Privacy Impact Assessment
of
Oracle Financials

Program or application name:

Oracle Financials

System Owner:

Board of Governors of the Federal Reserve System's ("Board") Management Division

Contact information:

System Owner:	Bill Mitchell
Organization:	Management Division
Address:	1850 K Street, NW Washington, D.C. 20551
Telephone:	202-973-5012

IT System Manager:	Reginald Roach
Organization:	Management Division
Address:	1850 K Street, NW Washington, D.C. 20551
Telephone:	202-452-5260

Description of the IT system:

Oracle Financials (Oracle) is an IT system designed to maintain financial information for the Board of Governors of the Federal Reserve System (Board) and the Federal Financial Institutions Examination Council (FFIEC). Oracle consists of separate modules that each performs one of the following functions: Accounts

Payable, Accounts Receivable, Cash Management, Fixed Assets, General Ledger and Purchasing.

1. The information concerning individuals that is being collected and/or maintained:

Oracle collects and maintains the following personally identifiable information concerning individual vendors, scholars and contractors:

a. Name;
b. Tax identification number or social security number;
c. Personal address and/or vendor address;
d. Phone number(s);
e. Financial institution account number; and
f. Financial institution routing number.

2. Source(s) of each category of information listed in item 1.

The personal information collected and maintained in Oracle is provided by an individual and/or an organization's employee.

3. Purposes for which the information is being collected.

The personal information collected and maintained in Oracle is used to assist Board staff in preparing invoices, IRS Form-1099's, and payments to the individuals.

4. Who will have access to the information?

Access to the personal information in Oracle is limited to authorized Board employees and contractors who have a need for the information for official business purposes. In addition, all information in the system may be disclosed for enforcement, statutory, and regulatory purposes; to another agency or a Federal Reserve Bank; to a member of Congress; to the Department of Justice, a court, an adjudicative body or administrative tribunal, or a party in litigation; to Federal, state, local and professional licensing boards; to the EEOC, the Merit Systems Protection Board, the Office of Government Ethics, and the Office of Special Counsel, to contractors, agents, and others; to labor relations panels; and where security or confidentiality has been compromised. Records may also be used to disclose information to the following:

a. to the Office of Child Support Enforcement of the United States Department of Health and Human Services, for use in locating individuals, verifying Social Security Numbers, and identifying their income sources to establish paternity, establishing and modifying orders of child support, identifying sources of income, and for other child support enforcement actions;
b. to appropriate federal and state agencies to provide required reports including data on unemployment insurance;
c. to the Social Security Administration to report FICA deductions;
d. to charitable institutions to report contributions;
e. to the Internal Revenue Service and to state, local, tribal, and territorial governments for tax purposes;
f. to the Office of Personnel Management in connection with programs administered by that office;
g. to an employee, agent, contractor, or administrator of any Board, Federal Reserve System, or federal government employee benefit or savings plan, any information necessary to carry out any function authorized under such plan, or to carry out the coordination or audit of such plan;
h. to officials of labor organizations recognized under applicable law, regulation, or policy when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions;
i. to a federal agency for the purpose of collecting a debt owed the federal government through administrative or salary offset or the offset of tax refunds;
j. to other federal agencies conducting computer matching programs to eliminate fraud and abuse and to detect unauthorized overpayments made to individuals; and
k. to verify for an entity preparing to make a mortgage or other loan to an employee the individual's employment status and salary, at the request of the individual

5. Whether the individuals to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses).

Individuals may elect not to submit personal information for submission into Oracle; however, that failure will result in the Board's inability to consider them for procurement purposes (e.g. contract bids). Individuals are otherwise required to submit personal information in order for the Board to process payments.

Individuals may write "Please pay by check" if they decline to provide banking information.

6. Procedure(s) for ensuring that the information maintained is accurate, complete, and up-to-date.

The individual vendor, scholar or contractor is responsible for the accuracy, completeness and timeliness of the information submitted in to Oracle. However, Oracle does provide data entry validation checks to ensure the information is entered correctly. Board staff does have the capability to update information if they become aware that an individual's information is incorrect or changes.

7. The length of time the data will be retained, and how will it be purged.

The information collected and maintained in Oracle is covered by General Records Schedule 6, Item 1, Accountable Officers' Files, and is maintained a minimum of 6 years and 3 months after the period covered by account. However, individual vendor information is inactivated if the vendor is not assigned a purchase requisition, purchase order, or invoice for 24 months. Users cannot apply inactive vendor information to an active invoice, purchase requisition, or purchase order.

8. The administrative and technological procedures used to secure the information against unauthorized access.

Access to Oracle is restricted to authorized employees and contractors within the Board who require access for official business purposes. Board users are classified into different roles and common access and usage rights are established for each role. User roles are used to delineate between the different types of access requirements. Periodic audits and reviews are conducted to determine whether authenticated users still require access and whether there have been any unauthorized changes in any information maintained in Oracle.

9. Whether a new system of records under the Privacy Act will be created. (If the data is retrieved by name, unique number, or other identifier assigned to an individual, then a Privacy Act system of records may be created).

Oracle is covered by an existing Privacy Act system of records notice, BGFRS-9, Supplier Files.

Reviewed:

Raymond Romero ***/signed/***	03/11/2013
Chief Privacy Officer	Date
Sharon Mowry ***/signed/***	03/11/2013
Chief Information Officer	Date