SBA PRIVACY IMPACT ASSESSMENT
For
FOIA

Freedom of Information/Privacy Acts Office & Office of the Chief Information Officer
Small Business Administration
409 3rd Street, S.W.
Washington, DC 20416

TABLE OF CONTENTS

SECTION I
INTRODUCTION AND OVERVIEW

Introduction	The Small Business Administration recognizes the importance of protecting the privacy of clients, partners, and employees, especially as it modernizes its electronic systems. Privacy issues must be addressed when systems are being developed, and privacy protections must be integrated into the development life cycle of these automated systems. The vehicle for addressing privacy issues in a system under development is the Privacy Impact Assessment (PIA). The PIA process also provides a means to assure compliance with applicable laws and regulations governing client and employee privacy.
Purpose	The purpose of this document is to: • Establish the requirements for addressing privacy during the systems development process; • Describe the steps required to complete a PIA on a project; • Define the privacy issues a project must address when completing a PIA.
Background	The Small Business Administration is responsible for ensuring the privacy, confidentiality, integrity, and availability of client and employee information. The SBA recognizes that privacy protection is both a personal and fundamental right of all clients, partners, and employees. Among the most basic of clients, partners, and employees' rights is an expectation that the SBA will protect the confidentiality of personal, financial, and employment information. Clients, partners, and employees also have the right to expect that the SBA will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out agency responsibilities. Client and employee information is protected by the following: • Privacy Act of 1974, as Amended (5 USC 552a) which affords individuals the right to privacy in records that are maintained and used by Federal agencies. Note that 5 USC 552a includes the Computer Matching and Privacy Act of 1988 (Public Law 100-503); • Computer Security Act of 1987 (Public Law 100-235) which establishes minimum security practices for Federal computer systems; • 13 CFR 102.20 Privacy Act Regulations;

	• OMB Circular A-130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems; • OMB Circular A-11, Part 7: Planning, Budgeting, Acquisition and Management of Capital Assets, which prescribes how security and privacy safeguards should be treated in agencies' capital lans for major information technology projects. (Circular A-11 is re-issued annually) • Freedom of Information Act, as Amended (5 USC 552) which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.
The Freedom of Information/ Privacy Acts Office	The Freedom of Information/Privacy Acts Office is the SBA organization responsible for managing SBA's appellate function, as well as developing the Agency's policy and procedures regarding the FOI/PA. Besides the FOIA duties, the Office is responsible for: ensuring that the Agency adheres to requirements of the PA and maintains administrative control of SBA activities implementing the act; decides all administrative PA appeals; educates SBA components about their PA responsibilities, and advises Agency personnel, clients of the Agency and the general public regarding all aspects of the Act; prepares the Biennial Privacy Act Report to OMB.

SECTION II
PRIVACY IMPACT ASSESSMENT

Privacy and Systems Develoment	Rapid advances in computer technology make it possible to store and retrieve vast amounts of data of all kinds quickly and efficiently. This has raised concerns about the impact of large computerized information systems on the privacy of data subjects. Public concerns about highly integrated information systems operated by the government make it imperative to commit to a positive and aggressive approach to protecting individual privacy. The FOI/PA Office and OCIO have instituted the Privacy Impact Assessment in order to ensure that the systems the SBA develops protect individuals' privacy. The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design.
What is a Privacy	The Privacy Impact Assessment is a process used to evaluate privacy in information systems. The process is designed to guide system owners and

Impact Assessment?	developers in assessing privacy through the early stages of development. The process consists of privacy training, gathering data on privacy issues from the project, identifying and resolving any privacy risks, and approval by the Senior PA Officer. The PIA process is described in detail in Section III, Completing a Privacy Impact Assessment.
When is a PIA done?	The PIA is to be initiated in the early stages of the development of a system and completed as part of required system life cycle (SLC) reviews. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in the SBA.
Who completes the PIA?	Both the system owner and system developers must work together to complete the PIA. System owners must address what data is to be used, how the data is to be used, and who will use the data. The system developers must address whether the implementation of the owner's requirements presents any threats to privacy.
What systems have to complete a PIA?	New systems, systems under development, or systems undergoing major modifications are required to complete a PIA. The Senior PA Officer does reserve the right to request that a PIA be completed on any system that may have privacy risks. More specifically: • New systems and systems under development or undergoing major modifications are required to complete a PIA. • Legacy systems, as they exist today, do not have to complete a PIA. However, if the automation or upgrading of these systems puts the data at risk, a PIA may be requested by the Senior PA Officer. • Currently operational systems are not required to complete a PIA. However, if privacy is a concern for a system the Senior PA Officer can request that a PIA be completed. If a potential problem is identified concerning a currently operational system, the SBA will use best, or all reasonable, efforts to remedy the problem.

SECTION III
COMPLETING A PRIVACY IMPACT ASSESSMENT

The PIA	This section describes the steps that are required to complete a PIA. These steps are summarized in Table 1, Outline of Steps for Completing a PIA.
Training	Training on the PIA will be available, upon request. The training describes the PIA process and provides detail about the privacy issues and privacy questions to be answered to complete the PIA. The intended audience is the personnel responsible for writing the PIA document. PIA training is available to government and contractor personnel.
The PIA Document	Preparing the PIA document requires the system owner and developer to answer the privacy questions in Section V. A brief explanation should be written for each question. Issues that do not apply to a system should be noted as Not Applicable. During the development of the PIA document, the FOI/PA Office will be available to answer questions related to the PIA process and other concerns that may arise with respect to privacy.
Review of the PIA Document	The completed PIA document is to be submitted to the FOI/PA Office for review. The purpose of the review is to identify privacy risks in the system. The FOI/PA Office will work with the system owner and system developer to develop design requirements to resolve the identified risks. If there are risks in a system that cannot be resolved with the FOI/PA Office, the risks will be presented to the CIO for resolution.
Approval of the PIA	The SLC review process will be used to validate the incorporation of the design requirements to resolve the privacy risks. Formal approval will be issued in accordance with the SLC.

Table 1
Outline of Steps for Completing a PIA

Step	Who	Procedure
1	System Owner, and Developer	Request and complete Privacy Impact Assessment (PIA) Training.
2	System Owner, and Developer	Answer the questions in Section V Privacy Questions
3	System Owner, and Developer	Submit the PIA document to the FOI/PA Office
4	FOI/PA Office	Review the PIA document to identify privacy risks from the information provided. The FOI/PA Office will get clarification from the owner and developer as needed.
5	System Owner, Developer, FOI/PA Office, and OCIO	The System Owner, Developer and the FOI/PA Office should reach agreement on design requirements to resolve all identified risks. If an agreement cannot be reached then issues will be raised to the CIO for resolution.
6	System Owner, and Developer	The System Owner and Developer will incorporate the agreed upon design requirements and resolve the identified risks.
7	System Owner, Developer, and FOI/PA Office	Participate in the SLC required reviews to ensure satisfactory resolution of identified privacy risks and obtain formal approval.

SECTION IV
PRIVACY ISSUES IN INFORMATION SYSTEMS

Privacy Act of 1974 5 U.S.C. 552a As Amended	The Privacy Act of 1974 5 U.S.C. 552a As Amended requires Federal Agencies to protect personally identifiable information. It states specifically: "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;" • "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individuals rights, benefits, and privileges under Federal programs;" • "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;" • "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."
Definitions:	***Accuracy*** - within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination. ***Completeness*** - all elements necessary for making a determination are present before such determination is made. ***Determination*** **-** any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency. ***Necessary*** - a threshold of need for an element of information greater than mere relevance and utility. ***Record*** **-** any item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency. ***Relevance*** - limitation to only those elements of information which clearly bear on the determination(s) for which the records are intended. ***Routine Use*** - with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected. ***System of Records*** - a group of any records under the control of any agency from which information is retrieved by the name of the individual

	or by some identifying number, symbol, or other identifying particular assigned to the individual.
Information and Privacy	To fulfill the commitment of the SBA to protect personal data several issues must be addressed with respect to privacy. • The use of information must be controlled. • Information may be used only for a necessary and lawful purpose. • Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them. • Information collected for a particular purpose should not be used for another purpose without the data subjects consent unless such other uses are specifically authorized or mandated by law. • Any information used must be sufficiently accurate, relevant, timely and complete to assure fair treatment of the individual. Given the availability of vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the SBA, to share that information. With the potential expanded uses of data in automated systems it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses. These procedures do not in themselves create any legal rights, but are intended to express the full and sincere commitment of the SBA to the laws which protect client and employee privacy rights and which provide redress for violations of those rights.
Data in the System	The sources of the information in the system are an important privacy consideration if the data is gathered from other than SBA records. Information collected from non-SBA sources should be verified, to the extent practicable, for accuracy, that the information is current, and the information is complete. This is especially important if the information will be used to make determinations about individuals.
Access to the Data	Who has access to the data in a system must be defined and documented. Users of the data can be individuals, other systems, and other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers. When

	individuals are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties. If individuals are granted access to all of the data in a system, procedures need to be in place to deter and detect browsing and unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data. Other agencies can be International, Federal, state, or local entities that have access to SBA data.
Attributes of the Data	When requirements for the data to be used in the system are being determined, those requirements must include the privacy attributes of the data. The privacy attributes are derived from the legal requirements imposed by the Privacy Act of 1974. First, the data must be *relevant* and *necessary* to accomplish the purpose of the system. Second, the data must be *complete, accurate* and *timely*. It is important to ensure the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.
Maintenance of Administrative Controls	Automation of systems can lead to the consolidation of processes, data, and the controls in place to protect the data. When administrative controls are consolidated, they should be evaluated so that all necessary controls remain in place to the degree necessary to continue to control access to and use of the data. Data retention procedures should be documented. Data retention procedures require review to ensure they meet statutory and/or IRM requirements. Precise rules must be established for the length of time information is kept and for assuring that it is properly eliminated at the end of that time. The intended and potential monitoring capabilities of a system must be defined and safeguards must be installed to ensure the privacy of clients and partners and prevent unnecessary intrusion. The use of monitoring capabilities should be limited, at a minimum, to some judicially ascertainable standard of reasonableness in light of the statutory mission of the SBA and other authorized governmental users of the system.

SECTION V
PRIVACY QUESTIONS

Data in the System

1. Generally describe the information to be used in the system in each of the following categories: Citizen, Client/Partner, Employee, Other.

   Citizen's name, address, phone number, e-mail address; employee user id, office code and name.

2. What are the sources of the information in the system?

   Incoming correspondence from individuals submitting FOI/PA actions.

   a. What SBA files and databases are used?

      Sybase database,, Client database, Personnel database, program application files.

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

      N/A

   c. What State and Local Agencies are providing data for use in the system?

      N/A

   d. What other third party sources will data be collected from?

      N/A

   e. What information will be collected from the client/partner/employee?

      N/A

3. a. How will data collected from sources other than SBA records and the partner or client be verified for accuracy?

      N/A

   b. How will data be checked for completeness?

      N/A

   c. Is the data current? How do you know?

      N/A

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

FOIA system ERWIN data models.

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

SBA users and developers.

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

FOIA security roles/responsibilities, controls and procedures.

3. Will users have access to all data on the system or will the users' access be restricted? *No.*

Explain.

User access is based on the system security roles and responsibilities and the Privacy Act.

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

Security roles and the Privacy Act.

5. a. Do other systems share data or have access to data in this system? If yes, explain.

No

b. Who will be responsible for protecting the privacy rights of the citizens, partners, clients, and employees affected by the interface?

N/A

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

No

b. How will the data be used by the Agency?

N/A

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

N/A

d. How will the system ensure that agencies only get the information they are entitled to under 13 CFR 102.20?

N/A

Attributes of the Data

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

Yes

2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No

b. Will the new data be placed in the individual's record (citizen, client, partner, or employee)?

N/A

c. Can the system make determinations about citizens, clients, partners, or employees that would not be possible without the new data?

N/A

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

N/A

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

N/A

b. If processes are being consolidated, will the proper controls remain to protect the data and prevent unauthorized access? Explain.

N/A

4. a. How will the data be retrieved? Can it be retrieved by personal identifier? Explain.

By last name and/or case number. *Retrieved by last name.*

b. What are the potential effects on the due process rights of citizens, clients, partners, and employees of:

- consolidation and linkage of files and systems; *N/A*
- derivation of data; *N/A*
- accelerated information processing and decision making; *N/A*
- use of new technologies. *N/A*

How are those effects to be mitigated? *N/A*

Maintenance of Administrative Controls

1. a. Explain how the system and its use will ensure equitable treatment of citizens, clients, partners, and employees.

N/A

b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

One site only.

c. Explain any possibility of disparate treatment of individuals or groups.

N/A

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

National Archives Records Administration Retention Schedules

b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

SBA Privacy Act System of Records 160, Freedom of Information and Privacy Act Case Files and NARA GRS 14 and 21.

c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

N/A

3. a. Is the system using technologies in ways that the SBA has not previously employed (e.g., Caller-ID)?

No

b. How does the use of this technology affect citizen/client/partner/employee privacy?

N/A

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

Yes, the system displays the program office employees' user id and name.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

No

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

Access and use are limited to specified individuals and will require a user id.

5. a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.

Freedom of Information Act and Privacy Act Case Files – SBA 160.

b. If the system is being modified, will the SOR require amendment or revision?

No

Explain.

Storage specifications for SOR 160 include "computer data files."

APPENDIX A
DECLARATION OF PRIVACY PRINCIPLES

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

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

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

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

Principle 7:	Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the SBA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing, or any unauthorized access of citizen, client or partner information by any SBA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.
Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.

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

APPENDIX B
POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

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

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

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

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