Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Oracle Federal Financials (OFF)
Bureau/Office: Interior Business Center
Date: October 8, 2019
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
    ☐ Members of the general public
    ☐ Federal personnel and/or Federal contractors
    ☐ Volunteers
    ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Oracle Federal Financials (OFF) system is a component of the Oracle eBusiness Suite that supports financial management, reimbursement, reporting and collection activities provided by the Department of the Interior (DOI) Interior Business Center (IBC) to Federal customer

agencies. OFF provides IBC clients with a web-based application that contains customizable financial management modules that combine to provide a comprehensive financial software package to support budgeting, purchasing, Federal procurement, accounts payable, fixed assets, general ledger, inventory, accounts receivable, reimbursement, reporting, and collection functions. The OFF system is hosted by IBC, however, each customer agency accesses and manages their own data within the system. Federal customer agencies utilize OFF to meet financial management obligations to manage funds, process reimbursements, and ensure accurate accounting for monies owed.

The OFF software was developed by the Oracle Corporation and configured to meet specific needs of the Federal financial community. The application supports all core accounting system requirements established by the Joint Financial Management Improvement Program (JFMIP). The application contains Oracle Discoverer/Oracle Business Intelligence Enterprise Edition (OBIEE) reporting tools that provide common reports as well as ad hoc querying capabilities. The application contains Oracle Discoverer, a reporting tool that provides common reports as well as ad hoc querying capabilities. The Oracle Business Intelligence Enterprise Edition (OBIEE) reporting tool was added to the application in October 2018. OBIEE provides the Top 15 common reports as well as ad hoc querying capabilities. Oracle Discoverer will be phased out by December 31, 2019 and completely replaced by OBIEE as the reporting tool.

IBC purchases OFF licenses on behalf of its customer agencies and each customer agency reimburses IBC for the licenses and software maintenance as part of an interagency agreement with IBC. IBC provides a pre-configured instance of OFF to its Federal customer agency that incorporates common Federal financial accounting practices. Typical implementations of OFF include the following core financials modules: General Ledger, Federal Administrator, Payables, Receivables, Assets, Inventory, Purchasing, and Contractor Lifecycle Management.

IBC has provided several enhancements to the core Oracle product in the form of application extensions. Some of these enhancements include interfaces and integration with eTravel applications, Federal payroll providers, credit card providers, and procurement applications. IBC's pre-configured model includes a standard interface application for integration of these external data sources. It also includes pre-defined transaction code values that are fully compliant and pre-populated with the Department of the Treasury's Standard General Ledger (SGL) accounts. The system transmits to and receives information from the Department of the Treasury pertaining to financial transactions undertaken by or on behalf of Federal agency customers.

This privacy impact assessment covers OFF, its components, reporting tools, and the OFF Production Copy (ProdCopy), which is a test environment that is implemented, as needed, for Customer Acceptance Testing purposes.

C. What is the legal authority?

5 U.S.C. 301, Departmental regulations; 31 U.S.C. 3512, Executive Agency Accounting and Other Financial Management Reports and Plans; 5 U.S.C. 4111, Acceptance of Contributions, Awards, and Other Payments; 5 U.S.C. 5514, Installment deduction for indebtedness to the

United States; 5 U.S.C. 5701, et seq. Travel And Subsistence Expenses, Mileage Allowances; 31 U.S.C. 3512, Executive agency accounting and other financial management reports and plans; 31 U.S.C. 3711, Collection and Compromise; and the Office of Management and Budget Circular A-123, Appendix D, Compliance with the Federal Financial Management Improvement Act.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-999991141, Oracle Federal Financials System Security Plan (SSP)

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

DOI records are maintained under DOI-91, Oracle Federal Financials (OFF), 80 FR 66551 (October 29, 2015). Some records may be covered under government-wide system of records notices GSA/GOVT-3, Travel Charge Card Program; GSA/GOVT-4, Contracted Travel Services Program; and GSA/GOVT-6, GSA SmartPay Purchase Charge Card Program. Government-wide and DOI notices may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn. Though IBC hosts OFF, the customer records in the system are under the ownership and control of IBC's Federal customer agencies and as such are maintained under the system of records notices published by those agencies for these financial management activities.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Gender
☒ Truncated SSN
☒ Financial Information
☒ Credit Card Number (only last 6 visible)
☒ Emergency Contact
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

Individual employee financial institution, bank account number and bank routing number are collected to perform customer agency remittance activity. PII may also include government travel credit card number; email (government, personal, or business addresses as provided by customer agency or individual); phone numbers (government, personal, or business numbers as provided by customer agency or individual); vendor identification (ID), which is a system generated identification number not identifiable to an individual; Tax Identification Number (TIN); Employee Identification Number (EIN); invoice or payment document number; transaction date; employee number; supplier name, number, and bank records; amounts owed; record of payments; and customer name and number. This system also contains records on corporations and business entities that are not subject to the Privacy Act, including company name, address and telephone number, TIN, DUNS number, and bank account and routing number. However, personal information related to individuals may be subject to the Privacy Act.

Both the IBC Federal Personnel Payroll System (FPPS) and U.S. Department of Agriculture National Finance Center (NFC) payroll report data are visible for use through the OFF information system, based on restricted responsibilities. The Federal customer agency can only see their data and only a limited number of client users have access to these restricted reports, as

commensurate with their job duties (e.g., under 50 users out of nearly 1,500 users, or approximately 3% of users). Those data elements are captured below.

OFF Payroll Report Data Elements based on date pulled from interface with the IBC FPPS information system:

- Federal Employees Health Benefit (FEHB) option, amount, and plan
- Federal Employees' Group Life Insurance (FEGLI) option and amount
- Federal Employees Retirement System (FERS) option
- Retirement information (e.g., retirement plan code, TSP Basic, amount and matching, 401K Basic, amount and matching)
- Last 4 of SSNs
- Gender - only available via payroll reports and viewable by authorized users
- Pay information (e.g., Amount, Pay Code, Plan, Grade, Pay Type, Shift Code, Hours, Base rate)
- Leave category

OFF Payroll Report Data Elements based on data pulled from interface with USDA National Finance Center (NFC) information system:

- SSN (last 4)
- Pay information (e.g., Gross amount, Hourly Rate, Pay Plan, Grade, Step, Hours)
- Type appointment
- Type employment

Each Federal customer agency accesses and manages their own data within the OFF system. This may include reports generated that contain information on individuals that are necessary to meet financial management obligations to manage funds, process reimbursements, and ensure accurate accounting for monies owed. Reports may also include other employment related data obtained from individuals or other systems as deemed necessary by each customer.

B. What is the source for the PII collected? Indicate all that apply.

☐ Individual
☒ Federal agency
☐ Tribal agency
☐ Local agency
☐ DOI records
☒ Third party source
☐ State agency
☒ Other: *Describe*

IBC hosts the OFF system and is responsible for system administration functions and other management functions in accordance with interagency agreements with Federal customer agencies. Each customer agency has control over its own data, accesses and manages its own

data, and is responsible for maintaining and protecting that data and for meeting the requirements of the Privacy Act and other laws, regulations, and policies. IBC does not collect PII directly from individuals on behalf of the customer agency for this system.

The information sources are external Federal customer agencies, sole proprietors and suppliers, and individuals' bank card companies. Information is also obtained from the General Services Administration System for Award Management (SAM) system, eTravel Systems (Government Travel Credit Card), government payroll providers, IBC for the Federal Personnel Payroll System (FPPS) and National Finance Center (NFC), and includes information such as new employee names, addresses, banking information changes for existing employees, and other payroll related data. All of the aforementioned sources collect and maintain their own data.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☐ Email
☐ Face-to-Face Contact
☒ Web site
☒ Fax
☐ Telephone Interview
☒ Information Shared Between Systems *Describe*
☒ Other: *Describe*

The information sources are customer agencies, sole proprietors and suppliers, and individual's bank card company. Information is collected through the Oracle Supplier Request Form submitted by customer agencies through secure fax transmission. Information is also obtained from SAM, eTravel Systems, FPPS and NFC through electronic interface. PII information is used for customer agency reimbursement, collection, financial management, and financial reporting activities. Authorized users access agency data through a Java-based application accessed through a secure internet URL. Customer agencies provide the IBC a range of Internet Protocol (IP) addresses for access to the OFF web address; however, customer agencies may only view and export data through this interconnection.

D. What is the intended use of the PII collected?

The PII is collected for the purpose of financial management for customer agencies to include:

- Identifying and reimbursing Federal employees and contractors on official travel with electronic funds transfers or Department of the Treasury checks;
- Relating purchases and travel expenses on bank card bills to Federal employees with government bank card authority;
- Collecting accounts receivable owed to OFF customers, and
- Issuing payments to suppliers.

PII is also used for limited testing and development purposes in the OFF ProdCopy where the PII is required for the testing to ensure integrity, validity and accuracy of the data and system

processes when there are changes in the system that utilize PII. ProdCopy is a procedure to use in any one of our test environments that requires the use of PII data; the PII data does not remain unscrambled on a permanent basis, only when data is required for testing to be completed. We only use PII required for testing, for example, testing SAM interface with live bank information. Once testing is completed, the data is scrambled.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

IBC uses the data to facilitate customer agency financial management and reimbursement activities. Finance and budget office staff and immediate supervisors of Federal employees and contractors on official travel may have access to the data. Accounting or financial operations staff, including employee, contractor, and immediate supervisors, may have access to the data to facilitate the payment of customer agency invoices. The Accounting Operations Vendor Maintenance team processes the data through the Oracle Supplier Request Form that is submitted by the customer agency. Customer agencies are responsible for managing their own PII related data.

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

PII data is shared with other Federal agencies for reimbursement and reporting purposes. This includes the Department of the Treasury in the form of electronic funds transfers, automated clearing houses, and manual check transactions. The vendor Internal Revenue Service (IRS) Form 1099, MISC Income, is also transmitted annually to the IRS. Any DOI disclosures are made in accordance with the published routine uses in the DOI-91, Oracle Federal Financials (OFF) system of records notice. Some information may be shared with other agencies and organizations as described in the routine uses in GSA/GOVT-3, Travel Charge Card Program, GSA/GOVT-4, Contracted Travel Services Program, and GSA/GOVT-6, GSA SmartPay Purchase Charge Card Program. These notices may be viewed on the DOI Privacy Program SORN website at https://www.doi.gov/privacy/sorn. Customer agencies are responsible for managing their own PII, have control over their own records and are responsible for meeting the disclosure requirements of the Privacy Act.

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

Data may be shared with agency contractors providing program support, for processing transactions, or related functions such as processing credit card transactions or travel claims for reimbursement. Customer agencies are responsible for managing their own PII related data, and contractor staff may be used for this management.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

PII data is shared with credit card companies and other financial institutions for reimbursement activity, and for accounting or financial operations functions to facilitate the payment of customer agency invoices. Customer agencies are responsible for managing their own PII related data, and contractor staff may be used for this management.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

This system does not collect PII directly from individuals. Information comes from customer agencies who are responsible for requesting and managing PII for their reimbursement and financial management activity. Customer agencies are responsible for providing notice to individuals for the information collected, the right to consent to uses of the information, and the right to decline information. Individuals provide PII through forms, requests for reimbursements, etc. that are processed through each agency customer before it is entered into OFF. The PII is required to make payments on behalf of the customer agency; however, only the minimal amount of information necessary to perform that function is required. The amount of PII information collected outside this function is determined by the IBC OFF customer agency and may vary based on each customer agency's requirements.

For Federal employees, individuals grant consent to provide banking and related information for payroll related electronic deposit when they voluntarily sign the required documents during the orientation process or submit requests to process transactions. Employees may decline to provide such information and may receive manual checks for reimbursement where available.

For contractors, the amount of information required is stipulated in the terms of the contract entered with IBC or the customer agency. Alternative payment methods (e.g., manual checks) may be available for those individuals who decline to provide information or consent to the specific use of their PII to process financial transactions.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

Privacy Act Statements are provided when information is collected directly from individuals for entry into OFF, and customer agencies are responsible for providing notice to their employees for the information collected, the right to consent to uses of the information, and the right to decline information for their reimbursement and financial management activities. Information

may be collected through forms that contain Privacy Act Statements. For example, the SF 1012, Travel Voucher form has a Privacy Act Statement as it collects information from individuals for travel reimbursement requests that is processed by customer agencies and entered into OFF.

The IBC Oracle Supplier Request Form collects information from Federal customer agency employees to process payment requests to vendors or suppliers and contains a Privacy Act Statement.

☒ Privacy Notice: *Describe each applicable format.*

Individuals are also provided notice on how their PII is managed during these financial management activities through the publication of this PIA, systems of records notices published in the *Federal Register*, such as DOI-91, Oracle Federal Financials (OFF), and published government-wide system notices, including GSA/GOVT-3, Travel Charge Card Program, GSA/GOVT-4, Contracted Travel Services Program, and GSA/GOVT-6, GSA SmartPay Purchase Charge Card Program. Federal customer agencies also provide notice of their financial management activities through their own published system of records notices.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data may be retrieved manually or automatically by authorized system users through core OFF reports or the report functions in Discoverer or OBIEE. Data is accessed via Java and HTML-based forms by authorized users through keyword searches or system defined parameters. Information may be retrieved by name, vendor ID (a system generated identification number not identifiable to an individual), TIN/EIN, invoice or payment document number, and/or transaction date. Manual reports may include, but are not limited to, confirmation of individual vendor payments or analysis of contract disbursements for purposes of financial management. Automated reports are generated for payment-related (i.e., Department of the Treasury payment files) and mandatory reporting (e.g., IRS reporting).

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Reports produced on individuals are used to validate customer agency remittance activity. The reports are accessible to appropriate accounting or financial operations staff for the exclusive performance of these duties. Below is a list and description of these reports.

- Active Users Report - List of Oracle application users who does not have an end date. Reports can only be generated by system and security administrators.

- Unsuccessful Login User Report - List of Oracle application users with failed attempts logging into the application. Reports can only be generated by system and security administrators.
- IBC User Responsibility Report - List of Oracle application user accounts and their assigned user roles and responsibilities in the system. Reports can only be generated by system and security administrators.
- Active Responsibilities Report - List of Oracle application responsibilities and start dates. Reports can only be generated by system and security administrators.
- Identify Federal Employees - An employee debt and collection report by customer name and number, SSN, and Bill to Address for tax and Social Security Administration reporting purposes. Finance office staff with an official need to know have access to the report.
- Active Employee Listing - A report listing all active employees by system generated employee number and name. Finance office staff with an official need to know have access to the report.
- New Vendor Letter - A report listing vendor name, site, and address. Finance office staff with an official need to know have access to the report.
- Supplier Payment History - Report listing all payments made to employees and separate charge card expenses from those that are paid directly to the employee. Finance office staff with an official need to know have access to the report.
- Supplier Paid Invoice History - A report by employee supplier type to review payment history, discounts taken, and frequency of partial payments. Finance office staff with an official need to know have access to the report.
- 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. Finance office staff with an official need to know have access to the report.
- 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. Finance office staff with an official need to know have access to the report.
- IBC Vendor Audit Report - A report identifying changes made to supplier and bank records and the individual making the change. Finance office staff with an official need to know have access to the report.

☐ No

Section 3. Attributes of System Data

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

Customer agencies must submit the Oracle Supplier Request Form for entry into OFF. Each customer agency is responsible for managing and maintaining the data under their control, and for ensuring the data is accurate, relevant, timely, and complete. In addition, information is also obtained from SAM, government payroll providers, FPPS such as new employee names and

addresses, and banking information changes for existing employees, and NFC. Validation for such data is performed by these respective agencies.

B. How will data be checked for completeness?

Customer agencies must submit the Oracle Supplier Request Form when new vendor, customer, or supplier financial data is required. The accuracy, completeness, and validity of the financial data is the responsibility of the customer agency. Data entered into OFF is validated for accuracy by the IBC Vendor Team at the time the Oracle Supplier Request Form is processed. The IBC Vendor Team is a staff fully dedicated to the entry, update, and retirement of supplier-related data in OFF.

Data is also obtained from SAM, government payroll providers, FPPS (new employee names and addresses, and banking information changes for existing employees), NFC, and eTravel interface (employee government travel credit card number). Completeness of this data is validated by these respective agencies. OFF interfaces with the data as it is provided.

Additionally, an agency-specific Oracle User Access Request Form must be submitted by the Federal customer agency and signed by the appropriate client agency supervisory personnel and/or data custodian. Note: IBC employees have a separate User Access Request form. Both the client agency user access request form and IBC FMD-employee user access request forms are submitted to the OCIO Customer Support Center (CSC), whom opens a Remedy ticket, attaches the completed User Access Request Form and assigns the ticket to the IBC/FMD Security Points of Contact (SPOCs) in the FMD Information Assurance Office (IAO) for review and completion. The form can be used to add a new user, modify a user or remove (delete) a user. Note: we do not actually delete the user data in the database for audit tracking purposes. Requested roles and responsibilities must comply with IBC guidelines on internal controls and separation of duties. Additionally, there is a ProdCopy access request form that must be submitted to the IBC OFF System Administrators in the FMD Technical Services and Solutions Division (TSSD) for use by a predetermined set of customer agency test users and signed by the appropriate customer supervisory personnel and/or data custodian for customer acceptance testing purposes in the ProdCopy test environment. Note: essentially for the OFF ProdCopy environment, the OFF System Administrators in TSSD verify that the user (1) has access to Production that is not inactive or been revoked and; (2) that the access in ProdCopy is exactly what they normally have access to in Production.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

The timeliness of individual and supplier data initiated by customer agencies used for remittance purposes is ensured by customer agencies through the Oracle Supplier Request Form. The Oracle Supplier Request Form is provided to customer agencies to ensure data uniformity and the minimal collection of data required to perform financial transactions on behalf of customer agencies. The Oracle Supplier Request Form is submitted by the customer agency for new vendors, customers, and suppliers or for updates to existing customers. This form is tracked individually and completed by the IBC Vendor Team.

When data is updated in a record, the changes propagate throughout the system. OFF is a relational database with referential integrity that stores data in individual table records and each record has a record ID (i.e., primary key). Data is reported through the use of these keys.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Records maintained in OFF belong to customer agencies and are retained in accordance with applicable agency records retention schedules or General Records Schedules (GRS) approved by the National Archives and Records Administration (NARA), and customers are responsible for managing and disposing of their own records. Retention and disposition may vary based on the type of record and needs of the agency. For example, GRS 1.1 covers financial management records, and records are destroyed six years after final payment or cancellation. The customer agency provides the IBC with the appropriate records retention schedule for the customer agency data and is responsible for managing their own records in accordance with the Federal Records Act.

DOI records are maintained under Departmental Records Schedules (DRS) and GRS that cover administrative and financial management records, and retention periods may vary according to the subject matter and needs of the agency. DOI financial records are covered under DRS 1, Administrative Records (DAA-0048-2013-0001), and have a temporary disposition.

- DAA-0048-2013-0001-0010, 3.1 - Short-term Financial and Acquisition Records; Destroy 3 year(s) after cut-off. Cut off record as instructed in the agency/bureau records manual, or at the end of the FY in which the record is created if no unique cut-off is specified.

- DAA-0048-2013-0001-0011, 3.2 Long-term Financial and Acquisition Records. Destroy 7 year(s) after cut-off. Cut off record as instructed in the agency/bureau records manual, or at the end of the fiscal year in which files are closed if no unique cut-off is specified.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Each customer agency storing data in the system maintains those records under NARA approved records schedules for the retention of reports and data. While the IBC provides system administration and management support to agency clients, any records disposal is in accordance with client agency approved data disposal procedures and each customer agency is responsible for meeting records requirements and managing the disposition of those records at the end of the retention period.

Customer agencies are responsible for purging employee data according to the customer agency records schedule after an employee's access authority is terminated or the employee retires, changes jobs, or dies. The IBC does not purge or delete any customer financial records.

DOI records that are maintained under Departmental Records Schedules and GRS are disposed of by shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. **Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.**

There are risks to the privacy of individuals due to the volume of sensitive PII contained in the system. The protection of PII processed by the OFF system is a paramount consideration for DOI and IBC, and appropriate privacy and security controls have been implemented to mitigate these privacy risks.

There is a risk that individuals may not receive adequate privacy notice or consent to the uses of their information. This risk is mitigated through the Privacy Act Statement provided to individuals on various forms used by IBC and customer agencies when collecting information from individuals. Privacy notice is also provided through publication of this privacy impact assessment, and the published system of records notices for records maintained by DOI and by the customer agencies, as well as the government-wide system of records notices.

There is a risk that information or records will be maintained longer than necessary to achieve the agency's mission, or that records may not be properly destroyed. This risk is mitigated by managing records in accordance with a NARA-approved records schedule and providing extensive training to users on IT security, Privacy, Records Management and controlled unclassified information. This training specifically includes handling and disposal of records with sensitive information and also the proper procedures for handling faxed information. Customers are responsible for managing and disposing of their own records. The Federal customer agency provides IBC with the appropriate records retention schedule for the customer agency data and is responsible for managing their own records in accordance with the Federal Records Act. DOI records are maintained as temporary records under DRS-1, which was approved by NARA, and are disposed of by approved destruction methods in accordance with NARA guidelines.

There is a risk that PII may not be current, complete or accurate. The accuracy, completeness, and validity of the financial data is the responsibility of the customer agency that owns the data. The Oracle Supplier Request Form is submitted by the customer agency for new vendors, customers, and suppliers or for updates to existing customers. Data entered into OFF is validated for accuracy by the dedicated IBC Vendor Team at the time the Oracle Supplier Request Form is processed. This form is tracked individually and completed by the IBC Vendor Team. The IBC has implemented procedures and data validation checks to identify any discrepancies such as incomplete or duplicated data. When data is updated in a record, the changes propagate throughout the system.

There is a risk that PII may be misused or used for unauthorized purposes. Employees only have access to information that is needed to perform their official duties. DOI and customer agency employees and contractors are required to complete privacy, Federal Information Systems

Security Awareness (FISSA), and records management awareness training. DOI personnel authorized to manage, use, or operate the system information are required to complete annual privacy, security, and records management awareness training as well as privacy and security role-based training and sign the DOI Rules of Behavior prior to accessing the system. Employees are subject to monitoring in the system and DOI network. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, and criminal, civil, and administrative penalties. OFF audit logs are reviewed daily on an ongoing basis and anomalous events are investigated and immediately reported if found to be a potential breach or security incident. Audit records contain sufficient information for audit review. Suspicious events, such as excessive unsuccessful attempts to log in, unusual network traffic, unauthorized or unusual user activity, or any potential compromise of PII, are reported immediately upon detection to the DOI Computer Incident Response Center (DOI-CIRC), DOI's security incident reporting system, for investigation and escalation.

There is a risk of unauthorized access to the system, exposure, loss or compromise of PII. The OFF system has undergone a formal Assessment and Authorization and been granted a security accreditation in accordance with FISMA and NIST standards. OFF is rated as FISMA moderate based upon the type of data and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system. OFF traffic that originates from the Internet into the DOI Office of the Chief Information Officer (OCIO) network is encrypted in compliance with the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, point-to-point data transmission is also encrypted. Operational and technical controls in place include firewalls, malware identification, and periodic verification of system users, in addition to physical controls. Strong shared software tokens are used to authenticate the connection, as well as firewalls and other security controls. Customer agency interconnections with DOI are established for the purpose of sharing the OFF application. The Internet connectivity is expected to remain in compliance with OMB M-08-05, Implementation of Trusted Internet Connections. The connections at each end are located within controlled access facilities, which are guarded 24 hours a day. The data is stored in the tables of the OFF electronic database, which is hosted on servers under the control and supervision of the DOI OCIO.

OFF incorporates extensive access controls and monitoring of user activities at all times. These controls are implemented at the development of the production system, and are maintained and monitored throughout the life cycle of the system. Authorized users access their agency data through a Java-based application accessed through a secure internet URL. Customer agencies provide the IBC a range of Internet Protocol (IP) addresses for access to the OFF web address. Customer agency staff have remote access to OFF. Remote access is governed by individual customer agency Interagency Security Agreements. All transmissions are secure and encrypted. Customer agencies are responsible for determining their own rules and procedures for granting access to OFF.

The IBC follows the "least privilege" core security principle, such that only the least amount of access is given to a user to complete their required business or financial activity. All access is controlled by authentication methods to validate the authorized user. Some authorized users in support roles have "read only" access within OFF. Sensitive information is masked and is not

viewable to these users, only basic identifying information, such as supplier name, is available. Authorized users who have direct responsibility for completing customer agency remittance activities have "write" access within OFF to perform their official duties and may have elevated access to the PII required to fulfill their duties. This ensures only authorized personnel have access to PII or update or modify records.

A customer's user account is automatically deactivated due to user account inactivity for a specific period of time as follows: normal Oracle users are inactivated after 45 consecutive days of inactivity, and Oracle users with privileged or administrative access are inactivated after 30 consecutive days of inactivity. A list of users and assigned responsibilities is sent to each customer point of contact for review quarterly. Each customer agency contact verifies the appropriate access roles have been assigned to the end user as required in the performance of the end user's job. The customer agency is responsible for notifying the IBC of any users who no longer require their OFF access or requires access changes. Based on the notification by the customer agency, and at their request, selected users may have the access roles on their account removed, however, the account itself remains in its deactivated state for audit and historical purposes until such time as the customer terminates its business contract with the IBC and after the expiration of the retention period specified by the customer agency's records retention schedule.

Access to the DOI network requires two-factor authentication. Users are granted authorized access based on least privilege in order to perform their official duties and such privileges must comply with the principles of separation of duties. OFF uses the automated Oracle Fusion Governance, Risk, and Compliance (GRC) product to manage and enforce separation of duties (SOD) rules. These rules are maintained by IBC Functional Support staff. Controls over information privacy and security are compliant with and maintained in accordance with OMB A-123, Management's Responsibility for Internal Control, and NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

DOI and the customer agency utilizes audit trail features to record and monitor user access and activities in the system to include event types, date and time of events, user identification, successful or failed access attempts, and security actions taken by system administrators. DOI and customer agencies work together to ensure the security of the connected systems and the information stored, processed and transmitted as specified in the applicable individual agency Interagency Security Agreements, and as required by Federal laws, policies, and regulations.

Below are potential risks and the countermeasures to mitigate them.

- Password security: Access could be gained to the OFF application without a properly configured user ID and password combination. Users could make an unlimited number of attempts to guess a password without being locked out. Password length could be too short to provide adequate protection against guessing (non-compliance with DOI password length requirements). Passwords could be unchanged for too long, making it more possible that they could be guessed over time. Users could reuse their favorite password every time they reset it, thereby making it more possible to be guessed or

compromised. Passwords could be so simple in composition as to make them too easy to guess.

These risks are mitigated by OFF application account password security measures, which have been configured with the following requirements:

- ○ Passwords must be at least 12 characters in length;
- ○ Passwords expire every 60 days for a general user, and 30 days for privileged users;
- ○ Accounts become inactive after 45 days of inactivity for a general user, and 30 days for privileged users;
- ○ Users must wait 1440 days before reusing an old password;
- ○ Lockout after 3 consecutive unsuccessful login attempts;
- ○ Password complexity (alpha-numeric and 1 special character) is enforced; and
- ○ Initial passwords and passwords reset after lockout must be changed at first login.

- Access could be granted without proper documentation and approval. This risk is mitigated by ensuring access to the OFF application is granted based on a completed Oracle Access Request Form with Supervisor approval. For Accounting Operations Services Division personnel, an additional review and signature by the Internal Control and Audit Liaison Section is required.

- Terminated users are not removed on a timely basis, and accounts of terminated users could be used by unauthorized personnel. These risks are mitigated by disabling separated personnel's access to the OFF application upon exit clearance notification.

- Level of access privileges may not be commensurate with the user's job responsibilities or may no longer be needed. This risk is mitigated by disabling separated personnel's access to the OFF application upon exit clearance notification.

- Assigning roles: Users could be given access privileges that would allow them to perform overlapping or conflicting actions or to bypass necessary checks and balances in an unapproved or unauthorized manner. Users could be assigned roles that exceed the intended scope of authority required to perform their duties.

These risks are mitigated by using an automated GRC tool to prevent separation of duty conflicts from being assigned to OFF accounts. OFF users are assigned roles, which allow them to access various OFF menus and functions. Numerous role groupings exist based on the different job responsibilities of each user. As the control environment changes, the IBC performs an analysis of roles and functions to ensure the user's access is commensurate with their duties. Remedy tickets are required for new responsibilities.

There is a risk related to the use of reports produced on individuals for the purpose of validating customer agency remittance activities. This risk is mitigated by administrative and technical controls to manage and limit access to authorized personnel. Reports are accessible only to authorized staff for the exclusive performance of their duties. System use, user accounts, active

user reports can only be generated by system and security administrators. Active employee listings, vendor lists, payment history reports, supplier activity or deactivation reports, vendor audit reports, and employee debt and collection reports are only accessible by authorized finance office staff who have an official need to know to perform their duties.

Customers have access to reports for the data under their ownership and control:

- Data available for agency Discoverer users is limited to their specific Organization leveraging Oracle's Multi-Org Access Control (MOAC) capability. In addition to MOAC, PII data is constrained by the OFF named user account.
- Data available for agency OBIEE users is limited to their specific Ledger or Organization using security filters within the OBIEE Repository Database. PII data is further protected using Responsibilities (e.g. XXX Payroll OBIEE, where XXX is the acronym for the client agency) assigned by the IBC SPOC Team via a user access request and associated Remedy ticket.

In addition to the OFF MOAC capability that only allows individual agency customers to see their own agency data through their responsibilities, all reports generated for customers contain only that client agency's data. Please note that the OFF Oracle database has an ad-hoc database account 'apps_read' that can read different customers' data. This account is only used by IBC/FMD support personnel with privileges commensurate with their job duties. Other ad-hoc database access is limited to database administrators. Clients do not have access to that elevated access and data view.

System audit logs do not capture reports generated and downloaded by personnel or customers. OFF is a COTS product and by design, the OFF Oracle database only audits Data Definition Language used to create/alter database objects changes and Data Manipulation Language used to insert/update/delete statements to change data. The Structured Query Language select statements needed to generate reports cannot be audited due to the fact that there are too many select statements each day and auditing them would cause the database to hang, creating a lack of availability to both personnel and customers.

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*

The data is relevant and necessary to identify and reimburse Federal employees and contractors on official travel with the electronic funds transfers or Department of the Treasury checks; relate purchases and travel expenses on bank card bills to Federal employees with government bank card authority; collect accounts receivable owed to OFF customers; and issue payments to suppliers or vendors on behalf of customer agencies.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

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

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

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

Not applicable as OFF does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe*

An agency-specific Oracle Access Request Form must be submitted by the IBC or the Federal customer agency and signed by the appropriate supervisory personnel and/or data custodian. The forms are submitted to the IBC SPOCs for review and completion. Requested roles and responsibilities must comply with IBC guidelines on internal controls and separation of duties. Additionally, there is a ProdCopy access request form that must be submitted to the IBC SPOCs for use by a predetermined set of customer agency test users and signed by the appropriate supervisory personnel and/or data custodian for customer acceptance testing purposes in the ProdCopy test environment.

Users who have the direct responsibility for completing customer agency remittance activity have "write" access within OFF. In support of these activities, the procurement and purchasing roles and responsibilities (e.g., "Procure to Pay," "Purchase Requestor X," "Certifying Officer," etc.) have elevated access to the PII required to fulfill their duties.

Client Inquiry, Systems Accountant, Accountant, and other "support" roles and responsibilities has "read only" access within OFF. Sensitive information is masked and is not viewable to these users, only basic identifying information, such as supplier name, is available.

Customer agency staff have remote access to OFF. Remote access is governed by individual customer agency Interagency Security Agreements. All transmissions are secure and encrypted.

OFF is a financial management system that supports government financial accounting functions, and is subject to audit by internal and external oversight organizations. Information about individuals will be shared with these organizations only when authorized, consistent with applicable system of records notices.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access to OFF is granted by IBC SPOCs. The SPOCs grant access and assign responsibilities based on the submission of an Oracle Access Request Form. Oracle Access Request Forms are submitted by external customer agencies and internal IBC components. Customer agencies are responsible for determining their own rules and procedures for granting access to OFF. Customer agencies and IBC components designate authorized approvers for system access requests.

Only users who have the direct responsibility for completing customer agency remittance activity have "write" access within OFF. In support of these activities, the procurement and purchasing roles and responsibilities (e.g., "Procure to Pay," "Purchase Requestor X," "Certifying Officer," etc.) have elevated access to the PII required to fulfill their duties.

Client Inquiry, Systems Accountant, Accountant, and other "support" roles and responsibilities has "read only" access within Oracle. Sensitive information is masked and is not viewable by these users. Only basic identifying information, such as supplier name, is available.

OFF user administrators review information system accounts every three months (quarterly) to ensure that continued account access is necessary. Client administrators also review system accounts every quarter for the same purpose.

Temporary or emergency accounts are created with a defined expiration date and are automatically terminated on that date unless they are disabled before the account expires.

Oracle requires every supplier to be registered with a valid contact and an active user account to utilize the Surrogate Offer functionality. Users cannot record an offer against an unregistered supplier. To make this functionality available to CLM customers, every supplier has been associated with a contact and user account in the system. Though these are active user accounts, the supplier contacts do not have access to the account username and password, which prevents them from logging into the system. However, it is a requirement that the user accounts be active indefinitely (e.g., are not end-dated) in order for CLM customers to create surrogate offers in the system.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

The appropriate Federal Acquisition Regulation privacy clauses were included in the contract. Contract personnel are involved in the development and maintenance of the OFF system. IBC contractors are required to sign nondisclosure agreements as a contingent part of their employment and are also required to sign the DOI's Rules of Behavior and complete privacy, security, and records management training prior to accessing a DOI computer system or network. Privacy and security role-based security training must be completed on an annual basis as an employment requirement.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

OFF provides automated logging of all user activity while logged into the application for auditing and error resolution. Identification and monitoring may be performed within the OFF system for approved purposes over a limited time frame when authorized by the appropriate authority. The OFF system has no functionality to identify, locate, or monitor individuals

outside the system.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

Auditable events logged by OFF are specified by the 375 DM 19, Information Technology Security Program, implementation of NIST 800-53. Depending on the platform involved and the event logging capabilities each platform type creates security event logs compliant with the above standard. OFF audit logs generate the following types of information: event (type and success/failure); source of change (e.g., system logs include IP address, application and database logs associate all actions with a specific user ID); and the date and time of the event. Audit logs are reviewed daily by the system Database Administrators. Suspicious events, such as excessive unsuccessful attempts to log in, unusual network traffic, or any potential compromise of PII, are reported immediately upon detection to DOI-CIRC, DOI's security incident reporting system, for investigation and escalation.

OFF audit logs are reviewed daily on an ongoing basis and anomalous events are investigated and immediately reported if found to be a potential breach of security. Audit records contain sufficient information for audit review. System and network audit logs indicate what events occurred, the sources of the events, what software logged the event, and the outcomes of the events, such as pass, fail, or error. Current processes include scripting for manual review and parsing for ArcSight reporting, a security information and event management (SIEM) solution that helps identify and track security threats.

M. What controls will be used to prevent unauthorized monitoring?

Monitoring of OFF usage is strictly limited to only OCIO and IBC technical employees whose positions require them to have the necessary access, knowledge, and the requirements in their job assignments to perform such monitoring. Monitoring is a function of the host system and application system logs which operate behind the scenes in accordance with the system's authorized configurations and programming. The results of the logging systems are reviewed daily by administrative personnel responsible for conducting the audit reviews. Security anomalies are isolated and investigated to the degree necessary to ensure the continued protection of the system and its data. The OCIO ArcSight system routinely stores audit logs from OFF system servers and archives it centrally for long-term storage and reporting. In addition to the daily audit log reviews, ArcSight also produces warnings to OCIO staff in the event that suspicious violations or activity are detected. Employees only have access to information that is needed to perform their official duties. All DOI personnel must complete annual privacy and security training and sign DOI Rules of Behavior acknowledging their understanding to protect sensitive data.

N. 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*

The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and all other applicable security rules and policies. Facilities that host the system are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures. Server rooms are locked and accessible only by authorized personnel.

(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*

There are five available levels of electronic security to prevent unauthorized access, which include network access security limits, physical and logical access controls for the data center hosting the system, operating system controls, application passwords, and application data group security levels. Access to servers containing system records is limited to authorized personnel with a need to know the information to perform 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. Access to the system is also limited by network access or security controls such as firewalls, and encryption of system data. System interconnections with Federal agencies, financial institutions, and contractors are via secured network access controls, and OFF is subject to the continuous monitoring program to ensure controls are maintained on an ongoing basis.

(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*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The IBC Financial Management Directorate, Technical Services & Solutions Division (IBC/FMD/TSSD) Chief serves as the OFF Information System Owner and the official responsible for oversight and management of security controls and the protection of customer agency information processed and stored by the OFF system. The Information System Owner and the OFF Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in OFF, in consultation with the Departmental Privacy Officer. Customer agency data in OFF is under the control of each customer, and the customer agency is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as addressing complaints.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The OFF Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The OFF Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, and appropriate DOI officials in accordance with DOI policy and established procedures. The customer agency data in OFF is under the control of the customer agency. Each customer agency is responsible for the management of their own data and the reporting of any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data.