

U.S. Small Business Administration
409 3rd Street, S.W.
Washington, DC 20416

Office of the Chief Financial Officer

Joint Administrative Accounting Management System Privacy Impact Assessment January 7, 2021

System Owner

Nate Reboja
Information System Owner
Office of the Chief Financial Officer
Nathaniel.Reboja@sba.gov

Reviewing Official

Keith A. Bluestein
Senior Agency Official for Privacy
Chief Information Officer
Office of the Chief Information Officer
Privacy@sba.gov

This is a Controlled Unclassified Document

I. System Description/General Information

The Joint Administrative Accounting Management System (JAAMS) is a financial management application. It is the system of record for managing funding and expenditure of SBA's administrative funds. Title 6 General Account Office Policy and Procedures Manual, 31 U.S.C part 285, sections 112(a) and 113 of the Budget and Accounting Office Act of 1950 and 5 U.S.C. Chapters 55 thru 63 and 15 U.S.C. § 634 (b)(6) 44 U.S.C. § 3101 is the legal authority that supports the purchase and development of JAAMS.

JAAMS is implemented using the Financial Systems Integration Office (FSIO)-compliant core financial system software Oracle E-Business Suite (EBS), which is also known as Oracle Federal Financials.

The EBS modules that SBA uses include:

- 1) Accounts Receivable (AR) Processes many types of administrative receivables (parking, jury duty, vendor rebates, etc.). Field cashiers use it nationwide.
- 2) Accounts Payable (AP). Used by the Denver Finance Center (DFC) to pay vendors, employee travel vouchers in support of disasters, conferences etc.
- 3) General Ledger (GL) and Budget Execution (BE) Supports a consolidated general ledger.
- 4) Purchasing (PO) Supports issuance and tracking of purchase orders (PO) and blanket purchase orders (BPO).

SBA has integrated Oracle's Configuration, Extension, Modification, Localization, and Integration (CEMLI) software extension framework. CEMLI is Oracle's published guideline for developing and implementing custom extensions to Oracle Applications. Additional application tools following the CEMLI guidelines are used to improve flexibility and provide extra functionality not available in the standard product.

Administrative Officers create purchase orders for their offices and track spending. The SBA Denver Finance Center processes all financial transactions. Furthermore, SBA Denver Finance Center users include accounts payable technicians, accounts receivable analysts, and the general ledger team. They also provide Tier I help desk and troubleshooting support.

JAAMS contains information about individual members of the public and employees. The system maintains payment information on grantees and information on the vendors and contractors who provide products and services related to SBA's administrative functions. This information consists of tax IDs (which can be the Social Security Number (SSN) if company is a sole

proprietor, payment information including banking information and addresses).

II. System Data

The categories of individuals covered in the system are SBA employees and vendors. Sources of the information is obtained through other IT systems; specifically, SAM.gov which provides vendor data for usage in JAAMS, and National Finance Center (NFC) provides employee personnel and payroll data for usage in JAAMS. No other entities: tribal, state, local, or third-party sources are providing data for use in the system. No information is collected directly from the employee or the public.

The SBA receives data files from Health and Human Services (HHS), United States Department of Agriculture NFC, Citibank Government Card Services and United Parcel Service (UPS) that is checked for accuracy. Furthermore, the SBA processes internal data from the Surety Bond Guarantee (SBG) System.

The NFC processes SBA payroll. The U.S. Department of Treasury processes all payment requests generated by this administrative accounting system and provides confirmation.

HHS processes grant payments for SBA's Women Business Centers and provides the necessary data to generate the administrative accounting transactions. The data must be complete and current to process. You can find the data elements described in the JAAMS data dictionary.

III. Data Attributes

The use of the data is relevant and necessary for the purpose for which the system is being designed. Only the minimum data necessary for the accounting process for the agency are collected in accordance with the Chief Financial Officers (CFO) Act of 1990 (Public Law 101-576) as amended. 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 and periodic reports. 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.

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. New data is verified for relevance, timeliness, 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. Data can be retrieved through ad hoc queries and standard reports. A personal identifier can be used to retrieve data. SSN, TIN, Travel Voucher/Requisition Number, and name can be used. A variety of reports can be developed as needed. These reports are used for reconciliation purposes (payment confirmation, balances, and accounting reconciliation) and are distributed on a need-to-know basis. Suppliers have the right to decline to provide information or consent to uses of the information, however this prevents the SBA from the ability to do business with them. Creating payments for goods and services would be an example of such action.

IV. Maintenance and Administrative Controls

JAAMS 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.

The retention period for JAAMS is in accordance with NARA standards, data is retained for 6 years and 4 months. Disposition of the data at the end of the retention period comply with NIST SP 800-88, as amended.

JAAMS is under Privacy Act systems of records notice (SORN) SBA 23-Payroll Files and SBA-33 Travel Files.

V. Data Access

Authorized agency users have access to the system based on their specific roles or responsibility:

- 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 the contract support staff for OCFO, the SBA's Applications Service Provider for this system. This includes

systems and database administrators. Privacy Act clauses are in the contract.

The 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 an OCFO system administrator upon receipt of 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. The 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.

JAAMS employs an array of controls to protect individuals' data including database encryption, data redaction, database auditing, access control lists, and least privilege. For critical processes, the 'rule of two' are in place. This requires that data entry performed by one user is approved by another user. These two functions (data entry and approval) create a separation of duty.

Bi-annual account recertification reviews are used 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 are encrypted on the non-production environments during the cloning process. If unscrambled data is needed for specific testing, the environment is treated like a production environment.

External systems do not share data or have access to the data in JAAMS. Information System Security Officer, system owner, system administrator and the Senior Agency Official for Privacy are responsible for protecting the privacy rights of the public and employees in this system.

VI. Privacy Impact Analysis

There is a risk related to data type in which the sensitivity of the JAAMS data elements increases the risk for inadvertent disclosure which is susceptible to identity theft. There is also risk to ensure that the information is used as intended and the type of information collected. Some data provides significant

information about individuals has context with regard to individual's finances and business tax purposes. Revelation of JAAMS data could have a significant revelation impact to employees and external entities. Disclosure of JAAMS data would not significantly lose relevance over time. Disclosure of JAAMS data would not adversely affect any particular vulnerable population.

Privacy risks are mitigated through access control, auditing, secure application design and monitoring, encryption, and authentication. Mitigation also includes limiting context regarding grant information and ensuring collection is comparable to its' collection; ensuring collection follows statutory authority to collect, encryption of data in transit and at rest; incremental and full backups, data integrity checks, data redundancy, and Contingency Planning. Regarding the relevance of data, time diminishes the risk slightly as much of the information is intended would no longer be current or potentially applicable. Lastly, mitigation is also through education via annual Cybersecurity Awareness and Privacy Training.