Privacy Impact Assessment
Business Gateway

An E-Gov Initiative under the Management of the Small Business Administration

Version 1.0 September 5, 2003

Unique Project Identifier: 02800020004001024202072

Business Gateway Initiative & Office of the Chief Information Officer
Small Business Administration
409 3rd Street, S.W.
Washington, DC 20416

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the Business Gateway. This document has been completed in accordance with the requirements of the SBA System Development Methodology.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____ _____
E-Government Program Manager/Project Manager DATE
Sandra Gibbs

_____ _____
Program Area/Sponsor Representative DATE
Stephen Galvan

_____ _____
Privacy Officer DATE
Lisa J. Babcock

TABLE OF CONTENTS

1.0 INTRODUCTION AND OVERVIEW

1.1 Background

The Small Business Administration is the managing partner of the Business Gateway initiative with the General Services Administration as a major partner responsible for creating and operating the E-Forms Gateway. The initiative has three major parts all of which may impact on information security and privacy:

1. Creating a cross-agency portal for businesses by integrating content in SBA.gov, Business.gov, BusinessLaw.gov and FirstGov.gov.
2. Creating the E-Forms gateway that will serve as the access portal for all Federal, transactional forms for citizens and businesses.
3. Working with regulators, industry, and other Federal cross-agency business reengineering initiatives, to reduce amount of duplication and overlap in the data collection process through data, forms, and process harmonization.

The SBA recognizes that privacy protection is both a personal and fundamental right of all users of the Business Gateway applications. Among the most basic of rights of citizens and businesses is an expectation that the SBA will protect the confidentiality of personal identifiable information. Client user 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 prescribe how security and privacy safeguards should be, treated in agencies' capital plans 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.

1.2 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.

1.3 Privacy Impact Assessment

The Privacy Impact Assessment is a process used to evaluate privacy in information systems. The process is designed to guide system owners and 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.

2.0 PRIVACY ISSUES IN INFORMATION SYSTEMS

2.1 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."

2.2 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

2.3 Information and Privacy

To fulfill the commitment of the SBA as managing partner of the Business Gateway initiative 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 user privacy rights and which provide redress for violations of those rights.

2.4 Data in the System

Portal
The portal will provide access to expert tools that may require personal information. The user will have the option to use the tool or not. No data is kept of the transaction after use of the expert tool has been terminated. In many cases the user will have the option of downloading the tool and using it on his/her own computer.

E-Forms Gateway
This Gateway will handle access to all transactional forms in the Federal government, approximately 4000 forms. The goal of the gateway for 2003 and 2004 is to achieve the Federal GPEA goal, i.e. that Federal transactional forms are electronically fill-able, file-able, and permit electronic signatures. This is an example of a paper transaction becoming electronic and thereby covered by the PIA act. However, no new information will be collected or forms changed. The information requests are still handled by the Federal agency owning the process and data base. All that is supplied is a link to an agency hosted form, or a link to an agency form hosted at a Federal agency service provider where after it has been filled in it is sent securely to the agency that owns the process and the form. The E-forms Gateway is simply a conduit for hosted form data from user to Federal agency.

Data Harmonization
This part of the initiative seeks to reduce the amount of duplication and overlap in data collection using three perspectives: the regulatory agency, industry and process. Changes will be proposed and consequences for data elements and forms will be processed through ICR, GPEA, and PIA procedures.

2.5 Access to the Data

The E-Forms Gateway will initially provide links to agency hosted forms or to forms hosted by a Federal agency hosting provider. In either case, ICRs and PIA statements will have to be provided by the agency owning the forms. In later phases, agency form systems will be migrating to a formless environment where the E-Form Gateway will provide users with presentation formats, based on XML schemas and business rules, to be at the Gateway portal and then streamed as XML packets to the appropriate owner agency of the data.

The E-Forms Gateway will become a collector and conduit for the data supplied by the user, but will not use the data or store it. Questions of privacy and security need to be addressed with respect to this conduit function to ensure that there are no leakages or access to the data in transit.

As the collected data will be in transit, the XML schema must clearly indicate to which agency the data must be routed, and there must be procedures are in place to ensure that only the proper recipient receives the data.

2.6 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.

2.7 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

3.0 PRIVACY ASSESSMENT

The Business Gateway/E-Forms initiative will become a gateway for all 4400 GPEA transaction forms transmitting data to the agency responsible for the ICR as well as the use of the data. The Gateway will not process personal information in any other sense than to check the e-authentication credentials, validate the data against business rules and transmit the data to the authorized recipient.

3.1 Data in the System

1. Generally describe the information to be used in the system in each of the following categories: Citizen, business.

Citizen's name, address, phone number, SSN, e-mail address;
Business name, address, phone number, EIN, owners,

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

Data submitted in the process of filling in one of the 4000 Federal transactional forms.

a. What SBA files and databases are used?

None

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

None. Users (i.e. citizens and businesses) will provide data, as they do now, using the Gateway. Federal agencies will be providing the gateway with XML schemas and business rules but no data.

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 citizens and businesses?

Information to be collected consists of those data elements in forms approved through the ICR and PIA processes.

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?

As we are solely dealing with automating the processing of data for existing and approved Federal forms, data elements will be described in existing ICRs.

Access to the Data

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

N/A

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

Access is determined by security roles/responsibilities, controls and procedures and documented in the System Security Plan.

3. Will users have access to all data on the system or will the users' access be restricted?

N/A.

Explain.

The Gateway is a conduit to the Federal agency which is the user. The Gateway is not a user.

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?

GSA with respect to the conduit function of the Gateway, en user Federal agencies as to the use of the data as is now the case.

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

No. In the case where business reengineering of data collection processes leads to consolidation of forms and processes, agencies owning the data and the processes will have to submit revised ICRs and PIAs.

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

N/A

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

GSA and Federal agencies

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

Through business rules governing how data is transmitted from the Gateway to the appropriate Federal agency and through security procedures and systems.

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 E-forms Gateway is built to collect data elements and validate the data against predetermined business rules. It does not use data.

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 or businesses 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?

To the extent that data, form, or process consolidation occurs, the change will have to be part of an ICR and PIA process.

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

Yes.

4. a. How will the data be retrieved? *By last name, text and/or case number.*

N/A

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 and businesses.

In automating the Federal forms systems through the use of the E-Forms Gateway, there will still remain the possibility of manual submission of forms in paper format.

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?

N/A.

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?

N/A

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

N/A

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/business privacy?

N/A

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

N/A

.

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

N/A

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

N/A

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

As the data is "owned" by the various agencies that have submitted ICR forms, these agencies also are the keepers of the SORs. The Business Gateway Initiative will not maintain nor retrieve data using personal identifiers.

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

Yes.

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.

The obligation to protect user privacy and to safeguard the information users entrust to us is a fundamental part of the SBA's mission to administer the law fairly and efficiently. Users 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

To promote and maintain users' confidence in the privacy, confidentiality and security protections provided by the Business Gateway and E-forms Gateway, the SBA will be guided by the following Privacy Principles:

Principle 1:	Protecting citizen, client and partner privacy and safeguarding confidential citizen and business information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens or businesses that are not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Personally identifiable citizen or business information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
Principle 4:	Personally identifiable citizen or business information will be disposed of at the end of the transaction and transmission of the data to the Federal agency recipient.
Principle 5:	Citizen or business 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 6:	The privacy rights of citizens and businesses 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.