PRIVACY IMPACT ASSESSMENT

Name of System/Application: Surety Bond Guarantee/Preferred Surety Bond
Program Office: Office of Capital Access (OCA)

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?**

   Steve Kucharski
   Director of Systems, OCA
   202-205-7551
   Stepehen.kucharski@sba.gov

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

   Frank Lalumiere
   Associate Administrator for Surety Bond Program, OCA
   202-401-8275
   Frank.Lalumiere@sba.gov

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

   Frank Lalumiere
   Associate Administrator for Surety Bond Program, OCA
   202-401-8275
   Frank.Lalumiere@sba.gov

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

   Ja'Nelle DeVore, Chief Information Security Officer
   Office of the Chief Information Officer (OCIO)
   202-205-7103
   Janelle.Devore@sba.gov

5) **Who is the Senior Advisor who reviewed this document?**
   Ethel Mathews, Senior Advisor
   Office of the Chief Information Officer (OCIO)
   202-205-7173
   Ethel.Mathews@sba.gov

6) Who is the Reviewing Official?

Paul Christy, Chief Information Officer
Office of the Chief Information Officer (OCIO)
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, this system contains information that is collected online or by paper format. The information collected about individuals includes the borrower's full name, social security number, birth date, and address.

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

Yes, the information is about members of the public who apply for loans via SBA.

b. Is the information about employees?

No, the system does not collect information about employees.

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

The Surety Bond Guarantee/Preferred Surety Bond (SBG/PSB) system enables the Office of Surety Guarantees (OSG) to assist small contracting firms, which cannot obtain bid or contract surety bonds needed to perform work for which they are otherwise qualified. The SBG PSB system is comprised of a series of modules logically defined under an 'umbrella' that are used collectively and individually to enter bond applications as well as assist the underwriting staff in processing and approving bonds. The system maintains a record of such bonds and sureties.

The SBG/PSB system provides a method of tracking and controlling allotted program funds and tracking and generating claim payments through the Denver Finance Center, as well as a method of tracking, updating the bond records and general ledger for recoveries on claims paid, and tracking and posting fee collections. The actual Treasury payment files (Automated Clearing House (ACH) and checks) are produced by the Denver Finance Center using the output of the program as authorization and inputs to the Office of the Chief Financial Operations

(OCFO) central disbursing system. An accounting data file is produced by the SBG/PSB system and uploaded through the Denver Finance Center to the core accounting system.

3) Is the system in the development process?

The system is not in the development process.

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

The technology investment does not impact existing privacy processes.

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

The Small Business Act and Small Business Investment Act authorize the purchase/development of this system.

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

To mitigate disclosure of personally identifiable information, the Network Security (SSDD-System Security Display Designation) application controls user access to the SBG/PSB functionality and enables system security officers to manage user accounts and maintain user security profiles.

The following media protection controls are in place:

- o Access to the SBA Headquarters facility is controlled 24x7 by security guards and CCTV. All printers are in a secured area inside the facility that requires card access for entry. Only authorized personnel with special access can enter the data center where the media is stored.
- o Mainframe data tapes are transported to an offsite location by authorized personnel (known and designated by the contract between Unisys and the offsite storage company).
- o Offsite media is taken to a staging area, placed in secured tubs, and picked up by a vendor to be transported to offsite storage. Procedures are in place for the selection, transportation, archival, and retrieval of backup media
- o Before a tape is released from the SBA tape pool for reuse, the tape is degaussed and the tape library is audited monthly by a tape librarian. Tapes that are to be destroyed go to offsite vendors who perform certified destruction and provide SBA with a certificate of destruction.

- Media are sanitized prior to reuse and destroyed when no longer needed or operable. Sensitive printouts are either shredded or picked up by authorized contractor for destruction.

C. SYSTEM DATA

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

Applicants for SBA Surety Bond Guaranty are the only individuals that are tracked in this 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?

Data is only collected from surety partners/agents, Small Business Source System (SBSS) formerly known as the ProNet Database, and claims attorneys.

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

This system does not collect information from any other Federal agency.

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

This system does not collect information from any tribal, state, or local agency.

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

SBA does not collect data from third party sources.

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

There is no information collected from employees. SBA collects financial information, addresses, social security number, and name from individuals who apply for SBA surety bonds.

3) Accuracy, Timeliness, and Reliability

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

Data is only collected by agents and surety partners. The data is entered into SBG/PBS.

b. How is data checked for completeness?

The system is built with checks that determine if the data is complete.

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).

The database reflects information submitted or updated for bond guaranty on a daily basis. SBG/PSB is updated daily.

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

The SBG/PSB data elements are described in the SBG ERWIN data models.

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

Because the system collects some PII and not everyone has a need to know or access to the information, only those that have a need to know will be able to view the information. Also, users that need to query the database on SSN have permission do so. SBA uses access procedures and security roles to limit access to individuals information based on role in the organization.

D. DATA ATTRIBUTES

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

The collected data is used to manage SBA surety bond guarantees. SBA does not use the data for any other purpose.

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?**

   The system will not derive new data nor will it create previously unavailable data.

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

N/A

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

N/A

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

N/A

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

N/A

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".**

N/A

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

   Data can be retrieved by personal identifiers such as social security number and sole proprietor name.

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

   Reports can be produced on the records of individuals to respond to inquiries which comply with FOIA and Privacy Act requirements. Access is restricted to Program Officials with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines.

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.**

N/A-The surety partner/agent submits the information into the system and not the individual.

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

SBG/PBS users sign a rules of behavior document. In addition, SBA will predetermine roles for users in the system which means that data will be made available to a user depending on their job function at 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?**

SBG/PBS is not operated on multiple sites.

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

The retention periods are defined in SBA's Privacy Act Systems of Record, SBA 20 and SBA 21. In accordance with SBA Standard Operating Procedure 00 41 2, Item Nos. 50:04, 50:08, 50:09, 50:10, 50:11, 50:12, 50:13, 50:19, 50:22, 55:02, 70:09, 70:13, and appendices 17, 18, and 21.

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

SBA's disposition procedures are defined in SBA's Privacy Act Systems of Record, SBA 20 and SBA 21. In accordance with SBA Standard Operating Procedure 00 41 2, Item Nos. 50:04, 50:08, 50:09, 50:10, 50:11, 50:12, 50:13, 50:19, 50:22, 55:02, 70:09, 70:13, and appendices 17, 18, and 21.

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

SBG/PBS does not use technologies in a new way.

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

Use of the technology may result in confidential information being disclosed. To mitigate the risk of disclosing information, SBG/PBS access is restricted to Program Officials with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines.

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

No, the system cannot identify, locate, or monitor individuals.

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

SBA does not monitor individuals.

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

SBA has Personnel Security, Media Protection, and Technical Controls to prevent unauthorized monitoring. The controls are identified below.

- Personnel Security
  - The SBA has implemented a personnel security program in accordance with OMB Circular A-130.
  - SBA positions are classified in accordance with 5 CFR 731.106(a) and OPM policies and guidance.
  - All SBA users (SBA and contract employees) are subject to background investigations commensurate with the level of risk introduced by their access to the system and the sensitivity level of the position.
  - Contractors' access to the system and the facility is revoked immediately following termination. SBA personnel send out the list of separated employees to appropriate program offices to ensure proper removal of accounts biweekly.
  - System access user privilege listings are reviewed on a quarterly basis to ensure that access privileges are necessary to perform assigned duties. System administrators are notified of personnel changes.
  - A confidentiality agreement is signed when an individual submits data for a background investigation (SBA Form 1228).
  - SBA employees who violate established policies and rules of behavior are subject to disciplinary action that can be imposed under existing policies and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current

position, termination of employment, and/or criminal prosecution. The SBA will enforce security policy with the use of appropriate penalties against any user who willfully violates any SBA or federal system security polity. Likewise, the SBA will enforce security policy against any contractor who willfully violates SBA security policy, the SBA's rules of behavior, or federal system security policy. A contractor's access may be revoked and the contractor may be removed from the facility immediately. Contractors could also be subject to criminal prosecution.

- Technical Controls
  - SBA requires a unique USERID and a password for each account.
  - The SBA uses protocols to identify and authenticate devices over the network.
  - User IDs are only issued after a background investigation and positive identification of the user has been successfully completed. Access to the system is provided on a need-to-know, need-to-use basis.
  - VPN access over public communications is encrypted.
  - The SBA's Secure Baseline Configuration Standards provide detailed guidance for administrators in configuring access controls for the following major components in the SBA's architecture.
  - SBA policy requires the segregation of duties between major operating and programming activities, including duties performed by users, application programmers, and data center staff, is required.

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

The system operates under Small Business Administration Privacy Act System of Records, SBA 20 and 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)

   SBG/PSB data is accessed by contractors, users (partners), managers, system administrators, and developers who support the system.

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

   Access to data is determined by Agency Security Roles and Procedures/Controls. Access is limited by control assignment of a responsibility profile to all users. Each responsibility comes with a predetermined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user.

   The servicing centers have documented procedures and controls to ensure that employees have access to SBG/PBS to perform assigned duties.

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

   Access is limited by controlled assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the 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)**

   SBA has implemented security roles and procedures to prevent misuse of information. Access is limited by control assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user.

   System audit trails can be used to document suspicious or irregular log-ons and navigation of the system. Agency network long-on procedures mandate a posted Privacy notice be viewed and acknowledged prior to entry. SBA Privacy Act of System Records SBA 20 and SBA 21 define routine uses of this information and serve as control by defining acceptable uses. Access to sensitive financial information is limited to only those with a need to know.

Mandatory information security and privacy training is required by all employees to include contractors in accordance with agency policy.

Each contractor must sign a non-disclosure agreement. In addition, the privacy and security contract clauses are inserted in their contracts to address regulatory measures addressed.

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

Yes, the SBG/PSB does share data with other systems. The systems include:

- JAAMS for loan accounting information
- PIMS for partner information

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

The SBG/PSB System Administrator and System Manager are responsible for protecting the privacy rights of the public affected by systems or people accessing information from SBG/PSB.

7) 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, the system does not share data with other agencies.

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

N/A

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

N/A

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

To minimize the risk of data being accessed without permission, SBA stores SBG/PSB data in a secure database with limited access.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) **System Owner**

__________________**(Signature)** 4/11/2011 **(Date)**

Name: Frank Lalumiere

Title: Associate Administrator for Surety Bond Program, OCA

2) **Project Manager**

__________________**(Signature)** 4/11/2011 **(Date)**

Name: Stephen Kusharski

Title: Project Manager

3) **IT Security Manager**

Tracy Thompson for CISO **(Signature)** 5/25/10 **(Date)**

Name: Ja'Nelle DeVore

Title: Chief Information Security Officer

4) **Chief Information Officer (CIO)/Chief Privacy Officer (CPO)**

__________________**(Signature)** 5/25/11 **(Date)**

Name: Paul Christy

Title: CIO/CPO