

SMALL BUSINESS ADMINISTRATION
PRIVACY IMPACT ASSESSMENT (PIA)

Name of Project: Oracle Administrative Accounting System/JAAMS
Project's Unique ID: JAAMS

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- SBA IT Security Manager
- SBA OCIO IT Portfolio Division
- SBA Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

1) Who is the person completing this document?

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

2) Who is the System Owner?

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

3) Who is the System Owner Representative for this system or application?

Deepak Bhargava
Director, Office of Financial Systems
Office of Chief Financial Officer
202-205-7420
Deepak.Bhargava@sba.gov

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

David L. McCauley
Chief Information Security Officer
Office of the Chief Information Officer
(202) 205-7103
David.McCauley@sba.gov

5) Who is the Bureau/Office Privacy Act Officer who reviewed this document?

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? (According to OMB, this the agency CIO or other agency head designee who is other than the official procuring the system or the official who conducts the PIA).

Robert B. Naylor
Chief Information Officer/Chief Privacy Officer
(202) 205-6708
Robert.Naylor@sba.gov

B. PIA PROCESS APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

a. Is this information identifiable to the individual?

Yes

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

Yes

c. Is the information about employees?

Yes

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

The Oracle Administrative Accounting/JAAMS is a financial management system. It is used for SBA's administrative accounting only. The system is a place of financial record for the funding and expenditure of SBA's administrative funds.

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

Title 6 General Accounting Office (GAO) Policy and Procedures Manual, 31 U.S.C. Part 285, Sections 112(a) and 113 of the Budget and Accounting Procedures Act of 1950 and 5 USC Chapters 55 through 63 and 15 U.S.C. § 634(b)(6), 44 U.S.C. § 3101.

C. DATA IN THE PROCESS:

1) What categories of individuals are covered in this process?

Employee, Vendors

2) What are the sources of the information in this process?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, source then what other source?

Data is taken from other sources. The SBA receives external data files from Health and Human Services (HHS) (Payment Management System, USDA's National Finance Center (NFC) (Payroll and Employee information), JPMorgan Chase (Credit Card), and United Parcel Service (UPS). Furthermore, the SBA processes internal data from the Surety Bond Guarantee (SBG) system.

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

NFC processes SBA's payroll. The U.S. Department of Treasury processes all payment requests generated by this Administrative accounting system and provide confirmations.

HHS processes grant payments SBA's Women Business Centers and provides the necessary information to generate the administrative accounting transactions.

c. What State and local agencies are providing data for use in the process?

SBA receives paper requests for payments from state and local agencies for grants. Payment and accounting information is stored in the system. No electronic records are received.

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

Data will be collected from the JPMorgan Chase and UPS for reconciliation purposes.

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

SBA maintains information for payments to employees including banking information, (routing numbers and accounts) addresses, and SSN.

SBA maintains payment information on grantees and information on the vendors and contractors who provide products and services related to SBA's administrative functions. The information consists of tax IDs (which can be a SSN if the company is a sole proprietor), payment information including banking information and addresses.

3) Accuracy, Timeliness, and Reliability

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

The US Department of Treasury and the US Department of Agriculture's National Finance Center have controls in place to collect accurate data.

Health and Human Services information is reviewed and approved by the Office of Women's Business Ownership prior to the grant reimbursement payment being processed.

b. How will data be checked for completeness?

Each program office has the responsibility of reconciling the information that is received from the JPMorgan Chase and UPS. In addition, the system has been built with edits that assure the completeness of records including the generation of errors.

The Office of Women's Business Ownership has the responsibility of verifying and processing the HHS information prior to the accounting transactions generated and the reimbursement payment being made.

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)

Yes, the data is current. As part of the financial reporting process, the system records are reconciled at minimum on a monthly basis by the Office of the Chief Financial Officer. The documents include the financial statements and the SF224.

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

Yes. SBA implemented the Oracle Federal Financials suite of financial applications. The Oracle suite is well documented. SBA has additionally created enhancements to the Oracle functionality using Oracle provided tools. These extensions, that address gaps in functionality, are also well documented.

D. ATTRIBUTES OF THE DATA:

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

Yes. Only the minimum data necessary for the administrative accounting process for the agency is collected.

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?

New or previously unavailable data is potentially created as financial documents and summary reports generated when daily, weekly, monthly, and sometimes yearly business process cycles are executed and information in the system is reconciled. This may include address changes, voucher payments, vendor payments, periodic reports, etc... This system supports SBA financial processes with the latest data available so data is continually created and/or updated although not all of it would be considered privacy data.

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

Yes, new data will be placed in the individual's record. For example, when an employee voucher payment is made, the information will be reflected in the employee's record.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No

5) How will the new data be verified for relevance and accuracy?

The information is manually entered and reviewed. The request is then reviewed and approved by a second individual. Reports are run frequently to ensure that there is nothing left in the approval queue.

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

Data is not being consolidated in this system.

- 7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access through the process? Explain.**

Processes are not being consolidated.

- 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 through ad hoc queries and standard reports. Yes, data can be retrieved by SSN, Travel Voucher/Requisition Number and 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?**

A variety of reports can be developed as needed. Generally these reports are used for reconciliation purposes (payment confirmation, balances, and accounting reconciliation). Because of the sensitivity of the data, reports are treated as such. They are only distributed on a need to know basis.

- 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.)**

Suppliers have the right to decline to provide information or consent to uses of the information, but will prevent SBA from the ability to do business with them. For example, create payments for goods and services.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

- 1) **If the information in the process operated in more that one site, how will consistent use of the data be maintained in all sites?**

The system is web based and accessed by authorized SBA employees nationwide from the different SBA offices. The system is configured to ensure data consistency and has automated data entry rules to ensure quality of data. One system and set of financial records is in place for all SBA administrative accounting data.

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

In accordance with NARA standards, data is retained for 6 years and 4 months.

- 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?**

In accordance with NARA standards, data will be retained and archived following SBA policy.

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

No, the system is not using technologies in ways that the SBA has not previously employed.

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

There is no affect. SBA does not use this technology

6) Will this system in the process provided the capability to identify, locates, and monitors individuals? If yes, explain

Yes, the system can identify and locate SBA employees and vendors who are sole proprietors for purposes of making payments. The system does not monitor individuals.

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

The system does not use tracking technology to monitor individuals.

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

Users have to sign rules of behavior document. SBA has pre-determined roles for users in the Oracle system which means that specific forms are made available to a user depending on their job function at the SBA.

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

SBA 23 – Payroll Files
SBA 33 – Travel Files

10) If the system is being modified, will the Privacy Act Systems of records notice require amendment or revision? Explain.

N/A

F. ACCESS TO DATA:

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

- SBA employees with the responsibility of entering and maintaining records related to administrative accounting. For example, Administrative Officers and Budget Coordinators from the program offices.
- SBA Management with approval authority for administrative transactions
- SBA's Office of Procurement and Grants Management personnel related to administrative accounting functions
- SBA's Office of the Chief Financial Officer personnel related to administrative functions. This includes functional users as well as developers. Limited access is given to troubleshoot problems and assist end users.
- Authorized personnel from SRA, the SBA's Applications Service Provider for this system. This includes systems and database administrators.

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

SBA has pre-determined roles for users in the Oracle system which means that specific forms are made available to a user depending on their job function at the SBA. Access is provided by IT Security upon receipt of the written authorization by the user's manager indicating specifically which responsibilities should be associated with the named user. These pre-determined responsibilities are associated with specific authorization and approval levels, job functions, access to certain forms, data entry ability versus inquiry only, ability to modify data, access to certain data, etc. IT Security processes the access requests based on policy.

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

Least privilege policy is used. A user's access is based on the responsibility assigned to the user. Therefore, users' access is restricted by responsibility. The pre-determined responsibilities, as described in the question above, assign different forms and types of data to a user. For example, inquiry only responsibilities do not allow data entry or modification.

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

For critical processes, 'rules of two' are in place. These rules require that data entry performed by one user is approved by another user. These two functions (data entry and approval) create a separation of duty.

IT Security also conducts bi-annual security reviews of access to Oracle to validate that users are still performing the same job responsibilities within Oracle. The reviews require validation from managers to ensure that the access is appropriate and accurate.

Additionally, database activities are logged. User information is also tracked in the system for audit purposes such as unsuccessful logins and form access reports.

Data is scrambled on the non-production environments during the cloning process. In the event that unscrambled data is needed for specific testing, the environment is treated like a production environment. In addition, access is restricted and the data is only unscrambled for the time needed to perform the testing.

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, the JAAMS system is hosted by SRA. SRA performs an array of functions from Database Administration to functional support. A Privacy Act clause is in the base contract.

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?

N/A

8) Will other agencies share data or have access to the data in this system?

No

9) How will the data be used by the other agency?

N/A

10) Who is responsible for assuring proper use of the data?

N/A

G. Privacy Impact Analysis:

1) Discuss what privacy risks were identified and how they were mitigated for types of information collected.

Because JAAMS collects some PII information and not everyone needs to have access to the information, only those that need to know the EIN or SSN information can view it. Also only those need to query based on EIN or SSN have permission to do so.

Since production data is cloned to non-production environments, sensitive data is masked to avoid information being compromised. In the event that unscrambled data is needed for specific testing, the environment is treated like a production environment. In addition access is restricted and the data is only unscrambled for the time needed to perform the testing.

2) Describe any types of controls that may be in place to ensure that information is used as intended?

Users have to sign rules of behavior document. SBA has pre-determined roles for users in the Oracle system which means that specific forms are made available to a user depending on their job function at the SBA.

Data is scrambled in the non-production environments during the cloning process. In the event that unscrambled data is needed for specific testing, the environment is treated like a production environment. In addition access is restricted and the data is only unscrambled for the time needed to perform the testing.

3) Discuss what privacy risks were identified and how they were mitigated for information shared internal and external?

JAAMS uses extracts and lockboxes to exchange data with internal and external systems. Only required data is exchanged. Electronic data is transferred using secure interface including, VPN, secure lease line, file encryption, secure shell, and secure FTP.

A user's access is based on the responsibility assigned to the user. Therefore, users' access is restricted by responsibility. The pre-determined responsibilities, as described in the question above, assign different forms and types of data to a user.

4) 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 jobs, user accounts are assigned specific roles and responsibilities. Users have to log onto the system using a login and a SOP 90-47 compliant password. They are limited in their access to areas of the system appropriate for those responsibilities.

To ensure developers and testers don't access production data in the non-production instances the data is scrambled during the cloning process. In the event that unscrambled data is needed for specific testing, the environment is treated like a production environment. In addition, access is restricted and the data is only unscrambled for the time needed to perform the testing.

Privacy Impact Assessment PIA Approval Page

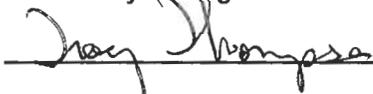
The Following Officials Have Approved this Document:

1) System Owner Representative

 _____ (Signature) 4/7/10 _____ (Date)

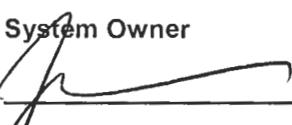
Name: Deepak Bhargava
Title: Director, Office of Financial System

2) IT Security Manager

 _____ (Signature) 4/22/10 _____ (Date)

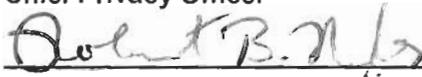
For Name: David McCauley
Title: Chief Information Security Officer

3) System Owner

 _____ (Signature) 4/2/10 _____ (Date)

Name: Jonathan I. Carver
Title: Chief Financial Officer

4) Chief Privacy Officer

 _____ (Signature) 5/4/10 _____ (Date)

Name: Robert B. Naylor
Title: Chief Privacy Officer