Department of the Interior
Privacy Impact Assessment

January 4, 2013

Name of Project: **Oracle Federal Financials**

Bureau: **Office of the Secretary**

Project's Unique ID (Exhibit 300): 010-000000392

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

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI 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.

A. CONTACT INFORMATION:

Departmental Privacy Office

Office of the Chief Information Officer

U.S. Department of the Interior

202-208-1605

DOI_Privacy@ios.doi.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) **Does this system contain any information about individuals** *{this question is applicable to the system and any minor applications covered under this system}*?

Yes.

a. **Is this information identifiable to the individual**[1] *{this question is applicable to the system and any minor applications covered under this system}*? (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, Sections C through F

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

can be marked not applicable. If YES complete all sections for system and any applicable minor applications).

Yes. The system contains personal information such as:

- Employee name, home address, telephone number, and personal email address.
- Employee financial information such as bank routing and account numbers, and debit and credit card numbers.
- Employee social security numbers.
- Personal transactional data such as travel expenses for business related trips and government small purchase card data.

b. Is the information about individual members of the public *{this question is applicable to the system and any minor applications covered under this system}*? (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Yes. Although the individuals covered by the system are Federal employees, upon retiring or leaving Government service these individuals become members of the public. In most cases, data related to an employee will remain in the system for a period of time after employment terminates.

c. Is the information about employees *{this question is applicable to the system and any minor applications covered under this system}*? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes, as discussed above, the system contains information about employees.

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

Oracle Federal Financials (OFF) will be used by the Department of the Interior's Interior Business Center (IBC) to provide U.S. Federal Government Agency clients with a suite of customized Oracle financial management modules that support functions including purchasing, procurement, accounts payable, fixed asset inventory and accounts receivable.

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

The Office of Management and Budget Circular A-127, Policies and Standards for Financial Management Systems authorizes the purchase or development of this system/application. This Circular is issued pursuant to the Chief Financial Officers Act (CFOs Act) of 1990, P.L. 101-576 and the Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.); and 31 U.S.C. Chapter 11.

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

- Federal employees of agencies that are IBC OFF clients, including employees who travel on work-related trips and require reimbursement of travel expenses and those that have travel/small purchase government bank cards.
- Employees of suppliers who provide services to IBC OFF clients, such as credit card and travel services vendors.

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?

All employee personal information is initially obtained from the employees and is provided to IBC by the agency clients. Individual information for vendor employees is provided by the vendors to IBC's OFF clients, who either enter the data into the OFF system directly or provide the information to IBC.

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

IBC has a variety of Federal agency clients for the OFF system. The precise client list changes over time. A current client list can be obtained by contacting the Program Manager listed above in section A(3). Otherwise, no data is being provided by Federal agencies for use in the system.

c. What Tribal, State and local agencies are providing data for use in the system?

No tribal, state or local agencies are providing data for use in the system.

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

Except for the vendors identified above in C(1), data is not being collected from any third parties.

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

See section B(1) above.

3) Accuracy, Timeliness, and Reliability

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

Data accuracy is verified by the receipt or non-receipt of travel reimbursements on the part of the Federal employee, through Budget office and supervisory review for correct organizational and cost accounts, and through supervisory review of bank card charges.

IBC OFF clients using the OFF system are responsible for the accuracy of the data they provide for use in the system.

b. How will data be checked for completeness?

Data completeness is verified by the receipt or non-receipt of travel reimbursements on the part of the Federal employee, through Budget office and supervisory review for correct organizational and cost accounts, and through supervisory review of bank card charges.

IBC OFF clients using the OFF system are responsible for the completeness of the data they provide for use in the system.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

Data currency is ensured by the receipt or non-receipt of travel reimbursements on the part of the Federal employee, through Budget office and supervisory review for correct organizational and cost accounts, and through supervisory review of bank card charges.

IBC OFF clients using the OFF system are responsible for the currency of the data they provide for use in the system.

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

The data elements that reside in the Oracle Federal Financials database are described in the written systems documentation provided by the system vendor, Oracle.

D. ATTRIBUTES OF THE DATA:

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

The data is relevant and necessary to:

- Identify and reimburse Federal travelers with electronic funds transfers or Treasury checks,
- Relate purchases and travel expenses on bank card bills to Federal employees with government bank card authority, and
- Issue payments to suppliers.

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, the system will not derive new data or create previously unavailable data about an individual.

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

Not applicable – the system will not derive new data or create previously unavailable data about an individual.

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

Not applicable – the system will not derive new data or create previously unavailable data about an individual.

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

Not applicable – the system will not derive new data or create previously unavailable data about an individual.

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

Not applicable – the system will not consolidate data.

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

Not applicable – 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.**

The selection of identifiers that will be used to retrieve information on the individual can vary depending upon the report or query. Some of the personal identifiers used to retrieve information on the individual are:

- employee name
- social security number
- government travel/small purchase bank card number

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

Active Users Report - Shows a list of Oracle application users who have not been end dated. *Accessible by system and security administrators.*

Unsuccessful Login User Report - Shows a list of Oracle application users failed attempts to log into the application. *Accessible by system and security administrators.*

IBC User Responsibility Report - A custom report showing a list of Oracle application user accounts and the active responsibilities to which they have access. *Accessible by system and security administrators.*

Active Responsibilities Report - Shows a list of Oracle application responsibilities and start dates. *Accessible by system and security administrators.*

Suppliers Report - Shows electronic banking information for federal employees. Those Federal travelers who do not have such data in the system must be reimbursed for their travel expenses with hard copy checks, which are more expensive than electronic funds transfers. The report can be used to reduce the number of hard copy checks, and thus the cost, associated with reimbursing Federal travelers. *Accessible by authorized finance office staff.*

Supplier Tax Identification Number Listing - A report by supplier name, number, type, and the supplier's taxpayer ID number. *Accessible by authorized finance office staff.*

Identify Federal Employees - A report by customer name and number, SSN, and Bill to Address. Selected finance office staff would have access to the report.

Active Employee Listing - A report listing all active employees by employee number and name. *Accessible by authorized finance office staff.*

New Vendor Letter - A report listing vendor name, site, and address. *Accessible by authorized finance office staff.*

Supplier Payment History - Shows all payments made to employees and separates charge card expenses from those that are paid directly to the employee. *Accessible by authorized finance office staff.*

Supplier Paid Invoice History - A report by employee supplier type to review payment history, discounts taken, and frequency of partial payments. *Accessible by authorized finance office staff.*

Aging - 7 Buckets Report - Shows outstanding receivable balances for the customer (i.e., employee) to ensure that all employee debts are being paid in a timely manner. *Accessible by authorized finance office staff.*

Suppliers Deactivation Report - A report by supplier name and number which shows supplier sites with no activity from a selected date and supplier sites which have been deactivated. *Accessible by authorized finance office staff.*

IBC Vendor Audit Report - A report identifying changes made to supplier and bank records and the individual making the change. *Accessible by authorized finance office staff.*

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.)

Disclosure of an individual's Social Security Account Number (SSN) is mandatory on vouchers claiming travel and/or relocation allowance expense reimbursement which is, or may be, taxable income.

Disclosure of the individual's SSN and other requested information is voluntary in all other instances; however, failure to provide the information (other than SSN) required supporting the claim may result in delay or loss of reimbursement.

Employees grant consent to the use of their personal information upon hire. New employees are given documentation disclosing and authorizing the uses of their personal information in their orientation packet.

Contractors grant consent upon signing a contractual agreement to perform services. Disclosures and authorizations are included in the contract documents.

E. 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 primary system location is IBC's General Purpose Computer Center in Denver but it is accessed for purposes of data entry and reporting by independent Federal agencies that are IBC clients. A backup system is located at a separate IBC facility in Reston, VA. All client data is centrally held to ensure consistency of data.

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

Each client agency storing dating in the system has its own NARA-approved records schedule for data retention.

Typically personal informational data on a Federal employee will stay in the system indefinitely unless deleted due to transfer, death, or retirement or until their travel/small purchase card is revoked. Personal transactional data may stay in the system (on-line or archived) for a number of years, whether the person is still a Federal employee or not.

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?

Each client agency storing data in the system has its own NARA-approved records schedule for the retention of its reports and data. Data is disposed of in accordance with client-agency approved data disposal procedures.

In general, retention and disposal proceeds as follows:

- Informational data (e.g. name, social security number, bank account info, purchase/travel card info, etc.) remains in the system indefinitely, with annual purges to remove employees whose employment or authority have been terminated. In addition, some clients perform an annual purge of employees who have not been the subject of a single system transaction within a certain period of time, usually between one and three years.

- Transactional data is retained for up to three years and then purged on an annual schedule. However, general journal data and selected electronic report copies may be retained indefinitely. Hard copy reports with Privacy Act information are shredded when the data is purged from the system.

4) Is the system using technologies in ways that the DOI 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 – the system is not using technology in ways that DOI has not previously employed.

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

No.

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

Not applicable – the system is not capable of monitoring individuals.

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

The records contained in the system are safeguarded in accordance with 43 CFR 2.51 and all other applicable security rules and policies. Paper records are maintained in locked file cabinets under the control of authorized personnel.

There are five available levels of electronic security to prevent unauthorized monitoring, which include network access security limits, operating system controls, application passwords, and application data group security levels.

Access to servers containing records in this system is limited to authorized personnel who have a need to know the information for the performance of their official duties and requires a valid username and password. Unique user identification and authentication, such as passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels.

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

Oracle Federal Financials System of Records Notice, OS-11, is expected to be published in the Federal Register in December, 2012. Portions of Oracle Federal Financials are also covered by GSA/GOVT-3, Travel Charge Card Program; GSA/GOVT-4, Contracted Travel Services Program; and GSA/GOVT-6, GSA SmartPay Purchase Charge Card Program.

In the event a client agency creates its own files or database outside of the OFF system using the agency's OFF records, the agency will be responsible for publishing its own Privacy Act system of records notice in the Federal Register to cover those records.

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

Not applicable – the system is not being modified.

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)**

System Administrators, System Managers, and Security Administrators, as well as authorized IT security personnel have access to the data in the system. Authorized contractors working on behalf of the System Administrators and Manager also have access to the data in the system.

A Data Custodian and selected finance office and budget office staff for each OFF client, as well as the immediate supervisors of Federal employees covered by the OFF system have access to the data.

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

A written request is received by the OFF Security Administrator from the clients' Data Custodian, IBC Project Manager, or IBC Accounting Operations Division's supervisor. The reason for the access, the type of data being accessed, and any restrictions on the access are stated on the request and reviewed by the application Security Administrator.

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

User access is typically restricted to selected data based upon need. Selected finance office staff members require access to the data to populate and maintain the independent agencies' suppliers (i.e., vendor) file. Supervisors of Federal travelers may require access to data on their immediate employees only for purposes of managing their travel program. Access is granted on the basis of least privileges, whereby users are granted the minimal amount of access needed to perform their job function.

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)**

The Security Administrators prevent unauthorized browsing by granting access only when there is a documented and justified management need, i.e. access is only granted to selected finance office staff members and immediate supervisors. Individuals with access receive applicable training and must sign and comply with DOI's internal Rules of Behavior prior to gaining access.

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?**

Contractors were involved in the design, development and implementation of the system and continue to assist with system maintenance. Privacy Act clauses were inserted in their contracts and all applicable regulatory measures have been addressed.

Contractor personnel are required to obtain appropriate clearances.

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

Yes. The Standard Interface Application (SIA), maintained by the Interior Business Center, Finance and Procurement Systems Division generates and transfers payroll, etravel data and other information between OFF and IBC's Federal Personnel and Payroll System (FFPS) for clients who utilize both systems. The SIA system resides within the hosted environment.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The System Administrators will ensure that only authorized personnel can access the OFF system by enforcing system access restrictions and reviewing audit reports to ensure compliance.

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

Except for IBC OFF clients, other agencies, as described above, other agencies will not share data or have access to the system.

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

Not applicable - except for IBC OFF clients, other agencies, as described above, other agencies will not share data or have access to the system.

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

The Chief Financial Officers and Data Custodians for each of IBC's clients will be responsible for the proper use of the data.