PRIVACY IMPACT ASSESSMENT TEMPLATE

Name of System/Application: Financial Management System (FMS)
Program Office: Office of the Chief Financial Officer

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?** *(Name, title, SBA Office, phone number, and SBA e-mail)*

Jonathan I. Jones
IT Specialist
Office of the Chief Financial Officer
(202) 205-7365
Jonathan.Jones@sba.gov

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

Jonathan I. Carver
Chief Financial Officer
Office of Chief Financial Officer
202-205-6449
Jonathan.Carver@sba.gov

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

Uma Yanamandra
Acting Director, Office of Financial Systems
Office of Chief Financial Officer
202-205-6106
Uma.Yanamandra@sba.gov

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

Chief Information Security Officer

JaNelle Devore
Chief Information Security Officer
Office of the Chief Information Officer
(202) 205-7103
JaNelle.Devore@sba.gov

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

Ethel 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?** *(Name, title, SBA Office, phone number. and SBA e-mail)*

Paul T. Christy
Chief Information Officer/Privacy Officer
(202) 205-6708
Paul.Christy@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

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

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

Yes. Both vendor and borrower information is processed through the disbursements subsystem. The information is generated from other agency systems and forwarded through FMS to Treasury for payment. The information processed is full name, social security number, address and bank account information.

b. Is the information about employees?

Yes. Employee payroll and travel reimbursement information is processed through the system for payment. The information that is passed is full name, social security number, address and bank account information.

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

The Treasury Disbursements sub system of the FMS stores all payment files sent to Treasury and maintains a register of all disbursements made, which includes employee, vendor, bank, and borrower information.

3) Is the system in the development process?

No

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

N/A

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

15 U.S.C. § 634(b) (6), 44 U.S.C. § 3101. Public Law 85536, 15 U.S.C. § 631 et seq. (Small Business Act, all provisions relating to loan programs); 44 U.S.C. § 3101 (Records Management by Federal Agencies); and Public Law 10362 (Government Performance and Results Act). Public Law 85699 as amended 15 U.S.C. §661 et seq. (Small Business Investment Act of 1958, all provisions relating to loan programs)

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

Primary risk is unauthorized viewing or reporting of PII information in the data set. This is mitigated by:

- Strict application of the least privilege concept, only those that need to know the information can view it.
- Access rosters are reviewed at least quarterly to insure that only authorized employees have access
- Login activity is logged and reviewed weekly. Database activity is logged and reviewed weekly.

C. SYSTEM DATA

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

Employees, Vendors, and Borrowers

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?

The initial information is gathered from the individual or bank representative by other internal systems including Joint Administrative Accounting System (JAAMS), Partner Identification Management System (PIMS), Electronic Loan Information Processing System (ELIPS), Surety Bond Guarantee (SBG) and Loan Accounting System (LAS). FMS receives this information from those sources, not directly, to use in disbursement processing.

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

The U.S. Department of Treasury is providing confirmation and payment collection information.

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?

The system does not collect any information from the employee or the public. Data is collected by other agency systems and forwarded through FMS to Treasury.

3) Accuracy, Timeliness, and Reliability

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

The U.S. Department of Treasury has controls in place to collect accurate data on payments they make and receive on behalf of federal agencies.

b. How is data checked for completeness?

All disbursements and collections result in adjustments to SGL 1010. The Agency's Cash Reconciliation system reconciles Agency accounting transactions against Treasury's records of disbursements and receipts. Differences are identified, reconciled, and corrected.

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).

This system processes the data passed to it from JAAMS, ELIPS, SBG, LAS, and PIMS systems. Those systems have procedures to validate information in them and provide opportunities for the information source to review and correct their information.

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

Yes. Currently there is a data model. OCFO is in the process of updating the data dictionary with more details.

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

There is a risk that employees can view PII data that is not required for them to perform their job. The risk is mitigated by assigning user accounts with specific roles and responsibilities which limit user's system access based on their job related responsibilities.

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, the information is necessary to process vendor payments and generate loan disbursements.

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?

No

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

No

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

No

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?**

The data is not being consolidated.

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.**

Yes. Information can be retrieved by screens or ad hoc queries for reconciliation by SSN, TIN, Name, and Loan Number.

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

Automated queries are done to evaluate the disbursement history, track down missing payments, and to process cancellation transactions on disbursements that are not actually cleared by the payee. Access to reports is limited to those individuals with authorized use and only for specific reports as it pertains to the user's role/need.

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.

The system only stores information previously collected by other agency systems.

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

The FMS controls restricts access to privileged functions and security-relevant information to explicitly authorized personnel. User accounts are only granted to authorized personnel and access minimum necessary to perform their assigned duties. The system has implemented the following role-based access controls. Database activity is logged and reviewed weekly for anomalies.

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?

It is operated at one site only.

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

As specified in SBA's Privacy Act Systems of Records, SBA 20 and SBA 21, In accordance with SBA Standard Operating Procedure 00 41 2 Records Management Program in appendices 17, 18, and 19.

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?

Procedures for disposition stated in SBA SOP 00 41 2, appendices 17, 18, and 19, retention for financial records.

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?

N/A

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

No

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

N/A

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

Agency Security Roles and Procedures/Controls – Agency Security Access Procedures – Access is limited by controlled 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.

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

SBA's Privacy Act Systems 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?**

It is not being modified.

F. DATA ACCESS

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

Users are members of the OCFO Staff located in the Denver Finance Center and Headquarters.

For performing system maintenance activities, authorized personnel from Office of Financial Systems, CFO's office will have access to FMS. This includes developers, system administrators, and database administrators. OFS resources include both contractors and employees.

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

There are technical controls to ensure that only authorized users have access, as well as managerial controls to ensure that users have authorized access.

Functional managers perform a quarterly recertification and reconciliations to ensure the quality of the security program.

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

Users who have been duly authorized access to the system have access based on roles. However, in place technical controls that make the data read only to these users ensure that they have no ability to change any data.

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**)

Access is limited via user id and password controls, and rights are assigned to groups within the Operating System. FMS follows the principle of least privilege as the most appropriate and significant control. Database activity is logged and reviewed weekly for anomalies.

In addition, agency personnel have to take a mandatory annual security training course which includes privacy act rules and prohibitions. Also agency security procedures mandate that a posted privacy notice be viewed and acknowledged prior to entry into 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 their contracts and other regulatory measures addressed?**

Yes, there is contract support to assist in the maintenance of the infrastructure. There is also contract support to provide system administration to the systems.

Yes. Privacy act contract clauses are in their contracts and other regulatory measures are addressed.

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

Information is forwarded through FMS to Treasury for process loan disbursement and vendor payment.

Information is not shared outside of FMS but is used by other process within FMS, such as the 1098 System for Cancelation. The 1098 System for Cancellation of disbursements accesses these records to determine who a payment was made to, and how to cancel the disbursement.

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

The System Manager is responsible for protecting the privacy rights of the public and employees.

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.**

The primary risks identified were maintaining confidentiality and integrity of the data. Because of the breadth of PII information required to disburse federal funds, maintaining confidentiality of the data is critical. This risk is mitigated by a two-step approach:

1. All PII data stored by the system is maintained in a secure directory for PII data with extremely limited access. Access to this directory is reviewed quarterly, and is limited to those individuals with a definable need for access to the information.

2. PII information stored in Sybase is controlled through the granting and revocation of roles. Sybase roles are reviewed quarterly.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) **System Owner**

_____ **(Signature)** 1/7/10 **(Date)**

Name: Jonathan I. Carver

Title: Chief Financial Officer

2) **Project Manager**

_____ **(Signature)** 1/6/2011 **(Date)**

Name: Uma Yanamandra

Title: Acting, Director, Office of Financial System

3) **IT Security Manager**

_____ **(Signature)** 1-6-2011 **(Date)**

Name: JaNelle Devore

Title: Chief Information Security Officer

4) **Chief Privacy Officer**

_____ **(Signature)** 1/10/2011 **(Date)**

Name: Paul T. Christy

Title: Chief Privacy Officer