



US International Development Finance Corporation (DFC) Privacy Impact Assessment (PIA):

Office of Information Technology (OIT)
US International Development Finance Corporation (DFC)
1100 New York Ave, N.W.
Washington, DC 20527



Overview

| | |
|---|---|
| Date of Submission: | December 4, 2020 |
| Technical System Owner: | Eric DeCarli, Senior Director, Applications Development (OIT) |
| Business System Owner: | William Ellett, Director Government Financial Management (FM) |
| Department(s): | Office of the Chief Information Officer (OCIO) |
| Title of the System: | Oracle E-Business Suite (EBS) |
| Is this system or information collection new? | No, Existing system |

PIA Approval

I have reviewed the Oracle E-Business Suite (EBS) Privacy Impact Analysis and concur with the information presented below.

Senior Agency Official for Privacy (SAOP)

Date

EBS System Owner

Date

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The US International Development Finance Corporation (DFC) has been given the responsibility to mobilize and facilitate the participation of United States private capital and skills in the economic and social development of less developed countries and areas, and countries in transition from nonmarket to market economies.

One of the programs that helps DFC fulfill this mission is Oracle EBS (EBS), which is to function as the financial system of record for DFC.

The primary purpose of EBS is to function as the financial system of record for DFC. It is the primary application used by the Financial Management (FM) Department to record all financial transactions related to DFC's administrative and working capital budgets. DFC's FM unit is responsible for managing the agency's



portfolio in a prudent manner that is in keeping with best practices in the areas of accounting, budgeting, and management reporting. The FM unit also provides all other DFC departments with timely and accurate reporting on the size, health, and makeup of DFC's portfolio, geographic and sector concentrations, commitment and disbursement activity, credit funding usage, the status of departmental budget allocations, and corporate budget formulation and execution. Additionally, the FM unit provides information to other departments on subjects ranging from travel regulations to billing and payment procedures to interest rates.

Privacy management is an integral part of EBS. DFC's privacy management process is built upon a methodology that has been developed and implemented in leading companies around the country and globally. The methodology is designed to help ensure that DFC will have the information, tools, and technology necessary to manage privacy effectively and employ the highest level of fair information practices while allowing DFC to achieve its mission of enhancing the economic and social development of underdeveloped countries. The methodology is based upon the following:

- **Establish priority, authority, and responsibility:** Appointing a cross-functional privacy management team to ensure input from systems architecture, technology, security, legal, and other disciplines necessary to ensure that an effective privacy management program is developed.
- **Assess the current privacy environment:** This involves interviews with key individuals involved in the EBS system to ensure that privacy risks are identified and documented.
- **Organize the resources necessary for the project's goals:** Internal DFC resources, along with outside experts, are involved in reviewing the technology, data uses, and associated risks. They are also involved in developing the necessary redress systems and training programs.
- **Develop the policies, practices, and procedures:** The resources identified in the paragraph above work to develop an effective policy or policies, practices, and procedures to ensure compliance with fair information practices. The policies are designed to protect privacy effectively while allowing DFC to achieve its mission.
- **Implement the policies, practices, and procedures:** Once the policies, practices, and procedures are developed, they must be implemented. This involves training all individuals who will have access to and/or process PII. It also entails working with vendors to ensure that they maintain the highest standard for privacy while providing services to the DFC project.
- **Maintain policies, practices, and procedures:** Due to changes in technology, personnel, and other aspects of any program, effective privacy management requires that technology and information be available to the privacy management team to ensure that privacy policies, practices, and procedures continue to reflect actual practices. Regular monitoring of compliance with privacy policies, practices, and procedures is required.
- **Manage exceptions and/or problems with the policies, practices, and procedures:** This step involves the development and implementation of an effective redress and audit system to ensure that any complaints are effectively addressed, and corrections made, if necessary.

General Information Collected

Personally identifiable records that are collected and stored in the system consist of individual or company names, points of contact, mailing addresses, remittance addresses, telephone numbers,



contract/award numbers, email addresses, TIN, Social Security Numbers (SSN), Data Universal Numbering System (DUNS) numbers, and bank account information including routing numbers, account numbers, Society for Worldwide Interbank Financial Telecommunication (SWIFT) codes, International Bank Account Numbers (IBAN), and account titles.

This information breaks down into the following general classes, based on DFC's relationship with the outside party:

- **Vendor Data:** This is limited to vendor or contractors conducting business with DFC and includes company name, point of contact, mailing address, remittance address, telephone number, contract/award number, email address, tax identification number (TIN) [which could be a SSN in the case of sole proprietors set up as individuals], banking data (see below) and DUNS number
- **Employee Data:** This is limited to DFC employees and includes employee name and bank account information for reimbursement. In addition, social security numbers may be collected for the purpose of tax reporting.
- **Customer Data:** This is limited to customers conducting business with DFC and includes company name, point of contact, mailing address, remittance address, telephone number, contract/award number, email address, tax identification number (TIN) and DUNS number.
- **Financial and other Banking Data:** This includes bank routing transit number, bank account number, and credit card number for all DFC purchase card, travel card, and fleet card holders.

1.2 What are the sources of the information in the system?

The information maintained in EBS is primarily received from other systems either via direct system interface or manual entry into EBS. Sources for each category of information include:

- **Vendor Data** is sourced from System for Award Management (SAM): The U.S. Government's official vendor portal where vendors self-maintain their business information. Vendor data in interfaced SAM system via an automated interface. Vendor information flows only from SAM to EBS.
- **Employee Data:** Employee data is manually collected directly from employees and entered into EBS. This data is interfaced to the US Treasury to make payments, and used for tax reporting to Federal and State tax agencies.
- **Customer Data:** Insight is DFC's back office software that collects data from external customers via the DFC Forms portal. Occasionally, a customer may directly provide or clarify information via a DFC finance officer.

1.3 Why is the information being collected, used, disseminated, or maintained?

- **Vendor Data** is used to issue awards acquisition awards, pay vendors, and report tax information to state and federal tax agencies (e.g. 1099s).
- **Employee Data:** Employee data is used for expense reimbursement, payroll processing and tax reporting to Federal and State tax agencies.



- Customer Data is used to evaluate customer finance, insurance, and equity applications, and to make these disbursements.

1.4 How is the information collected?

- Insight collects information either through self-entry by customers through the DFC Forms system, or manual entry by a Finance Officer in collaboration with the customer.
- EBS Vendor data is interfaced from the SAM vendor portal where vendors self-maintain their business information. Employee information is collected directly from the employee and manually entered into the system.

1.5 How will the information be checked for accuracy?

EBS receives data through automated interfaces and using manual entry. Systems external to EBS generally gather the information directly from agencies, vendors, and other commercial providers, and as such are considered to be accurate. In addition, EBS has various internal controls and procedures to ensure the data accuracy. For instance, the majority of data in EBS is received through automated system interfaces; the built-in system edits and configuration increases data accuracy by minimizing data entry errors. Before uploading to EBS, the source data is also automatically evaluated for errors (e.g., file format, duplicate records, incorrect financial data), and if errors are found, EBS will not accept the record(s) and will generate an error log that must be reviewed and reconciled by a user in consultation with the source system or provider. Once reconciled, the record is re-submitted to EBS as part of the next automated transmission.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

- Electronic payments are required under Federal Acquisition Regulation 52.232-25, which requires electronic payments where applicable. Electronic payments require a TIN data element.
- W-2 reporting is covered under Title 26 of the United States Code (26 U.S.C.). W-2 reporting requires the TIN data element.
- 31 U.S.C., Subtitle III, which describes the Federal financial management requirements and responsibilities to record accounting activities related to debt, deposits, collections, payments, and claims and to ensure effective control over, and accountability for, assets for which the agency is responsible.
- There are federal financial mandates and legal authorities that govern financial management systems support the collection of the information in EBS. These include The Chief Financial Officers Act of 1990, Public Law 101-576, and the Federal Financial Management Improvement Act (FFMIA) of 1996, Public Law 104-208, as well as guidance issued by the Office of Management and Budget: OMB Circular A-123 Management's Responsibility for Internal Control; OMB Memorandum 16-11, Improving Administrative Functions Through Shared Services (May 2016); and OMB Memorandum 13-08, Improving Financial Systems Through Shared Services.



Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Vendor data is used to award procurement actions; and pay vendors and service customers for support of DFC's mission and the resulting required federal reporting. In addition, vendor data is compared to the Federal Do Not Pay registry to validate payments.

Employee data is used to pay employees, reimburse business expenses, and report to state and federal tax agencies.

2.2 What types of tools are used to analyze data and what type of data may be produced?

EBS end-users have the ability to query and analyze information within the financial system. A variety of standard financial reports are available to monitor and detect differences or anomalies.

2.3 If the system uses commercial or publicly available data, explain why and how it is used. This response should explain the following:

While EBS does not integrate publicly available information from commercial sources, it does receive data from commercial sources available to the general public. For example, the SAM portal is used by staff within OPM's acquisition organization to manually search and gather contractor/vendor information. The SAM database is available for the public to search; however, acquisition professionals have privileged access to SAM in order to gather additional contractor/vendor information in SAM that is not made available to the public (e.g., DUNS number, TIN, or information not made public by the vendor). OPM's acquisition staff also uses SAM to verify the contractor/vendor is in good standing with the Federal Government. The contractor/vendor information is interfaced daily to EBS to add new or updated vendor information to support OPM contract awards, obligations, and expenditures for contractors/vendors that provide services to OPM. This information is used when generating payments for services rendered and transmitting required information to Treasury for tax purposes (e.g., 1099-INT and 1099-MISC forms).



Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

- **Vendor Data:** This is limited to vendor or contractors conducting business with DFC and includes company name, point of contact, mailing address, remittance address, telephone number, contract/award number, email address, tax identification number (TIN) [which could be a SSN in the case of sole proprietors set up as individuals], and DUNS number.
- **Employee Data:** This is limited to DFC employees and includes employee name and bank account information.
- **Customer Data:** This is limited to Federal agencies and private entities and includes customer name, treasury account symbol, agency location code, and trading partner.
- **Financial and other Banking Data:** This includes bank routing transit number, bank account number, and credit card number for all DFC purchase card, travel card, and fleet card holders.

3.2 How long is information retained?

Data in EBS and Insight is stored indefinitely.

3.3 Has the retention schedule been approved by the DFC records officer and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Under the National Archives and Records Administration General Records Schedule 1.1 and the item numbers set forth in Section 1.4, the information used to enter data into EBS is maintained for 7 years. Data in EBS is stored indefinitely.

Section 4. Internal Sharing and Disclosure

The following questions are intended to define the scope of information sharing within DFC.

4.1 With which internal organizations is information shared? What information is shared, and for what purpose?

Information in EBS is shared among all departmental groups in DFC to conduct day to day operations. All DFC departments that use EBS have access to the discrete functionality that supports their organization with assigned user roles and responsibilities.



4.2 How is the information transmitted or disclosed?

- The sharing described above is compatible with the original purpose for which the information was collected, namely, to perform financial management functions within EBS to support DFC business operations.

Section 5. External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DFC, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations is information shared? What information is shared, and for what purpose?

DFC shares information maintained in EBS outside of DFC with the Department of Treasury, the General Services Administration, and Financial Institutions.

EBS shares information with the Department of Treasury Financial Management Service (FMS) to facilitate payment disbursements to contractors/vendor, employees, and other Federal customers. Information shared with FMS is transmitted electronically via a direct upload to Treasury's SPS system. Transmission of data to Treasury via SPS is protected using public key infrastructure (PKI) encryption. The information includes the payee's name, address, TIN (when applicable), and bank account information, and is shared at the time the disbursements are submitted to Treasury for execution. Treasury uses the information provided to issue federal payments on behalf of DFC in the form of a paper check or EFT transaction.

As required on an annual basis, DFC shares financial information maintained in EBS with the Internal Revenue Service (IRS) to report payments issued to vendors/contractors for services rendered to DFC. This includes interest payments distributed to obligors (IRS Form 1099). This information includes vendor or individual's name, address, TIN (when applicable), and amounts paid and withheld. This information is shared with the IRS to support the federal income tax processing and in accordance with the Internal Revenue Code and IRS regulations.

DFC also shares information on debts with Treasury pursuant to the Debt Collection Improvement Act of 1996. The information shared could relate to all categories of individuals for whom financial transactions are processed as well as all categories of information maintained in EBS. The information shared could or does include name, vendor or individual's name, address, TIN (when applicable), and debt amount (e.g., unpaid amount, overpayment amount).

EBS has external connections with GSA systems to collect business-related data for vendors who provide goods and services to the Federal government. Data collected for this purpose company name, point of contact, mailing address, remittance address, telephone number, contract/award number, email address, tax identification number (TIN) [which could be a SSN in the case of sole proprietors set up as individuals], and DUNS number.



EBS also share bank account and routing information with external financial institution for merchant card processing, and other credit card processes and payments.

5.2 Is the sharing of information outside the agency compatible with the original collection?

Yes, based on 1.6, the sharing described above is compatible with the original purpose for which the information was collected, namely, to perform financial management functions within EBS to support DFC business operations.

5.2.1 If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of DFC.

Yes, DFC has a SORN for Oracle EBS.

5.3 How is the information shared outside the agency and what security measures safeguard its transmission?

EBS shares information with the Department of Treasury Financial Management Service (FMS) to facilitate payment disbursements to contractors/vendor, employees, and other Federal customers. Information shared with FMS is transmitted electronically via a direct upload to Treasury's SPS system. Transmission of data to Treasury via SPS is protected using public key infrastructure (PKI) encryption.

As required on an annual basis, DFC shares financial information maintained in EBS with the Internal Revenue Service (IRS) to report payments issued to vendors/contractors for services rendered to DFC. This includes interest payments distributed to obligors (IRS Form 1099). This information is uploaded through the IRS's Filing Information Returns Electronically (FIRE) system.

EBS has external connections with GSA systems to collect business-related data for vendors who provide goods and services to the Federal government. EBS utilizes web services provided by GSA's system, Federal Procurement Data System - Next Generation (FPDS-NG), to transmit this data.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information?

EBS does not generally collect information directly from individuals. Rather, it compiles information from several other sources that may collect information directly from individuals. Those systems that collect information directly from individuals are responsible for providing notice at the time of



collection. EBS does not provide notice directly to individuals to inform them of the collection, maintenance.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

Since information in EBS is primarily received from other sources, individuals do not have the option to consent to particular uses of their information once transmitted to EBS. Once collected, their information is used for the purposes described in response to Question 1.6 of this PIA. If consent is required, notification of use of PII was previously established in external/interface source system and distributed the individual.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No, DFC is mandated, as noted in section 1.6 of this PIA, to share information in a specified method

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

DFC customers can contact the Finance Officer or Monitoring Officer who handles their loan(s) to access their information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

DFC customers can contact the Finance Officer or Monitoring Officer who handles their loan(s) to access their information.

Employees and members of the Finance department collaborate to update missing or changed Employee information.

7.3 How are individuals notified of the procedures for correcting their information?

Loan customers are made aware of how to correct their information as they are completing the loan package. For vendors that are not maintained in SAM, they are notified through contractual procedures.



7.4 If no formal redress is provided, what alternatives are available to the individual?

Loan customers may contact their account representative to update their information. For vendors that are not maintained in SAM, they may contact the DFC Contracting Officer for their contract.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Each user account is assigned specific roles with a defined set of privileges to ensure overall system integrity. The EBS system administrator can elect to assign all the privileges for a given role or can select only certain privileges to assign. Access is limited to DFC employees who have a need to access the system based on their roles in support of financial administration and management operations at DFC. To gain access to EBS, users must submit an online request for system access. The roles and privileges assigned to a particular user are predetermined depending on the user's function.

EBS PII access privileges is limited to the following roles:

| Role | Access | Safeguards |
|---|---|--|
| Payables Manager | Capability enter and update taxpayer ID | Director Government Systems/Systems and Accounting account access approvals. |
| Purchasing Super User | Capability enter and update taxpayer ID | Director Government Systems/Systems and Accounting account access approvals. |
| Site Administrator | Capability enter and update taxpayer ID | Director Government Systems/Systems and Accounting account access approvals. |
| CLM Purchasing Contracting Professional | Read only access to taxpayer ID | Director Government Systems/Systems and Accounting account access approvals. |

There are no users from other agencies that have access to EBS.



8.2 Will DFC contractors have access to the system?

DFC contractors do have access to EBS to perform operations and maintenance duties on the system. Their duties do not entail the maintenance of PII data. All system access requests are approved by key users from both the technical and functional system owners (e.g. IT and Finance) prior to application access being granted. MyForms is the DFC-wide standard application to request and approve application access.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

DFC offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

8.4 Has A&A been completed for the system?

Yes, EBS has an Information System Security Plan (SSP) which was last updated in April 10, 2020. A full Security Assessment and Authorization review of EBS was conducted to ensure the proper security controls and protocols were in place. The EBS application was granted an Authority to Operate (ATO) in September 2016.