Oracle e-Business Suite
Privacy Impact Assessment (PIA)

August 14, 2007

System Information

Name of System, Project or Program: Oracle e-Business Suite
OMB Unique Identifier: 015-35-01-01-01-1171-24

Contact Information

1. **Who is the person completing this document?**

   Matthew J. Newell
   Management Analyst**,** ARC/BTD
   Bureau of the Public Debt
   200 Third Street
   Parkersburg, WV 26101
   5th Floor Avery Street Building
   304 480-7124
   matthew.newell@bpd.treas.gov

2. **Who is the system owner (Authorizing Official)?**

   Cynthia Z. Springer
   Executive Director, ARC
   Bureau of the Public Debt
   200 Third Street
   Parkersburg, WV 26101
   5th Floor Avery Street Building
   304 480-8760
   cindy.springer@bpd.treas.gov

3. **Who is the Information System Security Officer (ISSO)?**

   Matthew J. Miller
   Director, ARC/BTD
   Bureau of the Public Debt
   200 Third Street
   Parkersburg, WV 26101
   5th Floor Avery Street Building
   304 480-7056
   matthew.miller@bpd.treas.gov

4. **Who is the Information Systems Security Manager who reviewed this document??**

   Jim D. McLaughlin
   Manager, OIT/SAB
   Bureau of the Public Debt
   200 Third Street, Room 409
   Parkersburg, WV 26101
   304 480-7972
   jim.mclaughlin@bpd.treas.gov

5. **Who is the Bureau Privacy Act Officer who reviewed this document?**

   Denise K. Hofmann
   Privacy Officer, OMS/DAS/IMB
   Bureau of the Public Debt
   200 Third Street
   Parkersburg, WV 26101
   4th Floor Avery Street Building
   304 480-8402
   denise.hofmann@bpd.treas.gov

6. **Who is the IT Reviewing Official (Chief Information Officer)?**

   Kimberly A. McCoy
   Assistant Commissioner (CIO), Office of Information Technology
   Bureau of the Public Debt
   200 Third Street
   Parkersburg, WV 26101
   304 480-6635
   kim.mccoy@bpd.treas.gov

System Application/General Information

1. **Does this system contain any information in identifiable form?**

   Yes.

2. **What is the purpose of the system/application?**

   Public Debt's Administrative Resource Center (ARC) provides financial management and manufacturing applications to Public Debt 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, and Discoverer reporting.

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

   The Oracle e-Business Suite is an existing system, which received its most recent Authority To Operate (ATO) in September 2006.

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

4. **Under which Privacy Act SORN does the system operate? (Provide the system name and unique system identifier.)**

   TREASURY .009, Treasury Financial Management Systems—Treasury

Data in the System

1. **What categories of individuals are covered in the system?**

   Records cover present and former employees, contractors, and vendors for both the Bureau and franchise customers.

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?**

      Information is gathered from individuals, corporations, and government agencies.

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

      Federal payroll providers and the Central Contractor Registration (CCR) are providing data for use in the Oracle e-Business Suite.

   c. **What State and/or local agencies are providing data for use in the system?**

      None.

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

Data is also collected from purchase card providers.

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

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

3. Accuracy, Timelines, and Reliability

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

Much of the vendor Personally Identifiable Information (PII) within the Oracle e-Business Suite is provided directly by the vendor, which he/she submits via a proposal, invoice, or other related document. Authorized Public Debt employees enter this PII into the system.

ARC relies on the individual to update their information as appropriate.

b. How will the data be checked for completeness?

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

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. CCR maintains a feature within the database that inactivates vendor accounts if the data hasn't been updated within the past year.

ARC relies on the individual user to keep their information current.

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

Yes, the data elements are described in detail and well documented. Oracle produces manuals that cover the data elements.

Attributes of the Data

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designated?**

   Yes. This data is collected and maintained to assure the orderly processing of financial management actions within the Bureau 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, and how will this be maintained and filed?**

   No.

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

   Not applicable.

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

   Not applicable.

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

   Not applicable.

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 Public Debt 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 Public Debt where as 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 Public Debt (Public Debt) Information Technology (IT) Security Rules of Behavior ensure that users are made aware of their security responsibilities before accessing Public Debt's IT resources. All users are required to read and sign these rules acknowledging their responsibilities in protecting Public Debt'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; therefore, this question is not applicable.

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.

Users will be restricted to data that is only required in 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. ARC maintains Oracle User Manuals that lists all data elements within the system. (The data elements are too numerous to list in this PIA.

9. What kinds 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 ARC 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 privilege 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.

The provisions of these user privileges are established and monitored by Customer Support Branch (CSB) personnel, thus ensuring a separation of duties between CSB and the Oracle database administrators, who are from a separate organization within Public Debt. Additionally, Oracle e-Business Suite is enabled with Oracle Workflow, which helps manage Public Debt's business rules and control requirements.

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?**

   The system is operated at only one location.

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

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

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?**

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

   Reports are maintained in accordance with National Archives and Records Administration retention schedules.

   The Records Management Section is responsible for ensuring Public Debt'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 Public Debt complies with the recordkeeping requirements issued by the Office of Management and Budget, the General Service Administration, the National Archives and Records Administration, and the National Institute of Standards and Technology. The procedures used to facilitate this process are documented on Public Debt's intranet.

4. **Is the system using technologies in ways that the bureau/office 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?**

   Not applicable.

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 Public Debt 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 kinds of information are 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 Public Debt where as 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 Public Debt (Public Debt) Information Technology (IT) Security Rules of Behavior ensure that users are made aware of their security responsibilities before accessing Public Debt's IT resources. All users are required to read and sign these rules acknowledging their responsibilities in protecting Public Debt's IT systems and data. Noncompliance with these rules may result in termination of access privileges, administrative actions, and/or criminal prosecution if warranted.

9. Under which Privacy Act SORN does the system operate? Provide number and name.

TREASURY .009, Treasury Financial Management Systems—Treasury

10. If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

The system is not being modified, therefore this is not applicable.

Access to Data

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

   1. System Administrators.
   2. Data Base Administrators.
   3. Oracle e-Business Suite Support Staff.
   4. End Users.

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. 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, PD F 5409-1 E, *Administrative Resource Center (ARC) System Access Form - End User Applications,* is used to request access to "need-to-have" applications. The PD F 5409-1 E is 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 Public Debt where as 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? (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 Public Debt where as 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.

Information Technology (IT) Security Rules of Behavior (ROB) have been provided to all franchise customers. Access Request forms must be submitted to ARC 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.

Information Technology (IT) Security ROB have been reviewed and signed by each Public Debt employee. The IT Security ROB state that employees should:

1. Not read, alter, insert, copy, or delete any Public Debt 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 Public Debt 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.

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. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, was Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?**

   The Oracle e-Business Suite is a Commercial Off-The-Shelf (COTS) product and is in the Operational and Maintenance Phase of the life cycle. No contractors are involved in the maintenance of the system.

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

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

7. **Who will be 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 Bureau CIO have the responsibility to see that the data is protected from all threats.

8. **Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?**

   Yes. Customer agencies will have access to the data in the Oracle e-Business Suite. Department of Defense and Federal payroll providers share data with the system.

9. **How will the data be used by the other agency?**

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

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

Employees who have access to the system, the system manager, system owner and ultimately the Bureau CIO are responsible for assuring the proper use of data in the system.

The National Institute of Standards and Technology (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 Public Debt Disclosure Officer is responsible for administering requests for system data submitted to Public Debt involving the Privacy Act. Public Debt fully complies with the provisions of the Freedom of Information Act (FOIA), Title 5 U.S.C. Section 552, and the Privacy Act, Title 5 U.S.C Section 552a. Public Debt provides an established procedure to solicit requests to review and correct information recorded, and we have a dedicated Disclosure Officer who manages and administers the program.