U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

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: Business Integration Office Financial Business Management System Cloud (BIO FBMS-Cloud)
Bureau/Office: Office of the Secretary (OS)
Date: January 31, 2024
Point of Contact
Name: David Clark
Title: OS Departmental Offices, Acting Associate Privacy Officer
Email: OS_privacy@ios.doi.gov
Phone: N/A
Address: 1849 C Street NW, Room 7112, Washington, D.C. 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

B. What is the purpose of the system?

The Business Integration Office Financial and Business Management System Cloud (BIO FBMS-Cloud) is an enterprise-wide financial management system that consolidates the majority of the Department of the Interior's (DOI) business and financial management functions. BIO FBMS-Cloud has been fully implemented for all bureaus, and fully migrated to a cloud hosted infrastructure.

DOI is using an integrated suite of software applications to implement BIO FBMS-Cloud as a comprehensive approach to improving current business functions. The BIO FBMS-Cloud is comprised of several commercial off-the-shelf (COTS) packages and is designed to incorporate the majority of the financial management functions within DOI into a single solution. Fully deployed, BIO FBMS-Cloud eliminates over 80 DOI and bureau systems, enabling the alignment of business management system within the DOI's strategy of modernization, integration, accountability, and the creation of customer value.

BIO FBMS-Cloud supports Federal government general ledger management, funds management, payment management, receivable management, and cost management. It provides detailed transaction information necessary to comply with the Department, bureau, Department of the Interior Acquisition Regulations (DIAR), Department of the Treasury, Office of Management and Budget (OMB), and Federal Accounting Standards Advisory Board (FASAB), and Federal Acquisition Regulation (FAR) requirements.

BIO FBMS-Cloud provides critical financial reporting, budgetary status, and program information to agency managers. It provides effective internal controls and supports a large number of DOI projects by tracking costs, linking project costs to reimbursable agreements, and generating customer billings. BIO FBMS-Cloud also supports annual, multi-year, and no-year funding for many different sources of funding such as appropriated, franchise, reimbursable, revolving, available receipts, unavailable receipts, special/trust receipts, contract authority, and loan authority.

BIO FBMS-Cloud integrates Core Financials with numerous other business processes and other functional areas such as budget formulation, acquisition, real property, personal property and fleet management, financial assistance, travel, and permanent change of station. Major interfaces exist with the DOI's Federal Personnel and Payroll System (FPPS) and DOI's Charge Card provider, both of which include detailed transaction cost allocation functionality. Core Financials also has interfaces with additional bureau tracking systems. Systems, Applications & Products in Data Processing (SAP) Open Catalog Interface (OCI) is the technical and functional standard used by SAP and its suppliers to communicate shopping cart information. BIO FBMS-Cloud uses OCI as the standard for interfacing with suppliers for catalogs.

The FBMS Executive Management Information Systems (EMIS) provides all employees analytical capabilities and information on how their work contributes to the Department's overall strategic direction and will enable analysis of how the Department can improve on service delivery or program effectiveness. The detail needed to make the information useful will vary depending on the management purpose, but the EMIS analytic tools enables the same data to be used at Department, bureau, and field levels without making additional data inquiries. The EMIS warehouses data hosts from a variety of Department, bureau, and field level sources, and makes this data available to all DOI employees with FBMS access. Information can be summarized at the Departmental or bureau levels for senior leadership or viewed at the transaction level if needed for detailed analysis by managers and employees.

The FBMS EMIS encompasses the SAP Business Warehouse (BW) 4 High Performance Analytical Appliance (HANA) and supports the analytic reporting requirements of FBMS. BIO implemented SAP Business Objects and Tableau Server, which provides analytic and visualization against the data within BW and creates graphs, charts, and visualizations based on the data. SAP Business Objects and Tableau Server are browser based. The role-based access provides capabilities for the separation of both users and content. Individual permissions can be set for projects, dashboards, or any shared object.

BIO upgraded Enterprise Resource Planning (ERP) Central Component (ECC) to SuiteOnHana (SOH) to maintain technical currency including upgrading to the latest enhancement pack (Ehp8) and ECC Unicode conversion and are in the process of migrating to S4HANA in next couple of years.

The BIO FBMS-Cloud solution will be used by over 70% of DOI employees; it will affect all employees and operations. The solution provides the capability to balance financial and business management workload across DOI. These objectives are met through BIO FBMS-Cloud by providing eight functional areas. Users can perform a wide variety of business functions in the following general business areas:

- **Core Financials:** Core Financials is the backbone for BIO FBMS-Cloud. It supports many of the system's central accounting tasks and provides common processing routines and common data for many of the system's financial management functions.

- **Acquisition:** Acquisition supports the process of obtaining goods and services, including tracking the status of requisitions, purchase orders, and contracts; recording and validating the receipt of goods and services; and providing information needed to match invoices and issue payments.

- **Travel:** Travel is used for the financial management of the Department's travel and transportation activities.

- **Financial Assistance:** Financial Assistance is used to manage grants and subsidies to state and local governments, other organizations, or individuals.

- **Personal Property and Fleet Management:** Personal Property and Fleet Management provides physical and accounting control over the Department's personal property.

- **Real Property:** Real Property provides the information necessary to develop and implement improvements for Department owned land, buildings, structures, and facilities.

- **Budget Formulation and Planning:** The Budget Formulation and Planning function encompasses formulation of program, enterprise, and Department-wide level budget formulation requirements. The function supports budget development, advocacy, internal/external reporting, and full cost budgeting and management.

- **Enterprise Management Information:** The Enterprise Management Information Function supports collecting and retrieving current and historical financial, program, and related performance data for analysis, decision making, and performance reporting by managers at all levels.

The EMIS node represents the reporting and business warehouse functions within the BIO FBMS-Cloud. This functionality is a combination of the SAP BW application, SAP Portal, and canned reports delivered within the package applications. SAP's BW provides a complete information solution. BW is the central component in the SAP suite of applications with an added advantage of being a software package that can be used in both SAP and non-SAP environments. This system approach consolidates the external and internal sources of data into a single repository.

Master Data Governance (MDG) Tool: The MDG tool will provide DOI users with the ability to improve transaction level reporting based on grouping of the master data. MDG will also enhance master data maintenance utilizing automated processes, including workflow and notifications to improve creation, changes and auditability of master data. The MDG will allow the bureaus to group different master data together to improve reporting.

The MDG objects functionality will include Application of Funds (AoF), Fund, Functional Area, Work Breakdown Structure (WBS) Element, Funded Program, Funds Center, Cost Center, AoF and Fund Rollover, and Hierarchies/Grouping. The Fund and AoF (including rollover functionality) has been implemented across all the bureaus. The Office of Budget (POB) is available with the remaining master data objects.

BW Reporting: The BW provides management reporting, including non-SAP data sources into reports. This independent data warehouse solution summarizes data from ECC applications and external sources to provide executive information for supporting decision making and planning. Reports cover a wide range of information requirements, automated data staging, and standard ECC business process models. SAP BW supports the complete data warehousing process, from data integration, data transformation, consolidation, and cleansing to data provision for analysis.

Enterprise Resource Planning (ERP) Central Component (ECC): The BIO FBMS upgraded ECC to SuiteOnHanna (SOH) implemented in the BIO FBMS-Cloud environment to maintain technical currency including upgrading to the latest enhancement pack (Ehp8) and ERP ECC Unicode conversion, while improving user experience by migrating the SAP ECC system from an Oracle Database to a High-Performance Analytical Appliance (HANA) Database.

Payroll Fixed Costs (PFC) reporting system: PFC reporting starts with collecting data from the EMIS system, FPPS system, and OPM to create a data warehouse (tables and views) for reporting. As per the current process, the data collected will consist of employee payroll data up to the current pay periods extracted into BW via the nightly feeds. Users with full access shall upload the non-FBMS master data from external system and additional data attributes required

for reporting. This information will be maintained within the new tool as a part of ongoing process.

1099PRO Reporting: FBMS BIO uses the 1099PRO Reporting tool for reporting to Internal Revenue Service (IRS) of payments made to vendors deemed taxable by IRS guidance. These services include electronic filing, printing, and mailing of vendor 1099s and acts as a service bureau for preparers wanting to outsource the submission and distribution process for their IRS forms filing.

GrantSolutions (GS): GrantSolutions is a shared service managed by the Department of Health and Human Services. DOI grants management transitioned to GrantSolutions (GS) a software-as-a-service from Planning Tool for Resource Integration, Synchronization, and Management (PRISM) for processing financial assistance awards. An integrated business developed to manage an application from receipt to award. This integrates GS with SAP for processing commitment transactions (referred to as purchase requisition (PRs)) and obligation transactions (referred to as purchase orders (POs)).

The UiPath Robotic Process Automation (RPA): Low to no-code Commercial-of-the-shelf (COTS) software technology that enables rapid design, testing, and deployment of automations. The RPA technologies automate repetitive/rules-based tasks. Bots are new age digital assistants, which may interact with almost any system application and adapt to existing interfaces or workflows.

C. What is the legal authority?

Chapter 1 of Title 48, CFR Chapter 1 (Federal Acquisition Regulations); 5 U.S.C. 5514, 5701 et seq.; 26 U.S.C. 6402; 31 U.S.C. 3511 and 3512, 3701, 3702, 3711; 40 U.S.C. 483; Public Law 106-107, and 41 CFR 300-304.

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

E. Is this information system registered in the Governance, Risk, and Compliance platform?

☒ Yes: UII Code: 010-000000316; System Security and Privacy Plan (SSP) for Business Integration Office Financial and Business Management System Cloud

☐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.*
FBMS-Continuous Support Environment (CSE)	Internal interconnected environment providing a collection of tools that support items in BIO FBMS-Cloud	No	A Privacy Threshold Analysis was completed for FBMS-CSE.

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

☒Yes:

The FBMS records are covered under the following DOI SORNs:

- INTERIOR/DOI-86, Accounts Receivable: FBMS - 73 FR 43772 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021)
- INTERIOR/DOI-87, Acquisition of Goods and Services: FBMS - 73 FR 43766 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021)
- INTERIOR/DOI-89, Grants and Cooperative Agreements: FBMS - 73 FR 43775 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021)

The DOI SORNs may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices.

Travel records are covered the following Government-wide General Services Administration SORNs:

- GSA/GOVT-3, Travel Charge Card Program - 78 FR 20108 (April 3, 2013)
- GSA/GOVT-4, Contracted Travel Services Program - 74 FR 26700 (June 3, 2009); modification published 74 FR 28048 (June 12, 2009)

These Government-wide SORNs may be viewed at https://www.fpc.gov/resources/SORNs/.

☐No

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

☐Yes
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Sex
☒ Birth Date
☒ Truncated SSN
☒ Financial Information
☒ Credit Card Number
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Employment Information
☒ Other:

Vendor Unique Entity Identifier (UEI) Number; Taxpayer Identification Number (TIN); and Employee Identification Number (EID)

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:

DOI Records
FPPS provides labor cost accounting data to FBMS via a batch interface.

The following provides an overview of external system interfaces and describes any data

inbound to FBMS.

Federal Agencies

U.S. Department of Health and Human Services (HHS)

- Grants.Gov – Grants.Gov sends data into the FBMS Financial Assistance component. The Grants.Gov data includes DOI grant application forms and supporting materials that provide additional information on how the applicant intends to spend grant funds, schedules, diagrams, pictures, etc. The grantee reported expenditures information used to obligate grant funding can include grantee name, vendor UEI, SSN, address, and back account number.

U.S. General Service Administration (GSA)

- Mileage Express – The Mileage Express interface is only an outbound interface, with FBMS providing, on a monthly basis, mileage utilization data on GSA provided vehicles to GSA's Mileage Express system.

- Central Contractor Registration (CCR) – CCR feeds data into the FBMS Core Financials component to ensure FBMS uses a common vendor identifier. The CCR vendor data includes vendor name, bank address, and UEI/TIN numbers.

- Motor Pool Charges – The Motor Pool Charges interface from GSA to FBMS provides a monthly file of GSA motor pool utilization and repair charges, which are posted into FBMS (reversing the utilization accruals).

- GSAXcess – The interconnections between GSAXcess.gov and BIO FBMS-Cloud is bidirectional. The information follows primarily from the agency system to GSAXcess.gov. The interconnection is to facilitate real-time property data, image, and documentation reporting to the GSAXcess.gov.

U.S. Department of Treasury (Treasury)

- Automated Standard Application for Payments (ASAP) – FBMS provides grants payment data to the ASAP system at Treasury to request payments to grant recipients.

- Government Online Accounting Link System (GOALS) – GOALS is a collection of application that allows Treasury to collect data from and disseminate reports to the Federal Program Agencies.

- Secure Payment System (SPS) – This is an outbound interface from FBMS to Treasury's SPS to request payments on DOI's behalf.

- The Internet Payment Platform (IPP) – A secure web-based electronic invoicing and payment information system provided by the Treasury's Financial Management Service. The IPP allows Federal agencies to transform their existing paper-based order-to-pay

processes into a streamlined electronic flow. Federal agencies use the IPP to send electronic purchase orders (POs) to suppliers, to receive electronic invoices from suppliers, and for invoice routing and approval workflow. The IPP uploads payment remittance information from the Treasury and non-Treasury disbursed agencies, allowing agencies and their suppliers to view and download payment information.

- Intra Governmental Payments and Collections (IPAC) – Federal agencies use the IPAC system to pay for goods and services provided by other Federal agencies. The IPAC enhancement provides the ability to record outgoing cash transactions in the system to correspond to cash already debited/credited by Treasury.

- Pay.Gov – The Treasury Web Application Infrastructure (TWAI) provides a multi-tiered World Wide Web interface and common services within a robust infrastructure for multiple Treasury applications. The applications servers use database and other resources in Zone 3, as needed. Application-specific (Pay.Gov, for example) processing and storage components are generally in Zone 3, as objects requiring the protection of the deepest zone.

- DataBase Management System (DBMS) – The TWAI is a secure infrastructure with Internet and dedicated telecommunications connectivity. The DBMS provides support to the TWAI environment which includes web servers driven by login residing on an application server.

Third Party

- CitiBank SmartPay3 – The "Smart Card" credit card vendor (CitiBank) provides detailed charge card expenses to FBMS.

- Concur Travel System (CGTS) – Additional travel expense data will come into the FBMS system to support employee expense voucher processing and payment.

- CompuSearch (Fed-Connect) – Federal vendors enter their invoices through the GovPay web portal site. For DOI bureaus supported by FBMS, Fed-Connect then transmits these invoices to FBMS for processing.

- 1099PRO – A reporting tool which is used for reporting to the IRS of payments made to vendors deemed taxable by IRS guidance. The services include electronic filing, printing, and mailing of vender 1099s and acts as a service bureau for preparers wanting to outsource the submission and distribution process for their IRS forms filing.

- SAP Public Services – This interconnection is between the SAP and DOI, Office of the Chief Information Officer (OCIO) networks for the purpose of providing system users, located within SAP, access to the office of the Secretary (OS) / BIO based applications. This agreement contains available communications protocols, data transfer capabilities,

specific communications hardware, and encryption requirements to establish a secure connection to DOI.

- SAIC – Interconnection between SAIC and DOI/OCIO networks provides system users, located within SAIC, access to OS/BIO based applications. This agreement also covers connections made by application systems located within the SAIC network utilizing service accounts to transfer data through system-level interfaces.

- Microsoft Azure Commercial Cloud – Microsoft Azure Commercial Cloud is the Managed Service Provider (MSP) for the BIO FBMS-Cloud system. Interconnection between MSP and DOI/OCIO networks provides system users, located with the MSP, access to OS/BIO based applications.

- GrantSolutions – DOI and GS interface is between the GS Grants Management Module (GMM) and DOI's SAP-based FBMS financial system. The interface will align with DOI grants business process for financial assistance awards.

In summary, during the Operations and Maintenance phase, data will continue to come into the FBMS system from various areas within DOI. A few of the areas are eGov Travel, Fed-Connect for vendor invoices, CCR Vendor master data, Office of Surface Mining Reclamation and Enforcement's (OSMRE's) Coal Fee Collection and Management System (CFCMS) and Bureau of Land Management's (BLM's) CBS invoices, and acquisition and accounting generated paperwork.

On an ongoing basis, the Financial Assistance module of FBMS will use data coming from paperwork generated during the grant processing, grant applications received online from Grants.Gov website, and data entered directly into FBMS on-line.

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:

BIO FBMS-Cloud shares information with numerous DOI Bureaus and offices, Federal agencies, and third-party sources. Information listed in Section "E" below.

☒ Other:

Data may be manually entered into the FBMS by authorized personnel at respective bureaus and offices.

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

The primary use of the PII collected is to maintain accounting and financial information associated with the acquisition of goods and services, processing of travel authorizations and pay travel claims, billing debtors for amounts owed to DOI and follow-up on unpaid debts, and to award and manage grant and cooperative agreement awards.

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

☒ Within the Bureau/Office:

BIO FBMS-Cloud is an enterprise-wide application centrally managed by the DOI BIO. Each DOI bureau/office has assigned Account Controllers and other administrators that grant access to employees who have a need to know in order to perform their official duties. Each bureau/office only has access to its own information. Users access FBMS via the FBMS Portal. FBMS Transnational access is restricted only to users who have been granted authorized access.

FBMS Suite of reporting tools which includes the BW, SAP Businessobjects Web Intelligence (WEBI), SAP Business Objects Online analytical processing (OLAP) for Analysis and Tableau Client/Server. The Businessobjects and Tableau analytical tools will be used to extract existing data from FBMS SAP Business warehouse via Reports. This report data can be used to create data visualizations using aggregate, summary level, or detailed data. The output of the analytical tools can be shared via the tools themselves, shared drives (OneDrive, SharePoint, etc), email, and other DOI security approved data sharing methods. FBMS end users use this approach to share FBMS data, some of which may be sensitive information and/or personally identifiable information (PII). End users and report developers who have access to sensitive information and/or PII have the responsibility to ensure that FBMS data is shared only with the appropriate audience. DOI Rules of Behavior applicable to the end users and developers govern the appropriate use of data once it's extracted and shared outside of FBMS.

☒ Other Bureaus/Offices:

BIO FBMS-Cloud is an enterprise-wide application centrally managed by the DOI Business Integration Office. Each DOI bureau/office has assigned Account Controllers and other administrators that grant access to employees who have a need to know in order to perform their official duties. Each bureau/office only has access to its own information. Users access FBMS via the FBMS Portal. FBMS Transnational access is restricted only to users who have been granted authorized access.

FBMS Suite of reporting tools which includes the BW, SAP Businessobjects WEBI, SAP Business Objects OLAP for Analysis and Tableau Client/Server. The Businesobjects and

Tableau analytical tools will be used to extract existing data from FBMS SAP Business Warehouse via Reports. This report data can be used to create data visualizations using aggregate, summary level, or detailed data. The output of the analytical tools can be shared via the tools themselves, shared drives (OneDrive, SharePoint, etc), email, and other DOI security approved data sharing methods. FBMS end users use this approach to share FBMS data, some of which may be sensitive information and/or PII. End users and report developers who have access to sensitive information and/or PII have the responsibility to ensure that FBMS data is shared only with the appropriate audience. Rules of Behavior applicable to the end users and developers govern the appropriate use of data once it's extracted and shared outside of FBMS.

Bureau of Reclamation (BOR)
Interconnection is established between FBMS and BOR for the purpose of providing system users, located within BOR, access to OS/BIO based application. The BOR Budget and Reporting System supports the budget execution processes of BOR. The primary processes are the Funds Transfer and Allocation processes.

Office of Surface Mining Reclamation and Enforcement (OSMRE)
The CFMS supports OSMRE's Fee Compliance Program. OSMRE collects and stores coal company permit data in FBMS. Data is not shared and is kept internal to OSMRE. The system supports various aspects such as: maintaining reported coal-mining operations activity and Abandoned Mine Land fees due; account, billing, payment processing, debt collection functions; and supporting the civil penalty enforcement program.

Bureau of Land Management (BLM)
CBS sends collection and billing files to FBMS to ensure that all collections, and all bills, adjustments and reversals posted in CBS are also posted in the FBMS ledger of record, and the two systems are kept in sync.

Office of Aviation Services (OAS) – Inbound interface twice a month from the DOI Aviation Management Division containing the charges of all FBMS bureaus for aircraft usage.

Alaska Fire Store and National Interagency Fire Center – Inbound interfaces, with FBMS receiving information regarding newly established Fire Codes, along with descriptive information, project definition, and potentially multiple WBS elements for each new Fire Code. The new fire code project and associated WBS elements are established for use within FBMS.

☒ Other Federal Agencies:

Data is shared and reported to other Federal agencies, including the Treasury, GSA, HHS, and FedBizOpps as required. Data may be shared pursuant to the routine uses contained in these published SORNs: INTERIOR/DOI-86, INTERIOR/DOI-87, INTERIOR/DOI-89, and GSA/GOVT-3, and GSA/GOVT-4.

Treasury

ASAP - FBMS provides grants payment data to the ASAP system at Treasury to request payments to grant recipients. The Treasury ASAP system returns a payment status file to FBMS with grant payment confirmation information.

SPS - This is an outbound interface from FBMS to Treasury's SPS to request payments on DOI's behalf.

GOALS - A collection of applications that allows Treasury to collect data from and disseminate reports to the Federal Program Agencies. FBMS invoices are paid by Treasury. This interface from the Treasury GOALS system to FBMS conveys disbursement confirmation information and check cancellation data. This data is used to record the disbursements in FBMS.

IPP - A secure web-based electronic invoicing and payment information system provided by the Treasury's Financial Management Service. The IPP allows Federal agencies to transform their existing paper-based order-to-pay processes into a streamlined electronic flow. Federal agencies use the IPP to send electronic POs to suppliers, to receive electronic invoices from suppliers, and for invoice routing and approval workflow. The IPP uploads payment remittance information from the Treasury and non-Treasury disbursed agencies, allowing agencies and their suppliers to view and download payment information.

IPAC - Federal agencies use the IPAC (Intra Governmental Payments and Collections) system to pay for goods and services provided by other federal agencies. The inbound IPAC enhancement is intended to provide the ability to record outgoing cash transactions in the system to correspond to cash already debited / credited by Treasury.

DBMS - The TWAI is a secure infrastructure with Internet and
dedicated telecommunications connectivity. The DBMS provides support to the TWAI environment which includes web servers driven by login residing on an application server.

HHS

Connection between Grants.gov and IBC network to allow users data transfer capabilities. IBC provides hosting services and support for the HHS core personnel payroll system. FPPS handles all current regulations including specialized pay, garnishments, special appointment programs, and more. FPPS is the HHS payroll accounting system of record.

GSA

CGTS - A web-based, end-to-end travel management system to plan, authorize, arrange, process, and manage official federal travel. Connection used to transfer Extensible Markup Language (XML) files containing financial and accounting data between OCIO and GSA CGTS.

☐Tribal, State or Local Agencies

☒Contractor:

Information may be shared with contractors as authorized and outlined in the routine uses contained in the following SORNs: INTERIOR/DOI-86, INTERIOR/DOI-87, INTERIOR/DOI-89, GSA/GOVT-3, and GSA/GOVT-4.

☒ Other Third-Party Sources:

SAIC Corporation
Interconnection is established for the sole purpose of sharing applications with SAIC. Billing, collection, payment, and other financial information is critical to the timely accomplishment of the SAIC mission.

Microsoft Azure Commercial Cloud
Microsoft Azure Commercial Cloud is the MSP for the BIO FBMS-Cloud system. Interconnection between MSP and DOI/OCIO networks provides system users, located with the MSP, access to OS/BIO based applications.

SAP Public Services
Allows the FBMS SAP Solution Manager Enterprise Edition instance(s) to communicate with the SAP Enterprise Support Services for reporting SAP software malfunctions via error messages to SAP and to allow download of SAP Support packages and software releases and SAP Notes.

CitiBank SmartPay3
CitiBank is established for the sole purpose of sharing the system for government cardholders and administrators to track and report expenses which occur on their Citibank government issued credit cards. Citi Manager serves as a system for government cardholders and administrators to track and report expenses which occur on their CitiBank government issued credit cards.

1099PRO – BIO FBMS uses 1099PRO Reporting tool for reporting to IRS of payments made to vendors deemed taxable by IRS guidance. The services include electronic filing, printing, and mailing of vendor 1099s and acts as a service bureau for preparers wanting to outsource the submission and distribution process for their IRS forms filing.

COMPUSEARCH (Fed-Connect) - Federal vendors enter their invoices through the GovPay web portal site. For DOI bureaus supported by FBMS, Fed-Connect then transmits these invoices to FBMS for processing.

GrantSolutions (GS) - DOI and GS interface is between the GS GMM and DOI's SAP-based FBMS financial system. The interface will align with DOI grants business process for financial assistance awards.

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

☒ Yes:

Federal employees have the option of not providing information on forms required during the application and onboarding process. These official forms contain Privacy Act Statements notifying individuals of the authority, purpose, and uses of the information. Employees are required by law to provide certain types of information, such as name and SSN as a part of the employment process. This information is required by applicable Federal statutes, including tax and employment eligibility regulations, and are necessary data elements in FBMS.

Declining to provide this information may affect the employment eligibility and pay status of the individual, and other processes and requirements related to employment.

☐ No

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

☒ Privacy Act Statement:

Privacy Act Statements are provided when PII is requested directly from individuals on various government forms at the time a request is made for goods, services, travel claims, application for grant, or other services.

Privacy Act Statements are also provided on the forms used during the onboarding process.

FBMS is a Privacy Act System and authorized users are presented with a Privacy Act Statement as a disclaimer at sign on to the FBMS.

☒ Privacy Notice:

Notice is also provided through publication of this PIA and the following system of records notices: INTERIOR/DOI-86, INTERIOR/DOI-87, INTERIOR/DOI-89, GSA/GOVT-3, and GSA/GOVT-4.

☐ Other:

☐ None

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

Personal identifiers may be used to retrieve data in FBMS. Due to the open nature of the search fields, virtually any type of personal identifier that is described in this document could be used to retrieve information on individuals, including the following identifiers: EIN, UEI, applicant

name (company name or person), street address, organization ID, name, phone number, fax number, email address, vendor number, vendor name, SSN (only for DOI employees carried within the vendor file to support travel voucher reimbursement payments), charge card information to include last name, first name, and account number.

I. Will reports be produced on individuals?

☒Yes:

FBMS can produce the following reports related to individuals:

Labor Reporting Report identifies labor costs by pay periods, business areas and organizations, or fund areas and programs. The reports can drill down to detailed labor cost record information needed to verify individual employee labor charges by account assignment. For instance, the system can generate detail reports by business area, employee, pay period, to report the number of hours recorded by pay code and account assignment. A Labor Interface Specialist may extract reports to ensure proper classification and reconciliation of labor charges.

Charge card reports may assist in tracking budget, supporting 1099 processing, and supporting program controls for card settings and defaulting schemes. Access is granted to an Agency/Organization Program Coordinator to create management control reports. Fleet managers have access to maintain fleet charge cards, as well as run queries and reports on fleet cards under their authority.

☐No

Section 3. Attributes of System Data

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

Most of the data collected from sources other than DOI records come from Federal government agencies such as the Treasury and GSA and is deemed reliable at the time it is provided. However, the system performs validation and reconciliation of information at each system-to-system interface to ensure that the data is transferred and stored properly, without data errors.

Data integrity checks will be performed by FBMS as incoming and outgoing data is processed through the FBMS portal. Both systems will contain data integrity checks to ensure data accuracy. Data that conforms to business rule and integrity checks will be posted. Non-conforming data will be posted to a suspense file for examination and resubmission upon correction.

In a few cases, such as credit card and travel data, information is provided by third party vendors. The PII included in the data submitted by these vendors is not independently verified; however,

any such PII is initially supplied by the individuals to the third party, so the data is deemed to be accurate.

B. How will data be checked for completeness?

Data will be checked for completeness as it is entered into the system. DOI-defined business rules and database integrity will determine if the data is complete. One type of verification of completeness check involves creating a list of valid inputs and checking inputs against the table.

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

Data is checked to see if it is current and not duplicated by comparing the incoming data with the data already in the system. This check is performed when being processed through the FBMS portal.

Most of the data collected from sources other than DOI record come from Federal government agencies such as the Treasury and GSA and is deemed to be current. Third-party vendors providing data for FBMS are required to update data when needed. In all cases, data is automatically checked for currency by comparing the incoming data with the data already in the system as the data is being processed.

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

Retention periods for FBMS vary as records in FBMS are maintained by subject matter in accordance with the applicable Department-wide, bureau or office records schedule, or General Records Schedule, approved by the National Archives and Records Administration (NARA) for each specific type of record maintained by the Department. Records retention periods are also subject to litigation holds, court orders, and preservation notices issued by the Office of the Solicitor.

FBMS data is covered under Departmental Records Schedules, DAA-0048-2013-0001, 1.3-Financial and Acquisition Management, and 1.4, Information Technology, which may include short term and long-term records. Records are temporary and are cut off as instructed in the bureau manual or at the end of the fiscal year in which the files are closed, then destroyed 3 years or 7 years after cutoff depending on the record.

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

Currently BIO FBMS-Cloud retains all records while FBMS is implementing an Information Lifecycle Management (ILM) tool to manage records and data in the system. Records will be disposed of in accordance with the applicable record schedule and Departmental policy. Paper

records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with NARA guidance and Departmental policy.

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 is a risk to the privacy of individuals due to the volume of sensitive PII contained in the system. The major privacy risks associated with FBMS are related to the transfer, maintenance, and use of PII. PII contained in FBMS is shared with external organizations or agencies only when authorized. Interconnection Security Agreements are maintained between the DOI and organizations that have systems connecting to FBMS to ensure that data is maintained in compliance with Departmental security control standards and regulations. FBMS has multiple layers of application security that protect PII at the role level, which can be applied to a user or groups of users. System security roles that provide access to PII are carefully controlled and only assigned by Account Controllers to end users in compliance with the principles of least privilege. PII that is maintained in FBMS is protected by FIPS compliant Data at Rest encryption at the database level. FBMS users complete DOI mandated annual security, privacy, and records management training and role-based privacy and security training, and sign DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy.

There is a risk that data may be inappropriately accessed, used, or disclosed. FBMS has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. FBMS is a cloud system rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system. A system security and privacy plan were completed to address security and privacy controls and safeguards for the BIO FBMS-Cloud system. Controls outlined in the BIO FBMS-Cloud System Security and Privacy Plan that adhere to the standards outlined in NIST SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems, and includes the use of role-based security training, encryption, and maintaining data in secured facilities, among others.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance. An audit trail of activity will be maintained sufficient to reconstruct security relevant events. The BIO follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Access to the DOI network requires multi-factor authentication (MFA). Users are granted authorized access to perform their official duties and such privileges must comply with the principles of separation of duties. 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, Security and Privacy Controls for Federal Information Systems and Organizations.

PII and sensitive data are collected in the FBMS Financial system. BIO FBMS-Cloud is a IaaS (Infrastructure as a Service) located in the Microsoft Azure Commercial Cloud FedRAMP authorized and has met DOI's information security, privacy and records requirements. BIO FBMS-Cloud is internal to DOI and can only be accessed via DOI.Net with communications encrypted and secure to prevent information from being read, intercepted, or changed. To minimize the risk users must use MFA when signing into DOI.Net and Single Sign-On /Secure Authentication Markup Language (SSO/SAML) when signing into FBMS.

There is a risk that data may be stored for longer than necessary with BIO FBMS-Cloud financial system. Records are maintained and disposed of under a NARA approved records schedule. User accounts containing PII that are inactive are disabled by system administrators, however, user created content is maintained as long as it remains active. Information collected and stored within the DOI Active Directory (AD) is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

All FBMS users receive privacy notices and acknowledge by logging in that they are subject to monitoring of the system for lawful, authorized, and appropriate use. There is a risk that individuals may not receive adequate notice of DOI privacy practices or the extent of the use of their PII data in FBMS applications. Individuals voluntarily provide their identifying information when requesting a user account to access FBMS and are provided a DOI Privacy Notice on the sign in page on the Enterprise FBMS Portal. General notice is provided through the publication of this privacy impact assessment and the related published SORNs. Users may also view the Privacy Statement Supplement by DOI Privacy Office that addresses their use, storage, sharing and disclosure of personal data collected through the use of FBMS system accounts. Users may also contact DOI, bureau and office privacy officials with any questions or privacy concerns at https://www.doi.gov/privacy/contacts.

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:

FBMS is an enterprise-wide financial management system that consolidates the majority of DOI's business and financial management functions. All data contained within the FBMS are necessary for the support of DOI Business Process Operations, including, but not limited to, the following:

Support of the Department's central accounting tasks, common processing routines and common data for many of the system's financial management functions, acquisition of goods and services, including tracking the status of requisitions, purchase orders, and contracts; recording and validating the receipt of goods and services; providing information needed to match invoices and issue payments; management of the Department's travel and transportation activities; management of grants and subsidies to state and local governments, other organizations, or individuals; physical and accounting control over the Department's personal property; development and improvement of Department owned land, buildings, structures, and facilities; and data collection and analysis for performance reporting.

1099PRO Professional software is used each tax year by FBMS to fulfill 1099, W-2, and other IRS documents filing requirements. The benefit of using 1099PRO includes reducing government operating costs, providing greater functionality, improving efficiency, and reducing the risk of inputting the wrong data for vendors.

☐No

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

☐Yes

☒No

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

☐Yes

☒No

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

☐Yes

☒No

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

FBMS does not derive or create new information about individuals.

F. Are the data or the processes being consolidated?

☐Yes, data is being consolidated.

☒ Yes, processes are being consolidated.

FBMS uses the audit log feature that can be used to run reports on authorized users' access to and actions within the system. Additionally, FBMS contains a user traceability program that can detect unauthorized access attempts or access to files outside of an authorized user's permissions.

☐ 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:

Application Administrators - FBMS system administrators, application administrators, contractors, and users supporting the system and performing system maintenance and other related activities may have access to the data in the system.

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

FBMS follows Governmental and Departmental standards for application access controls. All system access requires a MFA authentication. The FBMS Access Control Policy outlines the requirements for gaining access to FBMS.

Bureau/Office administrators are responsible for controlling and monitoring access of authorized employees. Bureau/Office Administrators and authorized employees will only receive access to data for their own Bureau or Office. A user must have a valid DOI Active Directory (AD) account prior to submitting a new user registration request. The request is initiated in Governance, Risk and Compliance (GRC) and processed through automated approvals by the requisite parties (Bureau Security Points of Contact (SPOCs) and Bureau Account Controllers). The SPOC and Account Controller must approve the new user registration request before the user is granted access to FBMS. Once established in the system, account privileges can be assigned to users as part of a role-based access control security model. Role requests are also initiated in GRC and processed through automated approvals involving Bureau SPOCs, Bureau Account Controllers, Bureau Internal Controls Coordinators, and Bureau Training Coordinators.

1099PRO data is restricted to only designated authorized users assigned the role to administer and process 1099PRO tax documents.

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:

Contractors are responsible for designing and developing the system and with maintaining the system. Privacy Act contract clauses are included in all contractor agreements. BIO 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 security and privacy training prior to accessing a DOI computer system or network. Information security and privacy awareness training and role-based privacy and 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

☒No

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

☒Yes:

FBMS audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system, to include attempts to access files or transactions beyond the user's assigned permissions. The logs capture account creation, modification, disabling, and termination in the logs. The application name, date and time is captured, item ID, type, location, event type date and action taken on item is captured in the logs. Audit logs are enabled on all host and server systems as well as the firewalls and other network perimeter security devices and IDS. All logs automatically roll up to the logging system for consolidation, analysis, retention, and reporting purposes. The logger is configured to automatically email the OCIO Security Operations staff for any high severity events.

☐No

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

FBMS audit logs can be used to run reports detailing an individual users' authorized access and actions performed within the system, to include attempts to access files or transactions beyond the user's assigned permissions. The logs capture account creation, modification, disabling, and termination in the logs. The application name, date and time is captured, item ID, type, location,

event type date and action taken on item is captured in the logs. Audit logs are enabled on all host and server systems as well as the firewalls and other network perimeter security devices and IDS. All logs automatically roll up to the logging system for consolidation, analysis, retention, and reporting purposes. The logger is configured to automatically email the OCIO Security Operations staff for any high severity events.

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

Controls outlined in the FBMS System Security and Privacy Plan that adhere to the standards outlined in NIST SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems, are in place to prevent unauthorized monitoring. This includes the use of role-based security and privacy training, encryption, and maintaining data in secured facilities, among others. FBMS assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any FBMS assets. FBMS IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

Only authorized users with valid DOI AD credentials will be able to access the system. In addition, all users must consent to the DOI Rules of Behavior and complete Federal Information System Security Awareness, Privacy and Records Management training before being granted access to the DOI network or any DOI system, and annually thereafter.

BIO FBMS-Cloud has Single Sign-On (SSO) enabled, users who log onto the DOI network can access the Privacy Policy via the link located at the bottom of the FBMS, Enterprise Portal page or the DOI.GOV website. Users must use PIV card and can only access BIO FBMS-Cloud within the DOI network.

FBMS is a Privacy Act System and authorized users are presented a Privacy Act statement in the warning banner prior to signing into the application.

FBMS users are presented with a Terms and Conditions of Use prior to signing on to the application:

This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access,

and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

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

(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: TLS – Transport Layer Security

(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

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 Director, Office of Financial Management, is the FBMS Information System Owner and the official responsible for oversight and management of the FBMS security and privacy controls and the protection of information processed and stored by the FBMS system. The Information System Owner and the FBMS Privacy Act System Manager(s) 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 FBMS, and for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, as well as meeting the requirements of the Privacy Act, providing adequate notice, making decisions on Privacy Act requests for notification, access, amendments, and complaints in consultation with DOI Privacy Officials.

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 FBMS Information System Owner is responsible for oversight and management of the FBMS security and privacy controls, and for ensuring to the greatest possible extent that FBMS data is properly managed and that all access to data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC, Cybersecurity & Infrastructure Security Agency, and privacy officials within 1-hour of discovery in accordance with Federal policy and established procedures.