; and 2) a user's manual to provide guidance to the FOIA personnel who will be regular users of the system.

(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 contracts, and other regulatory measures addressed?

Yes, contractors are involved with the design and development of the system and may be involved with the maintenance of the system. Contractors also may be involved in developing upgrades to the system. When a contract provides for the operation of a system of records the Privacy Act requirements and regulations on the Privacy Act must be applied to such a system (See the U.S. Small Business Administration Privacy Act regulations at 13-C.F.R-102: Government Contracts). The Federal Acquisition Regulations also require that certain information be included in contract language and certain processes must be in place. A Privacy Act clause was included as part of the statement of work and the contractor was provided with copies of the Privacy Act regulations and applicable policies.

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

No, the EFTS is a closed system.

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

There is no interface. All employees who have access to information in a Privacy Act system bear some responsibility for protecting personal information covered by the Privacy Act. The information owner and system manager (identified in the Privacy Act System Notice) share overall responsibility for protecting the privacy rights of individuals by developing guidelines and standards which must be followed.

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

Information from this system will only be shared with other agencies consistent with the FOIA/PA statutory exceptions and the routine uses set forth in the Privacy Act system of records notice, SBA-71, Electronic FOIA Tracking System and FOIA Case Files- Interior.

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

Access will only be provided to those parties identified in the routine use section of the Privacy Act system of records notice, SBA-71, for purposes consistent with the purpose for which the system was developed.

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

The FOIA/PA officers/coordinators and appropriate attorneys. All federal employees will be in compliance with the requirements in OMB Circulars A-123 and A-130 as well as the Privacy Act Office responsibilities.

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

The system operates on one site only and cannot identify, locate or monitor individuals. It does not use tracking technology to monitor individuals. The system cannot identify, locate or monitor individuals. It can retrieve information by name, however, only that information that is already in the system, and only by those who have been granted access to the system and then only specific to their role with SBA/FOIA.

Privacy Impact Assessment Approval Page

The Following Officials Have Approved this Document:

1) System Owner

_____ (Signature) _____ (Date)

Name:

Title:

2) Project Manager

_____ (Signature) _____ (Date)

Name:

Title:

3) IT Security Manager

_____ (Signature) _____ (Date)

Name:

Title:

4) Chief Privacy Officer

_____ (Signature) _____ (Date)

Name:

Title:

APPENDIX B

Privacy Threshold Analysis (PTA)

This form is used to verify if a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002. It is important to note that the use of some information will not require a PIA. This document is used as a tool in assisting system owners in thinking through the privacy risks associated with their system/applications.

The PTA will consist of several questions requesting a description of the system/application, and the type of data and mitigating controls used to protect that data.

Please complete this form and send it to:

Information Privacy Office
Small Business Administration
409 Third Street, SW
4th Floor
Washington, D.C. 20416

Upon receipt, the Privacy Office will review this form and may request additional information. If a PIA is mandatory, you will be required to submit a completed PIA. A copy of the SBA Privacy Impact Assessment Guide and Template is also available on the SBA Privacy website, <http://www.sba.gov/aboutsba/sbaprograms/OCIO/pia/index.html>

Privacy Threshold Analysis

System/Application Name: _____

Program Manager: _____

PTA QUESTIONS

1. Provide a description of the system/application and its purpose: (Please provide a general description of the system/application and its purpose.)

2. Status of Project:

1. Is this a new development effort? (Yes/No)
2. Is this an existing project? (Yes/No)
3. When did the system begin operation? (Date of Operation)
4. Has the system undergone major changes since its last Accreditation? (Yes/No) If Yes, provide a brief explanation.
5. Does a system or record notice exist for the information system?

3. If this project is a technology/system, does it relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?]

1. No. Please continue to the next question.
2. Yes. Is there a log kept of communication traffic?
 - No. (Continue to the next question)
 - Yes. What type of data is recorded in the log?

4. Does the system collect, maintain, and or share information that can be used to directly or indirectly identify an individual?

1. No. Please skip ahead to question 5.
2. Yes. (Discuss how the data within the system could be identifiable to an individual.)

5. Do you use or collect Social Security Numbers (SSNs)? (This includes truncated SSNs)

1. No.
2. Yes. Why does the program collect SSNs? <Please provide the function of the SSN and the legal authority to collect it. >

6. What information about individuals could be collected, generated or retained? <Please provide a specific description of information that might be collected, generated or retained such as names, addresses, emails, etc. >

7. Is there a Certification & Accreditation record within the OCIO FISMA tracking system?

1. Unknown
2. No.
3. Yes. Please indicate the determinations for each of the following:

Confidentiality:	<input type="checkbox"/> Low	<input type="checkbox"/> Moderate	<input type="checkbox"/> High	<input type="checkbox"/> Undefined
Integrity:	<input type="checkbox"/> Low	<input type="checkbox"/> Moderate	<input type="checkbox"/> High	<input type="checkbox"/> Undefined
Availability:	<input type="checkbox"/> Low	<input type="checkbox"/> Moderate	<input type="checkbox"/> High	<input type="checkbox"/> Undefined

SBA INFORMATION PRIVACY OFFICE

SBA Privacy Office review date: _____

Name of the SBA Privacy Office Reviewer: <Please enter name of reviewer. >

DESIGNATION:

1. This is NOT a Privacy Sensitive System – the system contains no Personally Identifiable Information.
2. This is a Privacy Sensitive System
 - a. PTA sufficient at this time
 - b. A PIA is required
 - c. Legacy System

COMMENTS: _____

APPENDIX C

The US SBA PII Survey

1. Do you handle personally identifiable information within your office? (Yes or No)
2. Does your office have a system/application which utilizes personally identifiable information? (Yes or No)
3. Has a Privacy Impact Assessment been developed on your information system? (Yes or No)
4. What type of Personal Information is requested, collected, used, generated, retained, etc within your area?
 - No Personal Information
 - Name
 - Address
 - Telephone Number
 - Social Security Number
 - Financial Account Information
 - Date of Birth
 - Email
 - Other
5. Does your office share PII with an external Agency? If “Yes,” indicate how data is transmitted i.e., “Electronically” or “Manually” in Comment box below. (Yes or No)
6. Is PII data shared with a third party? If “yes,” please explain the process used in comment box below. (Yes or No)
7. Do you utilize “Separation of Duties” in your system/application which contains PII data? If “No” explain why not in the Comment Box. (Yes or No)
8. Is PII data stored off-site? If “Yes,” please explain how the data is protected. (Yes or No)
9. When sending emails or faxing documents with PII do you properly mark the document to alert the reader of the need to protect the data? (Yes or No)
10. In your Program Office are procedures in place to prevent the casual viewing of PII data on monitors by persons without a need-to-know? (Yes or No)
11. Is the storage of PII data allowed on personal media or storage devices? (Yes or No)

12. Is removable portable storage devices containing PII data (e.g. laptops, hard drives, thumb drives, CD's DVD's) encrypted before being removed from the work place? (Yes or No)
13. When disposing of documents and media containing PII do you discard it into a recycling bin without shredding it because you think the recycler will shred it? (Yes or No)
14. Do you utilize a locked file cabinet to store documents containing PII data within your office or work area? (Yes or No)
15. Has your Program Office had any data breaches within the past year? (Yes or No) If yes, was the individual whose information was disclosed contacted? Please explain the information in the Comment Box.
16. If you were associated with a PII Data Breach who would you contact? Select the best answer or answers:
 - Immediate Supervisor
 - Department Head
 - Chief Information Security Officer
 - All of the above