The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):

http://www.fiscal.treasury.gov/fsreports/fspia/fs_pia.htm

Name of System: Oracle E-Business Suite (OeBS)

Document Version: 540.SCM.1.FS.11

Document Date: August 26, 2014

SYSTEM GENERAL INFORMATION:

1) System Overview:

The Bureau of the Fiscal Service's Financial Accounting Operations (FAO) provides financial management and manufacturing applications to Fiscal Service and franchising customers via the Oracle e-Business Suite. These applications include general ledger, budget execution, purchasing, accounts payable, accounts receivable, fixed assets, inventory and order management, transportation planning, and Discoverer reporting.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate?

TREASURY .009, Treasury Financial Management Systems—Treasury

3) If the system is being modified, will the SORN require amendment or revision?

__yes, explain.
_X_no

4) Does this system contain any personal information about individuals?

_X_yes
__no

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

b. Is the information about employees or Contractors? Yes

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

The system is not currently undergoing modification, other than continued maintenance and minor application upgrades.

Authority for maintenance of the system is permissible under: 31 U.S.C. Section 3512; 31 U.S.C. Section 3711; 31 U.S.C. Section 3721; 5 U.S.C. Section 5701 et seq.; 5 U.S.C. Section 4111(b); Pub. L. 97–365; 26 U.S.C. Section 6103(m)(2); 5 U.S.C. Section 5514; 31 U.S.C. Section 3716; 31 U.S.C. Section 321; 5 U.S.C. Section 301; 5 U.S.C. Section 4101 et seq.; 41 CFR 301–304; Executive Order 11348; and Treasury Order 140–01.

DATA in the SYSTEM:

1) **Identify the category of individuals in the system**
   Check all that apply:
   - **_X_ Employees**
   - **_X_ Contractors**
   - **_X_ Taxpayers**
   - **_X_ Others (Government Agencies and Franchise Customers)**

2) **Identify the sources of information in the system**
   Check all that apply:
   - **_X_ Employee**
   - **_X_ Public**
   - **_X_ Federal agencies**
   - **___ State and local agencies**
   - **_X_ Third party**

   a. **What information will be collected from employees or contractors?**

      Federal payroll and Central Contractor Registration (SAM.gov website) information and data for use in the Oracle e-Business Suite.

   b. **What information will be collected from the public?**

      Collected employee and Contractor data includes names, addresses, social security numbers, Tax Identification Numbers (TINS), and financial institution Automated Clearing House (ACH) data, (i.e., account numbers and bank routing numbers).

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

      Central Contractor Registration (SAM.gov) and Government franchise agencies.

   d. **What state and local agencies are providing data for use in the system?**

      None.

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

      Data from purchase card providers.

3) **Accuracy, Timeliness, and Reliability**

   a. **How will data collected from sources, other than Fiscal Service records, be verified for accuracy?**

      The majority of the vendor Personally Identifiable Information (PII) within the Oracle e-Business Suite is provided directly by the vendor, which is submitted via a proposal, invoice, or other related document. Authorized Fiscal Service employees enter this PII into the system.

Fiscal Service relies on the individual or vendor to update their information as appropriate.

b. How will data be checked for completeness?

Data is checked for completeness by the data validation rules within the Oracle e-Business Suite.

c. What steps or procedures are taken to ensure the data is current?

CCR (SAM) maintains a feature within the database that inactivates vendor accounts if the data hasn't been updated by the vendor within the past year. All other data is verified to ensure that it is current against the SAM database.

d. In what document(s) are the data elements described in detail?

Oracle produces manuals that cover the data elements.

ATTRIBUTES OF THE DATA:

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

The data is collected and maintained to assure the orderly processing of financial management and manufacturing actions within Fiscal Service and its franchise customers.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? How will this be maintained and filed?

The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

The system will not derive new data or create previously unavailable data about an individual through aggregation.

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

No, the system will not derive new data or create previously unavailable data about an individual through aggregation.

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

The system will not derive new data or create previously unavailable data about an individual through aggregation.

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

The Oracle e-Business Suite has the ability to track individual actions within the application. The audit and accountability controls are based on Treasury and Fiscal Service policies and standards, which, in turn, are based on the applicable laws and regulations. These controls assist in detecting security violations, performance problems, and flaws in applications.

Users are restricted to data that is only required in the performance of their duties. The concept of "least privileged" is followed at Fiscal Service whereas the information system shall enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Additionally, the Department of the Treasury (Treasury), Bureau of the Fiscal Service (Fiscal Service) Information Technology (IT) Security Rules of Behavior (ROB) ensure that users are made aware of their security responsibilities before accessing Fiscal Service's IT resources. All users are required to read and sign these rules acknowledging their responsibilities in protecting Fiscal Service's IT systems and data. Noncompliance with these rules may result in termination of access privileges, administrative actions, and/or criminal prosecution if warranted.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? (Explain)

Processes are not being consolidated.

8) How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.)

Users are restricted to the data required for the performance of their duties. Only authorized personnel are able to run queries. Queries may be executed based on any data element within the Oracle e-Business Suite. Fiscal Service maintains Oracle User Manuals that lists all data elements within the system.

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

Multiple reports can be generated using the Oracle e-Business Suite data. These reports are executed while performing the day-to-day services that Fiscal Service provides to its customers. Examples of these reports include Active Suppliers and Customers, Purchase Order Summaries, etc. User access to the reports is granted based on the separation of duties principle through assigned access authorizations and the least privileged principle. The privileges granted will be based on job function. The Oracle e-Business Suite application is configured to allow the users to access specific functions of the system through responsibilities. The responsibility determines the user's access to a specific application; an organization; and specific windows, functions, and reports.

Additionally, the Oracle e-Business Suite is enabled with Oracle Workflow, which helps manage Fiscal Service's business rules and control requirements.

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

Individuals have the opportunity to decline or to consent to particular uses of the information on the SAM.gov (CCR) website. The Privacy Act Policy and Laws are listed on the website.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) What are the retention periods of data in this system? How long will the reports produced be kept?

Records are maintained in accordance with National Archives and Records Administration (NARA) retention schedules.

2) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?

Paper and microform, records ready for disposal, are destroyed by shredding or maceration. Records in electronic media are either electronically erased using accepted techniques or shredded.

Reports are maintained in accordance with the NARA retention schedules.

The Records Management Section is responsible for ensuring Fiscal Service's functions are adequately documented by ensuring permanent records are preserved, records no longer of current use are promptly destroyed, retention schedules are developed and implemented, and that Fiscal Service complies with the recordkeeping requirements issued by the Office of Management and Budget, the General Service Administration, NARA, and the National Institute of Standards and Technology (NIST).

The disposition procedures used to facilitate this process are documented on Fiscal Service's intranet.

3) If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites?

The system is operated at only one location.

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

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

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

Fiscal Service is not using technologies in ways that the Fiscal Service has not previously employed before (e.g., monitoring software, Smart Cards, Caller-ID).

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

The Oracle e-Business Suite is not intended, nor does it have the ability, to identify, locate, and monitor individuals. However, the Oracle e-Business Suite has the ability to track individual actions within the application. The audit and accountability controls are based on Treasury and Fiscal Service policies and standards, which, in turn, are based on the applicable laws and regulations. These controls assist in detecting security violations, performance problems, and flaws in applications.

7) **What kind of information is collected as a function of the monitoring of individuals?**

1. Date and time of access.
2. Subject identity (UserID or ProcessID).
3. Outcome of events (logon attempts and failures).
4. Information/file accessed or modified.
5. User account management (creation, deletion, and modification).
6. Actions by privileged users.
7. Location of the event.

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

Users are restricted to data that is only required in the performance of their duties. The concept of "least privileged" is followed at Fiscal Service whereas the information system shall enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Additionally, the Department of the Treasury (Treasury), Bureau of the Fiscal Service (Fiscal Service) Information Technology (IT) Security Rules of Behavior ensure that users and administrators (both Contractor and Government employees) are made aware of their security responsibilities before accessing Fiscal Service's IT resources. All users and administrators (both Contractor and Government employees) are required to read and sign these rules acknowledging their responsibilities in protecting Fiscal Service's IT systems and data. Noncompliance with these rules may result in termination of access privileges, administrative actions, and/or criminal prosecution if warranted.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
Check all that apply:
_X_ Contractors
_X_ Users
_X_ Managers
_X_ System Administrators
_X_ System Developers

_X_ Others (explain) Oracle e-Business Suite Support Staff

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

Access to data by a user is determined by the "need-to-know" requirements of the Privacy Act, the user's profile based on the user's job requirements, and managerial decisions.

Criteria, procedures, controls, and responsibilities regarding access are documented. Treasury Department Publication (TD P) 85-01 documents that the system manager is responsible for ensuring access to the information and data is restricted to authorized personnel on a "need-to-know" basis. Additionally, Portable Document Format (PDF) 5409-1 E, *Administrative Resource Center (ARC) System Access Form - End User Applications,* is used to request access to "need-to-have" applications. Access is requested and routed to appropriate managers for review and approval prior to access being granted.

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

Users will be restricted to data that is only required in the performance of their duties. The concept of "least privileged" is followed at Fiscal Service whereas the information system shall enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

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)**

Users will be restricted to data that is only required in the performance of their duties. The concept of "least privileged" is followed at Fiscal Service, and the hosting Contractor, whereas the information system shall enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Oracle e-Business Suite users are assigned a unique user ID and password. User identifiers are managed by the following:

1. Verifying the identity of each user.
2. Receiving authorization to issue a user identifier from an appropriate organization official.
3. Ensuring that the user identifier is issued to the intended party.
4. Disabling user identifier after 30 days of inactivity.
5. Archiving user identifiers.

Users, logging into the Oracle e-Business Suite application, are presented with a sign-on screen requiring entry of a user name and password.

IT Security RoB was provided to all franchise customers. Access Request forms must be submitted to FAO in order to obtain access to the Oracle e-Business Suite. The franchise

customer employee must sign the Access Request form stating that they have reviewed and understand the RoB and Privacy Act Procedures.

IT Security RoB have been reviewed and signed by each Fiscal Service employee and Contractor employees that support the Oracle e-Business Suite. The IT Security RoB states that employees (and Contractors) should:

1. Not read, alter, insert, copy, or delete any Fiscal Service data except in accordance with assigned job responsibilities. Ability to access data does not equate to authority to manipulate data. In particular, users must not browse or search data except in the performance of authorized duties.
2. Notify their Supervisor when access to IT resources is no longer required, and make no further attempts to access the resources.

Privacy Act Procedures state the employees (and Contractors) should:

- not disclose information to any employee other than those who need it to perform official duties.
- refer disclosure requests from the public or from other agencies to your supervisor.
- make sure information on your computer or desk is not in view of others not authorized to see it.
- make sure records are secured when you are not at your computer or desk.
- not discuss information in the automated systems with anyone who does not have an official need to know it.
- maintain the confidentiality of information even if you leave your position or the subject of the information leaves.
- treat copies with the same care as originals.

And outlines the penalties for non-compliance with the Privacy Act regarding automated records to be:

- Charge of a criminal misdemeanor and fine up to $5,000 for willfully disclosing information known to be prohibited from disclosure, or requesting or obtaining any record concerning an individual under false pretenses.
- The United States can be liable to an individual for damages and attorney's fees and costs when willful and intentional failure to comply with the Privacy Act causes an adverse effect on an individual.

The above mentioned controls are used to prevent or discourage unauthorized use of the data. Audit features are in place and used to identify any unauthorized use that has already taken place. These audit features are reviewed regularly.

5) If Contractors are/will be involved with the design, development or maintenance of the system, were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?

Yes, Contractors are involved with the design and development of the system and will be involved with the maintenance of the system.

Privacy Act clauses, statutory, and regulatory clauses were addressed and inserted into the appropriate contract(s).

6) **Do other systems share data or have access to the data in the system?**
   _X_ yes
   __no

   If yes,

   a. Explain the interface.

   Other systems share data in the Oracle e-Business Suite through interfaces for such transactions in the form of batch processes, file uploads, etc.

   b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.

   Although all employees who have access to information in a Privacy Act system have the responsibility for protecting personal information covered by the Privacy Act, the information owner, system manager, and ultimately the Fiscal Service CIO have the responsibility to see that the data is protected from all threats.

7) **Will other agencies share data or have access to the data in this system?**
   _X_ yes
   __no

   If yes,

   a. Check all that apply:
   _X_ Federal
   __State
   __ Local
   _X_ Other (explain) Department of Defense and franchise customers.

   b. Explain how the data will be used by the other agencies.

   The other agencies may:

   1. Receive payment schedules generated by the Oracle e-Business Suite.
   2. Create summary accounting entries in the Oracle e-Business Suite system for payroll disbursements and monthly payroll expense accruals.
   3. Capture actual hours, completion quantities, scrap, item transfers, transportation planning, manual/system cycle counts, and inter-business unit transfer receipts.

   c. Identify the role responsible for assuring proper use of the data.

   Fiscal Service employees and Contractor employees who support the Oracle e-Business Suite, the system manager, system owner and ultimately the Bureau CIO are responsible for assuring the proper use of data in the system.

NIST requires Government organizations to establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

The Fiscal Service Disclosure Officer is responsible for administering requests for system data submitted to Fiscal Service involving the Privacy Act. Fiscal Service fully complies with the provisions of the Freedom of Information Act, Title 5 U.S.C. Section 552, and the Privacy Act, Title 5 U.S.C Section 552a. Fiscal Service provides an established procedure to solicit requests to review and correct information recorded, and it has a dedicated Disclosure Officer who manages and administers the program.