Office of Information Technology (OIT)

Privacy Impact Assessment

Oracle E-Business Suite (EBS)

February 1, 2023

1100 New York Ave NW
Washington, DC 20527

Overview

The U.S. 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 E-Business Suite (EBS).

The primary purpose of EBS is to function as the financial system of record for DFC. It is the primary application used by the Office of Finance & Portfolio Management (OFPM) Financial Management (FM) unit 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. This PIA is being conducted because EBS collects, maintains, or disseminates information in identifiable form from or about members of the public and contains sensitive PII.

The PII collected by EBS breaks down into the following general classes:

- 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, Taxpayer Identification Number (TIN), banking data (see below) and Data Universal Numbering System (DUNS) number.
- Employee Data: This is limited to DFC employees and includes employee name and bank account information for reimbursement of business and travel expenses.
- Customer Data: This is limited to customers (i.e., organizations) conducting business with DFC and includes company name, point of contact, mailing address, remittance address, telephone number, contract/award number, email address, TIN, and DUNS number. However, most of the time, the contact information is traced to an organization and not to an individual and therefore would not constitute PII.

Section 1. Characterization of the Personally Identifiable Information (PII)

The following questions are intended to define the scope of the PII 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 PII is collected, used, disseminated, or maintained by the system? Indicate all that apply.

☒ Name
☐ Social Security Number (SSN)
☐ Date of Birth
☐ Place of Birth
☐ Driver's License
☐ Race/Ethnicity
☐ Passport Number
☒ Personal Bank Account Number
☒ Business Bank Account Number

☐ Gender
☐ Religion
☐ Security Clearance
☐ Personal Phone Number
☒ Business Phone Number
☐ Personal Email Address
☒ Business Email Address
☐ Personal Mailing Address
☒ Business Mailing Address
☐ Spouse Information
☐ ID Number
☒ Financial Information
☐ Group Affiliation
☐ Medical Information
☐ Mother's Maiden Name
☐ Marital Status
☐ Disability Information
☐ Biometrics
☐ Fax Number
☐ Health Plan Number
☐ Civil or Criminal History
☐ Alien Registration Number
☐ Photograph
☐ Credit Card Number
☐ Child or Dependent Information
☐ Other Names Used
☐ Law Enforcement
☐ Employment Information
☐ Truncated SSN
☐ Education Information
☐ Military Status/Service
☐ Legal Status
☐ Emergency Contact
☐ Internet Protocol (IP) Address
☐ Account Password
☐ Citizenship or Immigration Status
☐ Retirement Information
☒ Taxpayer Identification Number (TIN)

☒ Other: Data Universal Numbering System (DUNS) Number, Society for Worldwide Interbank Financial Telecommunications (SWIFT) Code, International Bank Account Number (IBAN), Company Name, Remittance Address, Contract/Award Number, Routing Number, Account Title

1.2 What are the sources of the PII 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: The System for Award Management (SAM). SAM is the U.S. Government's official vendor portal where vendors self-maintain their business information. EBS is integrated with SAM via an automated interface. Vendor information flows only from SAM to EBS.
- Employee Data:
  - E2 Solutions. E2 Solutions is a web-based end-to-end travel and expense management tool that offers a convenient way and user-friendly way to create and track travel authorizations, get approvals, submit vouchers, receive reimbursements, and book travel reservations. Travel voucher and travel authorization information are collected by EBS.
  - Employee bank account numbers are manually collected directly from employees. The FM unit collects this information over phone call. This data is interfaced to the U.S. Department of the Treasury (Treasury) in EBS to reimburse employees for travel expenses.
- Customer Data: Insight. 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 PII being collected, used, disseminated, or maintained?

- Vendor Data: Is used to issue acquisition awards, pay vendors, and report tax information to federal and state tax agencies (e.g., 1099s).

- Employee Data: Is used for business and travel expense reimbursements, 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 disbursements.

1.4 How is the PII collected?

- Vendor Data: Is interfaced from the SAM vendor portal where vendors self-maintain their business information.
- Employee Data: Is collected directly from the employee and manually entered into the system.
- Customer Data: Is interfaced from Insight where information is sent to EBS, either through self-entry by customers through the DFC Forms system, or manual entry by a DFC finance officer in collaboration with the customer.

1.5 How will the PII 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's accuracy. For instance, the majority of data in EBS is received through automated system interfaces; the built-in data verification system 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 with the source system or provider. Once reconciled, the record is re-submitted to EBS as part of the next automated transmission.

1.6 If the information is retrieved by a personal identifier, what System of Records Notice (SORN) applies to the information. If a SORN is not required, what specific legal authorities, arrangements, and agreements define the collection of PII?

- The System of Records Notice (SORN) that applies to the information in EBS is DFC-01: Oracle E-Business Suite (EBS), 85 FR 43210 (July 16, 2020).
- Electronic payments are required under Federal Acquisition Regulation 52.232-25, which requires electronic payments where applicable. Electronic payments require a TIN data element.
- 31 U.S.C. Subtitle III (Financial management) 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.
- 31 U.S. Code § 3332 (Required direct deposit) requires that all federal wage, salary, and retirement payments be paid to recipients of such payments by electronic funds transfer, unless another method has been determined by the Secretary of the Treasury to be appropriate.
- The Federal Credit Reform Act (FCRA) of 1990 requires agencies to measure the government's cost of federal credit programs over the length of a loan. This facilitates better cost comparisons between credit and noncredit programs. FCRA only applies to loans and loan guarantees made to non-federal borrowers.

- The Debt Collection Improvement Act of 1996 seeks to maximize collections of delinquent nontax debt owed to the federal government. The act also seeks to reduce losses by requiring proper screening of potential borrowers and information sharing within and among federal agencies.
- There are federal financial mandates and legal authorities that govern financial management systems and 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): OMB Circular No. A-123, *Management's Responsibility for Internal Control*; OMB Memorandum M-16-11, *Improving Administrative Functions Through Shared Services*; and OMB Memorandum M-13-08, *Improving Financial Systems Through Shared Services*.

1.7 Privacy Impact Analysis: Related to Characterization of the PII

Privacy Risk: There is a risk that more PII will be collected than is relevant and necessary.

Mitigation: This risk is partially mitigated. EBS only collects information that is necessary to process financial transactions as required by federal law. In addition, most of the PII collected in EBS is received directly from other systems (i.e., SAM, E2 Solutions, Insight), which limits the amount of PII that could be collected by the system.

Privacy Risk: There is a risk that the PII collected will be inaccurate or incomplete.

Mitigation: This risk is partially mitigated. Before uploading to EBS, the source data is 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 with the source system or provider. If that information is still not correct, a customer may directly provide or clarify information via a DFC finance officer.

Section 2. Uses of the PII

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

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

The FM unit is responsible for maintaining DFC's accounting and financial records. In addition to financial statements, government-mandated financial reporting, and the annual financial audit, FM is also responsible for payment of all vendor, government, payroll, and travel expenses; recording and applying all cash receipts; and administering Metro check/SmarTrip program benefits.

Vendor Data: Is used to award procurement actions, pay vendors, and service customers who complete work for DFC in support of the agency's mission. In addition, vendor data is compared to the Federal Do Not Pay registry to validate payments and prevent improper payment to entities or people who should not be paid. DFC also reports 1099s to the Internal Revenue Service (IRS).

Employee Data: Is used to reimburse employees for their business and travel expenses.

Customer Data: DFC retains financial data in EBS in order to support its financial modeling efforts and to comply with the FCRA. In addition, the financial data is used to respond to data calls from OMB, which in part helps to inform U.S. Presidents on what their focus for DFC will be during their respective administrations. No PII is disclosed from EBS as part of these data calls.

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. There are over 300 prebuilt financial key performance indicators (KPIs) to monitor business performance (e.g., profitability and loss, balance sheet, receivables, payables) and over 100 prebuilt procurement and spend KPIs (e.g., spend summary, supplier summary, off contract spending). Built-in graph analytics enable users to visualize relationships and connections between data entities. Analyses will only be conducted on the financial data for financial modeling purposes and not on individuals.

2.3 If the system uses commercial or publicly available data, explain why and how it is used.

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 DFC acquisition staff 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). DFC's acquisition staff also uses SAM to verify that the contractor/vendor is in good standing with the federal government. The contractor/vendor information interfaces daily to EBS to add new or updated vendor information to support DFC contract awards, obligations, and expenditures for contractors/vendors that provide services to DFC. This information is used when generating payments for services rendered and transmitting required information to the U.S. Department of the Treasury for tax purposes (e.g., 1099-INT and 1099-MISC forms).

2.4 Privacy Impact Analysis: Related to Uses of the PII

Privacy Risk: There is a risk that PII will be used inappropriately.

Mitigation: This risk is partially mitigated. EBS employs role-based access controls so that only authorized DFC personnel can view certain information in the system. A DFC employee or contractor must obtain approval from their supervisor and provide justification for their request before an EBS administrator will consider their access privileges. Additionally, all DFC personnel are required to take annual privacy awareness training and sign the DFC Privacy Rules of Behavior to attest that they will handle PII appropriately.

Section 3. Retention of PII

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

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

Records in EBS are maintained under the National Archives and Records Administration (NARA) General Records Schedule (GRS) 1.1 - Financial Management and Reporting Records, Item 010 - Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting.

3.2 For what reason is the PII retained?

The PII included in NARA GRS 1.1, Item 010, is maintained by accountable officers to account for the availability and status of public funds, and is retained to enable the Government Accountability Office, Office of Inspector General, or other authority to audit the system. Financial transaction records include those created in the course of procuring goods and services, paying bills, collecting debts, and accounting for all finance activity.

3.3 How long is the PII retained?

To limit the risk of harm to an individual that would occur from a breach, personal bank account numbers are only retained for 60 days after an employee has departed the agency. DFC retains all other financial data in EBS in order to support its financial modeling efforts and to respond to OMB data calls. Therefore, with the exception of personal bank account numbers, records are not purged from EBS due to their ongoing business use.

3.4 How is the PII disposed of at the end of the retention period?

Personal bank account numbers are manually deleted from EBS within 60 days after confirmation that all payments have been made to separated employees.

3.5 Privacy Impact Analysis: Related to Retention of PII

Privacy Risk: There is a risk that PII may be retained for a longer period than necessary.

Mitigation: This risk is partially mitigated. Personal bank account numbers are manually deleted from the system when they are no longer relevant and necessary, which is within 60 days assuming confirmation is received that there are no pending payments still to be paid to the separated employee. To comply with the FCRA and respond to OMB data calls, other financial records in EBS are never destroyed. However, any PII in these records is limited to business contact information.

Section 4. Internal Sharing and Disclosure

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

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

Information in EBS is shared among all departmental groups in DFC who are involved in financial operations. Most users of EBS are requisitioners, system accountants, or contracting staff responsible for operations and

maintenance of the system. All DFC departments that use EBS have access to the discrete functionality that supports their department. Access to PII is restricted on a need-to-know basis based on the duties of the user.

4.2 How is the PII transmitted or disclosed internally?

Access to PII is disclosed internally to DFC personnel in the system on a case-by-case basis in order to perform the financial operations needed for their respective departments. 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 privileges or certain privileges for a given role depending on the user's function.

4.3 Privacy Impact Analysis: Related to Internal Sharing and Disclosure

Privacy Risk: There is a risk that PII may be shared internally with individuals who do not have a need to know.

Mitigation: This risk is partially mitigated. Access to EBS is limited to DFC personnel who have a need to know to perform their official duties in support of the agency's financial operations. DFC personnel must submit an online request for system access and be approved by their supervisor before the EBS system administrator considers their application for access. Privileges are assigned to users on a case-by-case basis and are limited to only the information that is required for users to fulfill their role in support of DFC's financial administration and management operations.

Section 5. External Sharing and Disclosure

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

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

DFC shares PII maintained in EBS outside of DFC with the U.S. Department of the Treasury and the U.S. General Services Administration (GSA).

EBS shares PII with the U.S. Department of the Treasury's Financial Management Service to facilitate payment disbursements to contractors/vendors, employees, and other federal customers. The information shared includes the payee's name, business address, TIN (when applicable), and bank account information, and is shared at the time the disbursements are submitted to the Treasury for execution. The Treasury uses this information to issue federal payments on behalf of DFC in the form of a paper check or electronic funds transfer (EFT) transaction.

As required on an annual basis, DFC shares financial information maintained in EBS with the 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 the individual's name, vendor name, business address, TIN (when applicable), and amounts paid and withheld. This information is shared with the IRS to support federal income tax processing and in accordance with the Internal Revenue Code and IRS regulations.

DFC also shares information on debts with the U.S. 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 may include the individual's name, vendor name, business address, TIN (when applicable), and debt amount (e.g., unpaid amount, overpayment amount).

Lastly, EBS sends procurement data to the GSA Federal Procurement Data System-Next Generation (FPDS-NG). The FPDS-NG is the U.S. Government's repository for information on government contracts and includes information on organizations who have or had contracts with the federal government. The only PII involved in this sharing is the business email address of DFC officials involved in the procurement process. All other information is related to the terms of the contract and linked to an organization and not an individual.

5.2 Is the sharing of PII outside the agency compatible with the original purpose for the collection?

Yes, 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.

5.3 Is the external sharing 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 outside of DFC.

Yes, the external sharing described in Section 5.1 may be covered by one of the following routine uses in the DFC-01: Oracle E-Business Suite (EBS) SORN:

A. To the Department of Treasury for Administering the Do Not Pay Initiative under the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA). As required by IPERIA, the Bipartisan Budget Act of 2013, and the Federal Improper Payments Coordination Act of 2015 (FIPCA), records maintained in this system will be disclosed to (a) a Federal or state agency, its employees, agents (including contractors of its agents) or contractors; or, (b) a fiscal or financial agent designated by the Bureau of Fiscal Service or other Department of the Treasury bureau or office, including employees, agents, or contractors of such agent; or, (c) a contractor of the Bureau of Fiscal Service, for the purpose of identifying, preventing, and recovering improper payments to an applicant for, or recipient of, Federal funds. Records disclosed under this routine use may be used to conduct computerized comparison to identify, prevent, and recover improper payments, and to identify and mitigate fraud, waste, and abuse in federal payments.

J. Disclosure to Any Source from Which Additional Information Is Requested During the Acquisition and Procurement Contract Lifecycle Management Process. Information may be disclosed in connection with the requisitioning, commitments, obligations, invoicing, travel expense reimbursements, and reimbursements to employees for local travel expenses and other ancillary expenses.

K. Disclosure of Information in Connection with Business Transaction Activities to a Federal Agency. Information may be disclosed to the Treasury Department via electronic file to enable processing of business payment and payable commitments for the life of each business transaction.

L. Disclosure of Information in Connection with Business Transaction Activities to a Federal Agency. Information may be disclosed to a Federal agency in connection with initial due diligence processes in

assessing new business transaction proposals and as part of the improper payment risk mitigation process that occurs for the life of each business transaction.

M. Disclosure of Information to Another Federal Agency, a Court, or a Third Party. Information may be disclosed where the counterparty to a business transaction has not remitted agreed upon and contracted fees for an extended period of time.

5.4 How is the PII shared outside the agency and what security measures safeguard its transmission?

Information shared with the U.S. Department of the Treasury's Financial Management Service is transmitted electronically via a direct upload to the Treasury's Secure Payment System (SPS). Transmission of data to the 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 IRS to report payments issued to vendors/contractors for services rendered to DFC as well as for debt forgiveness for U.S.-based borrowers. This includes interest payments distributed to obligors (IRS Form 1099). This information is manually uploaded through the IRS's Filing Information Returns Electronically (FIRE) system and by manual paper-based reporting.

Lastly, EBS has an external connection to the FPDS-NG to securely push procurement data to GSA.

5.5 Privacy Impact Analysis: Related to External Sharing and Disclosure

Privacy Risk: There is a risk that PII may be shared externally with individuals who do not have a need to know.

Mitigation: This risk is partially mitigated. Information from EBS that is sent outside of the system is done so securely through the U.S. Department of the Treasury's SPS and IRS's FIRE systems. There are no users outside of DFC that have access to EBS. In addition, all DFC personnel must sign the annual DFC Privacy Rules of Behavior attesting that they will handle PII appropriately and are subject to disciplinary and criminal penalties for disclosing Privacy Act information to unauthorized persons.

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 PII?

EBS does not generally collect information directly from individuals. For the most part, 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.

For personal bank account numbers that are collected from DFC employees by the FM unit over the phone, a Privacy Act Statement is provided to the individual on the OFPM SharePoint site. The Privacy Act Statement is displayed below:

Privacy Act Statement

Authority: The collection of bank account numbers is authorized by 31 U.S. Code § 3332 (Required direct deposit), which states: "Notwithstanding any other provision of law, all Federal wage, salary, and retirement payments shall be paid to recipients of such payments by electronic funds transfer, unless another method has been determined by the Secretary of the Treasury to be appropriate."

Purpose: Bank account numbers are collected in order to allow DFC to initiate business and travel expense reimbursements for DFC employees. DFC accounting staff will have access to this information, as well as contracting staff responsible for the operations and maintenance of the Oracle E-Business Suite (EBS) system.

Routine Uses: This information is shared with the U.S. Department of the Treasury (Treasury) to issue federal payments on behalf of DFC in the form of an electronic funds transfer. This information is not shared with any other entity outside the agency except to the extent required by law or as necessary to represent the agency in litigation. Information on authorized routine uses may be found in the System of Records Notice: DFC-01: Oracle E-Business Suite (EBS), 85 FR 43210 (July 16, 2020).

Disclosure: Providing this information is voluntary; however, failure to provide a valid bank account number may delay receipt of payment as the Treasury will be required to send a paper check to your mailing address.

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

Employees have the right to decline to provide their bank account number, but by declining to provide this information, it may result in a delay of payment to them for their business and travel expense reimbursements because receipt of payment would have to be in the form of a paper check mailed from the U.S. Treasury instead of as a direct deposit into their bank account.

Since most other information in EBS is primarily received from other sources, individuals do not have the option to decline to provide PII. Once collected, their information is used for the purposes described in Section 1.3 of this PIA. If consent is required, notification of use of PII was previously established in the external/interface source system and distributed to the individual.

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

No, as noted in Section 1.6 of this PIA, DFC is mandated to use the PII in a specified manner to satisfy the agency's financial management requirements and responsibilities. The uses of PII are consistent with legal authorities, regulations, and other federal guidance.

6.4 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not be made aware of the uses of their information

Mitigation: This risk is partially mitigated. DFC provides notice to the public through this PIA and the SORN, which are publicly available on the Internet. In addition, DFC employees who provide their personal bank account number to the FM unit over the phone are directed to read the Privacy Act Statement on the OFPM SharePoint site.

Section 7. Access, Redress, and Correction

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

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

To make a Privacy Act request for records in a system of records, a requester may submit a written request to the Director of Human Resources Management, either by mail or delivery, to U.S. International Development Finance Corporation, 1100 New York Ave NW, Washington, DC 20527 or electronic mail to privacy@dfc.gov. Alternatively, a requester may address the request to the system managers that are provided in the SORN. The envelope or subject line should read "Privacy Act Request" to ensure proper routing. Individuals requesting access must comply with DFC's Privacy Act regulations regarding what information to include in the request and provide the proper verification of identity (22 CFR Part 707). To protect PII in transit, individuals should encrypt any sensitive PII sent to the agency over email or request to submit it to the agency through DFC's secure Box.com portal.

DFC customers can also contact the DFC 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?

To make a Privacy Act amendment request on records in a system of records, a requester may submit a written request to the Director of Human Resources Management, either by mail or delivery, to U.S. International Development Finance Corporation, 1100 New York Ave NW, Washington, DC 20527 or electronic mail to privacy@dfc.gov. Alternatively, a requester may address the request to the system managers that are provided in the SORN. The envelope or subject line should read "Privacy Act Request" to ensure proper routing. Individuals requesting amendment must comply with DFC's Privacy Act regulations regarding what information to include in the amendment request and provide the proper verification of identity (22 CFR Part 707). To protect PII in transit, individuals should encrypt any sensitive PII sent to the agency over email or request to submit it to the agency through DFC's secure Box.com portal.

DFC customers can also contact the DFC finance officer or monitoring officer who handles their loan(s) to request correction of inaccurate or erroneous information. Employees and members of the OFPM 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 whose information is not maintained in SAM, they are notified of the procedures through contractual procedures. In addition, this PIA, SORNs, and DFC's Privacy Act regulations provide notice to individuals on how to correct their information.

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

N/A; formal redress is provided through the Privacy Act request process.

7.5 Privacy Impact Analysis: Related to Access, Redress, and Correction

Privacy Risk: There is a risk that individuals will not be able to access or correct any information maintained on them by EBS.

Mitigation: This risk is partially mitigated. DFC's Privacy Act regulations provide instructions for individuals to request access or amendment of their records. If a bank account number needs to be corrected or updated in the system, an employee may reach out to the FM unit. External customers may directly provide or clarify information via a DFC finance officer. However, as the majority of data received by EBS is automatically transferred from external systems (i.e., SAM, E2 Solutions, Insight), individuals should reach out to the system managers for those systems to ensure that the source data is accurate.

Section 8. Technical Access and Security

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

8.1 How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password

☒ Firewall
☒ Encryption
☒ User Identification
☒ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy, and Records Management Training
☐ Other. *Describe*

8.2 Will DFC contractors have access to the system? If so, how frequently are contracts reviewed and by whom?

DFC contractors have access to EBS to perform operations and maintenance duties on the system. Their duties include access to PII, but they do not edit or modify PII in EBS. All system access requests are reviewed by approvers from both the technical and functional sides (i.e., Office of Information Technology and OFPM) prior to application access being granted.

During the official solicitation process, the Office of Administration includes the applicable Federal Acquisition Regulation privacy clauses and other privacy provisions into contracts, as appropriate, that outline roles, responsibilities, training, incident reporting, and other privacy requirements for contractors who have access to PII. Contracts are reviewed periodically by the Contracting Officer's Representative and Contracting Officer, at minimum during modifications, addition of new key personnel, and the annual contract option.

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

DFC offers annual privacy and information security awareness training, which instruct users on the need to protect agency data and provide best practices for handling sensitive PII.

8.4 Has Assessment and Authorization (A&A) been completed for the system?

Assessment and Authorization (A&A) has been completed for EBS by the Chief Information Security Officer (CISO) team. An authorization to operate (ATO) letter was signed by DFC and re-authorized in fiscal year 2023.

8.5 Privacy Impact Analysis: Related to Technical Access and Security

Privacy Risk: There is a risk that PII will not be properly secured.

Mitigation: This risk is partially mitigated. The DFC CISO team has conducted a full security assessment of EBS and authorized it to operate at a Moderate impact level, meaning it is approved to handle information containing PII and Controlled Unclassified Information. EBS is only accessible from inside the DFC network, so all users must have an active DFC network account. DFC has employed numerous cybersecurity tools to identify threats to the DFC network and to prevent data breaches from occurring. Transmission of data from EBS to external entities is only done through secure connections.