PRIVACY IMPACT ASSESSMENT

Name of System/Application: Standard 7(a) Loan Guaranty Processing System

Program Office: Office of Capital Access

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

A. CONTACT INFORMATION

1) Who is the person completing this document?

Jeffrey Browning,
IT Specialist
Standard 7(a) Loan Guaranty Processing Center
606-436-0801 X233
Jeffrey.Browning@SBA.GOV

2) Who is the system owner?

Frank Pucci
Center Director
Standard 7(a) Loan Guaranty Processing Center
916-735-1969
Robert.Pucci@SBA.GOV

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

Jeffrey Browning,
IT Specialist
Standard 7(a) Loan Guaranty Processing Center
606-436-0801 X233
Jeffrey.Browning@SBA.GOV

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

Ja'Nelle DeVore,
Chief Information Security Officer
Office of the Chief Information Officer
202-205-7103
Janelle.Devore@SBA.GOV

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

Ethel Matthews,
Senior Privacy Advisor
Office of the Chief Information Officer
202-205-7173
Ethel.Matthews@SBA.GOV

4) Who is the Reviewing Official?

Paul Christy,
Chief Privacy Officer
Office of the Chief Information Officer
202-205-6756
Paul.Christy@SBA.GOV

B. SYSTEM APPLICATION/GENERAL INFORMATION

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

Yes.
The system collects the following information on the loan applicant:

- Name (Last, First, Middle Initial and Suffix)
- Social Security Number (SSN)
- Address (Street, City, State and Zip)

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

b. Is the information about employees?
No

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

The Standard 7(a) LGPS was developed to meet the Standard 7(a) loan guaranty processing requirements. Data is generated from Standard 7(a) loan guaranty applications received from financial institutions. In addition to tracking Standard 7(a) loan application information, credit scoring information is generated from the information.

3) Is the system in the development process? No

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

The technology investment does not impact existing privacy practices.

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

Government Paperwork Elimination Act(GPEA), Pub. L. No. 105-277, 1701-1710(1998) (codified as 44 U.S.C.A. 3504 n. (West Supp. 1999)).

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

To ensure employees do not view PII data not required in the performance of their job duties, user accounts will be assigned specific roles and responsibilities. Internal system controls will be used to limit users' access to areas of the system appropriate for those roles and responsibilities.
The Standard 7(a) Loan Guaranty Processing System (LGPS) utilizes a manual approach to create user accounts.
Administrators assign user roles and permissions based on a 'need to know' basis.

C. SYSTEM DATA

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

Information will be acquired and retained on Standard 7(a) Loan Applicants.

The following are the categories of users:

General Center Users - Standard 7(a) LGPS Clerk Users - Performs general data processing functions in support of Standard 7(a) LGPS customers, its mission and goals.

General Center Loan Officer Users - Standard 7(a) LGPS Loan Officer Users - Performs general processing functions related to loan application review.

General Center Team Leader Users - Standard 7(a) LGPS Team Leader Users - Performs general processing functions related to loan application review of loan officer analysis and recommendations.

General Center Admin Users - Standard 7(a) LGPS Admin Users – Perform general admin duties for the Standard 7(a) LGPS.

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 the system is derived from the individuals applying for a Standard 7(a) Loan Guaranty.

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?

Credit Scoring information is obtained from FairIsaac Corporation.

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

The system captures the SBA domain user login ID of the employee during the execution of the system for user role privileges but does not write this information to any media, this data is retained in memory until the executable terminates.

The system will collect the following information on the loan applicant:

- Name (Last, First, Middle Initial and Suffix)
- Social Security Number (SSN)
- Address (Street, City, State and Zip)

3) Accuracy, Timeliness, and Reliability

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

Current 7(a) Loan Guaranty Application information is verified by a SBA loan staff, they contact the lender to obtain missing information or to verify questionable information. The lender is notified by email, phone or by fax.

Also, the Standard 7(a) LGPS uses electronic forms that provide

format validation capabilities during data entry. In addition, there will be quality checks performed throughout the life cycle to identify stale or inconsistent information.

b. How is data checked for completeness?

Both visual verification and internal software controls. Once an application is received, the data is inputted by clerks and assigned a control number. Then a loan officer pulls up the data by referencing the control number. They review the data for any missing or questionable data. There are select fields that will produce an error if the information provided does not meet specific criteria by the internal software controls.

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).

Applicant Information is verified by the lender and SBA employee review and verification; if data is not current a SBA employee makes necessary contacts to obtain current information.

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

Yes, Etrans Data Model was used in the standardization of data elements.

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

The systems collects some PII information and not everyone needs to have access to the information, only LGPC staff that needs access to the EIN or SSN information will be able to view the data. Only authorized LGPC staff will have permissions to query and view PII Information through control of access privileges within the system. The system executes within the SBA domain and inherits all SBA domain implemented policies, procedures and controls.

D. DATA ATTRIBUTES

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

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?**

Credit score information will be obtained from FairIsaac website (https://www.liquidcredit.com/DecisionEngine/LiquidCredit.asp) and stored electronically in the SBA Domain Member Microsoft SQL Server DBMS and an electronic copy of the credit information will reside on the SBA Domain Member File Server.

3) **Will the new data be placed in the individual's record?** Yes, the credit score information will be collected and maintained on the applicant's SQL Server DBMS Record.

4) **Can the system make determinations about employees or members of the public that would not be possible without the new data?** No. Credit Information is a critical process in Loan Processing.

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

The credit information is obtained through major credit bureaus and includes personal information that results in a positive match with our records.

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

The data is being consolidated in the Standard 7(a) LGPS, and is maintained on a Sequential Query Language (SQL) server and file servers. These servers reside on the the SBA domain and is protected by the SBA firewall and have internal auditing settings and user permissions configured to identify users and to prevent unauthorized access. The individual servers also have an active configured firewall in place to prevent unauthorized access from outside the local subnet. All servers are in compliance with SBA directives as updates and configuration follows OCIO's guidance.

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".**

Yes, the Standard 7(a) LGPS functions within the SBA domain and is protected by the SBA Firewall; it uses a HTTPS Connection with VeriSign Digital Certification Authentication for communication with FairIsaac. Each server has auditing and user permissions configured and has implemented a local firewall to prevent unauthorized internal traffic. All servers are in compliance with SBA directives as updates and configuration follows OCIO's guidance.

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.** No, once an application is received it is given a unique identifier or control number for the application and it is automatically generated by the DBMS and is not part of the applicant's personal information.

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 can produce reports for the LGPC staff only, reports are those necessary for loan guaranty decision making. Another report is statistical information in nature and given to HQ, i.e. the number of S/RLA loans processed in a specific week. Typically, the reports are not printed out, but if printer they are maintained according to SBA records management.

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.**

These options would be through the 7(a) Loan Guaranty Application, either on the SBA Form 4 or the SBA Form 2301.

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

The system has authentication controls and role-based access controls. Auditing is used to track user activity in the system. A process exists for both user provisioning and cancellation of accounts in a timely fashion. Additionally, users of all SBA systems must certify themselves on a yearly basis by completing SBA Security Awareness Training. Users will have to read and sign a rules of behavior document. Since the system is hosted by the SBA Domain, SBA will pre-determine roles for users which will mean specific access will be made available for users depending on their job function at the SBA.

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 information is used within the LGPC site only.

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

Due to the possibility of litigation against the SBA, legal has mandated all data records be kept indefinitely. In case of possible lawsuits that may arise from a lender or applicant.

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? The hardcopies of the data is disposed by shredding. The reports will be kept typically no longer than six months by hardcopies and indefinitely by electronic storage for legality reasons and the life of a loan. The procedures are documented in SOP 50-10(5)C.**

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?** The information on applications is sensitive in nature and should be protected from unauthorized access.

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.** No. The system has the capability to only retrieve and store applicant information.

7) **What kinds of information are collected as a function of the monitoring of individuals?** No individual monitoring occurs with the system.

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

   The system functions within the SBA Firewall and is hosted by the SBA Domain inheriting all SBA Domain controls. In addition, the system uses internal software controls to identify users and prevent unauthorized access.

9) **Under which Privacy Act systems of records notice (SORN) does the system operate? Provide number and name.** SBA Privacy Act System of Records – SBA 21.

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

F. DATA ACCESS

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

LGPC staff is the only users of the system, based on need to know login access. The LGPC staff consists of loan specialists, managers, automation assistants, contractors, attorneys, and center IT specialists.

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

   The user is verified by internal software controls and assigned security levels based on userid.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.** Users will be restricted based on the assigned security role for each user.

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**)

LGPC staff has access to all Standard 7(a) Loan Information. Information could potentially be deleted by a number of staff members, however we have system audit trails and any change to anything in the system is date stamped to the second and identifies the user who made the change. The system also enforces separation of responsibilities to only allow access to data/functionality necessary to perform job functions.

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?** No

6) **Do other systems share data or have access to the data in the system? If yes, explain.** No

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?** The LGPC Information Resource Staff.

8) **Will other agencies share data or have access to the data in this system via transferred or transmitted (Federal, State, and Local, Other (e.g., Tribal))?** No

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

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

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

PII information has been collected and stored in the system SQL Server DBMS. This SBA Domain Member Server is an isolated server with controlled access and protected by SBA Domain Policies, Controls and Procedures. The system may also use extracts and lockboxes. Only required data will be exchanged. Electronic data will be transferred using a secure interface including, VPN, secure lease line, file encryption, secure shell, digital certificate authentication and SSL. The information that is sent by the aforementioned interfaces can include the Business name, it's EIN, it's address, the principal's name, their SSN, and address.

A user's access role will be based on the responsibility assigned to the user. Therefore, users' access will be restricted by responsibility. The pre-determined responsibilities, as described in the question above, assign different system modules that a user can create and the type of data/functionality that user possesses.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) **System Owner**

_____ (Signature) 6/14/11 (Date)

Name: Robert Pucci

Title: Center Director

2) **Project Manager**

_____ (Signature) 6/13/2011 (Date)

Name: Jeffrey Browning

Title: Center IT Specialist

3) **IT Security Manager**

_____ (Signature) 7/14/2011 (Date)

for Jo'Nelle DuBois

Name:

Title:

4) **Chief Privacy Officer**

_____ (Signature) 7/19/2011 (Date)

Name:

Title: