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 Enterprise Acquisition Reporting (BEAR) Application
Bureau/Office: Interior Business Center
Date: August 7, 2018
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 Business Enterprise Acquisition Reporting (BEAR) application is an Operational Data Analytics project of the Department of the Interior (DOI), Interior Business Center (IBC), Acquisition Services Directorate (AQD). BEAR incorporates industry standards and best practices to provide an integrated solution using Microsoft tools and technologies for both the front-end website and back-end database and leverages data from DOI's existing enterprise

systems to provide AQD-specific capabilities. This prototype of reporting and analytics solution augments the enterprise capabilities by integrating the financial and award information from the DOI Financial and Business Management System (FBMS), award information from the General Services Administration (GSA) Federal Procurement Data System (FPDS), and the contract data and AQD-specific information not residing in other systems. BEAR provides a reporting, business intelligence and data analytics platform with web-based functionality of more advanced features to meet the day-to-day needs of the contracting acquisition staff across all DOI AQD's divisions.

C. What is the legal authority?

Chapter 1 of Title 48, CFR Chapter 1 (Federal Acquisition Regulation)

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*

010-000002434; Business Enterprise Acquisition Reporting System Security Plan

☐ 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	Not applicable

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-87, Acquisition of Goods and Services: FBMS, 73 FR 43766, July 28, 2008

☐ 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
☒ Other: *Specify the PII collected.*

Names of the authorized system users will be entered by system administrators directly into the system through the web interface. FBMS's existing system user ID will be collected as part of the reports integrated from FBMS. FPDS system user ID will be collected as part of the data integrated from Federal Procurement Data System - Next Generation (FPDS-NG), which will be done via an Application Programming Interface (API).

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*

In addition to the system user ID, financial and contract data will be integrated from FBMS. Data will also be integrated from FPDS-NG, GSA's Federal government-wide contract reporting system via an API to capture publicly available contract data, which does not contain sensitive PII.

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*

User IDs from FBMS and FPDS are integrated into the BEAR application through a web interface.

☐ Other: *Describe*

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

Federal employee names and usernames from FBMS and FPDS-NG will be used to customize reports to filter records specifically related to Federal employee user in order to create and manage user accounts, link contracting data to contracting officers/acquisition personnel, and support reporting and analytics solutions during contract administration.

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.*

PII will only be available to the individuals within AQD, and will be used to manage workload, track status of work in progress and view historical accomplishments.

☐ 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.*

☐ 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.*

Contractor support will be responsible for web development and maintenance as well as database administrator activities for the underlying database. Contractors also serve a variety of roles within the office, including as Contract Specialists, Financial Analysts and Administrative support roles.

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

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.*

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

User data is obtained from other existing information systems such as FBMS and FPDS-NG and is collected during the onboarding process based on employee roles. Users are automatically added to BEAR as part of the onboarding process.

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.*

A Privacy Act Statement is provided to individuals when accessing the BEAR system.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this privacy impact assessment and the DOI-87, Acquisition of Goods and Services: FBMS, system of records notice, which may be viewed at https://www.doi.gov/privacy/doi-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.).

Personal identifiers of BEAR users will be used to retrieve data, including system User IDs from FBMS and FPDS-NG. Data is retrieved through automated reports within the system. When a user logs in, available data is filtered based on their User ID.

I. Will reports be produced on individuals?

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

Reports will be available related to contract actions, Purchase Requisitions (PRs), invoices and other contract related actions. These reports will be used to manage workload of teams, branches, and divisions, and will provide DOI personnel the ability to track their own workload in terms of pending contract actions, contracts being managed, and upcoming contract administration tasks.

☐ No

Section 3. Attributes of System Data

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

Data collected from FPDS-NG and FBMS will be subject to data quality checks, which will verify the accuracy of data through conditions defined in the Extract, Transform, and Load (ETL) process.

B. How will data be checked for completeness?

The transactional data and user names collected from sources other than DOI records come from Federal government agencies such as the 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 as part of the ETL process as incoming data is processed. BEAR will contain data integrity checks to ensure data accuracy. Data that conforms to business rules and integrity checks will be posted.

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

Data collected from FPDS-NG and FBMS are subject to data quality checks as part of the ETL process which maintains the currency of the data. The data quality checks employed during the ETL process are documented as part of the Source to Target Data Mappings.

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 BEAR vary as records in BEAR are maintained by subject matter in accordance with the applicable Department-wide records schedule, which was approved by the National Archives and Records Administration (NARA)(DAA-0048-2013-0001). Records retention periods are also subject to litigation holds, court orders, and preservation notices issued by the Office of the Solicitor. BEAR data is covered under Department Records Schedules,, 1.3-Financial and Acquisition Management, and 1.4, Information Technology, which includes both short term and long term records. Records are temporary and are cut off 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 specific record that may require additional retention. The operators/managers should err on using 7 year retention if they are uncertain as to which is applicable.

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

Records are deleted from the database in accordance with the records schedule identified in D above. The approved disposition methods include 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 is a minimal privacy risk due to the limited PII maintained in the BEAR system. BEAR is used to generate reports for the management of workload in terms of pending contract actions, contracts being managed and upcoming contract administration tasks. Only the names or user names of the users and system user are maintained, which are initially collected and processed through the DOI enterprise identity management process via proper notice and consent process.

There is a risk that individuals may gain unauthorized access to the information in BEAR. BEAR is rated as a FISMA low application based upon the type of data, and is designed with applicable security control features. It has multiple layers of application security that can enforce access controls and protect data at the role level, and on user or groups basis. The system security roles that provide access to data are carefully controlled and only assigned by Account Controllers to end users in compliance with the least privilege principle. Administrators and authorized employees will only be granted role-based access to the data for AQD. Accounts will be created as a need to access the system is identified and accounts will be disabled when the need ends, either through a role change or due to leaving the organization. Audit logs are used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination in the logs. FIPS compliant Data at Rest encryption at the database level is enforced to protect BEAR data. The use of BEAR is conducted in accordance with the appropriate DOI use policy.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting and sharing information with unauthorized recipients. This risk is mitigated by limiting access to the system to only those personnel who have an official need to perform their job duties. Access to information is role-based and is only granted on a need-to-know basis, and requires DOI credentials. 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 role-based security training must be completed on an annual basis as an employment requirement. DOI requires all DOI users to enroll in security, privacy and records management training when onboarding and subsequently on an annual basis. These trainings will ensure that throughout the life cycle of the information system and data management, the privacy and security controls and protections can be executed and maintained by meeting sufficient level of performance requirement.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored has intentionally been limited to only the minimal amount of data needed for

identification purposes and to conduct official functions of the system. Records are maintained in accordance with Department Records Schedules that were approved by NARA. BEAR records will be disposed of through standard procedures, which further mitigates any potential risk. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

There is a risk that individuals may not have notice that their PII will be collected or how it will be used. This risk is mitigated by the Privacy Act Statement posted at the BEAR log in screen, this PIA and the published DOI-87 system of records notice.

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*

All data contained within BEAR are necessary for the support of AQD Business Process Operations, including, but not limited to, support of acquisition of goods and services, and tracking the status of requisitions, purchase orders, and contracts.

☐ 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?

BEAR does not derive or create new information about individuals.

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.*

Access will be restricted to only AQD personnel. Access controls are integrated with employee in-processing and out-processing to ensure only current employees have access to the system. Integrated Windows Authentication (IWA) or Google Active Directory Federation Services (ADFS) are deployed to integrate access with user's digital certificate. Direct access to the underlying database will be restricted to web and data developers and limited to AQD staff with reporting responsibilities.

☐ 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*

BEAR system administrators will be responsible for maintaining the environment and overall application, and may have access to the data tables supporting the application. They will not have update or delete privileges to these tables.

BEAR application administrators will be responsible for maintaining user profile information through the web application. They will have the ability to create and update records, but will not be able to delete users.

BEAR users will have access to review data via reports, but will not be able to make changes to the data via BEAR.

Database administrators will be responsible for overall maintenance of the underlying data tables and will have full privileges to these tables as necessitated by their function.

Federal contractors will be performing as database administrators, system administrators and some user roles.

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

BEAR follows Governmental and Departmental standards for application access controls. All system access requires username and password authentication. User account management and control are part of the in-processing and out-processing procedures at AQD. Administrators are responsible for controlling and monitoring access of authorized employees. Administrators and authorized employees will only be granted role-based access to the data for AQD. Accounts will be created as a need to access the system is identified and accounts will be disabled when the need ends, either through a role change or due to leaving the organization.

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?*

Contractors are responsible for designing and developing the system and with maintaining the system. Privacy Act contract clauses are included in all contractor agreements.

AQD 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 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*

Audit logs will be maintained on user access to the system, as well as changes to data made by users within the system. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination in the logs.

☐ No

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

Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination in the logs.

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

Access to these audit log tables will be restricted to the Information Security Officer and system administrators responsible for monitoring access according to the least privilege principle.

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*

(2) Technical Controls. Indicate all that apply.

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

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior

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

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 Business Operations Division I Chief serves as the BEAR Information System Owner and the official responsible for oversight and management of the BEAR security and privacy controls and the protection of information processed and stored by the BEAR system. The Information System Owner and Information System Security Officer 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 BEAR, meeting the requirements of the Privacy Act, and responding to requests or 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 Business Operations Division I Chief serves as the BEAR Information System Owner and is responsible for oversight and management of the BEAR security and privacy controls, and for ensuring to the greatest possible extent that DOI data is properly managed and that all access to DOI data has been granted in a secure and auditable manner. Authorized users are responsible for ensuring their use of BEAR is in accordance with Federal law and policy. The Information System Owner is responsible for ensuring that any potential or confirmed loss, compromise, unauthorized access or disclosure of PII is reported to the DOI Computer Incident Response Center (DOI-CIRC) within 1-hour of discovery in accordance with Federal policy and established DOI procedures.