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: Financial Business Management System Decommissioning

Date: 06-08-2016

Bureau/Office: Office of the Secretary

Bureau/Office Contact Title: Departmental Privacy Officer

Point of Contact Email: Teri_Barnett@ios.doi.gov

First Name: Teri

M.I.:

Last Name: Barnett

Phone: (202) 208-1605

Address Line 1: 1849 C Street NW

Address Line 2:

City: Washington

State/Territory: District of Columbia

Zip: 20240

Section 1. General System Information

A. Is a full PIA required?

Yes

Yes, information is collected from or maintained on

All

B. What is the purpose of the system?

The Financial Business Management System (FBMS) is an enterprise-wide financial management system that consolidates the majority of Department of the Interior (DOI) business and financial management functions. FBMS was fully implemented for all Bureaus in November 2013 and was fully migrated to a cloud hosted infrastructure June 2015. Therefore, FBMS is being decommissioned in accordance with DOI Directive 2008-21, Establishment of the Information System Decommissioning (ISD) Methodology, and will no longer be used. Upon conclusion of all FBMS migration activities of the FBMS System, data, and documentation to the Federal Cloud infrastructure, the legacy DOI hosting

infrastructure (servers and storage) will no longer be needed and will be retired/decommissioned.

Software Archive Overview

The FBMS software is not being decommissioned; it has been migrated/converted to a new infrastructure provided by a Cloud Infrastructure As a Service (IaaS) provider. The FBMS Cloud based systems and software are supported by a tested replication disaster recovery solution, so the legacy DOI FBMS infrastructure is no longer needed and has been decommissioned.

Hardware Disposition Overview

As a result of the successful conversion/migration of the FBMS system, data, and documentation to the Federal Cloud infrastructure, the legacy DOI hosting infrastructure (servers and storage) is no longer needed and will be decommissioned.

Server hard drives will remain within the Data Center organizational control until destroyed on site. The Data Center Manager has property custody of the servers until custody is transferred to a property officer within the Office of Facilities and Services (OFAS), Property Management Office. The entire Storage hardware will be professionally sanitized (scrubbed) in accordance with standard DoD 5220.22-M specifications because it is being decommissioned. The hardware vendor will provide sanitization, verification, and certification.

All data has been migrated to the FBMS Cloud. To ensure that no data has been left on the old infrastructure, the tapes, hard drives and server have been cleared/stripped and overwritten. Tapes will be recirculated in the tape library and FMBS data will be overwritten. All tapes will remain within the data center's organizational control.

Data Archive Overview

The system is not being discontinued, but was migrated/converted to the cloud and continues to operate. The security configuration in these environments was migrated/converted to the Federal Cloud in June 2015. Each bureau's Security Points of Contact (SPOCs) and the FBMS Security team verified that the system security and access rights did not change during the migration.

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; DOI Directive 2008-21, Establishment of the Information System Decommissioning (ISD) Methodology.

D. Why is this PIA being completed or modified?

Retiring or Decommissioning a System

E. Is this information system registered in CSAM?

Yes

Enter the UII Code and the System Security Plan (SSP) Name

010-00-01-01-01-1127 - System Security Plan for Financial and Business Management System

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	Describe
None	None	No	

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)

Records are covered by four FBMS systems of records DOI–86: Financial and Business Management System (FBMS) – Accounts Receivable; Interior, DOI–87: Financial and Business Management System (FBMS) – Acquisition of Goods and Services; Interior, DOI–88: Financial and Business Management System (FBMS) – Travel Management Records; and Interior, DOI–89: Financial and Business Management System (FBMS) – Grants and Cooperative Agreements, which are being updated to reflect changes to the system.

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

No

Section 2. Summary of System Data

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

☐ Name	☐ Religious Preference	☐ Social Security Number (SSN)
☐ Citizenship	☐ Security Clearance	☐ Personal Cell Telephone Number
☐ Gender	☐ Spouse Information	☐ Tribal or Other ID Number
☐ Birth Date	☐ Financial Information	☐ Personal Email Address
☐ Group Affiliation	☐ Medical Information	☐ Mother's Maiden Name
☐ Marital Status	☐ Disability Information	☐ Home Telephone Number
☐ Biometrics	☐ Credit Card Number	☐ Child or Dependent Information
☐ Other Names Used	☐ Law Enforcement	☐ Employment Information
☐ Truncated SSN	☐ Education Information	☐ Military Status/Service
☐ Legal Status	☐ Emergency Contact	☐ Mailing/Home Address
☐ Place of Birth	☐ Driver's License	
☒ Other	☐ Race/Ethnicity	

Specify the PII collected.

This legacy system is no longer used to collect or maintain personally identifiable information (PII). The FBMS and its subsystems and data have been successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned.

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

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

Describe

This legacy system is no longer used to collect or maintain PII. The FBMS and its subsystems and data have been successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned.

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

☐ Paper Format ☐ Face-to-Face Contact ☐ Fax ☐ Telephone Interview

☐ Email ☐ Web Site ☒ Other ☐ Information Shared Between Systems

Describe

This legacy system is no longer used to collect or maintain PII. The FBMS and its subsystems and data have been successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned.

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

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information, please see the FBMS Cloud PIA.

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 or office and how the data will be used.

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information, please see the FBMS Cloud PIA.

☐ Other Bureaus/Offices

☐ Other Federal Agencies

☐ Tribal, State or Local Agencies

☐ Contractor

☐ Other Third Party Sources

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

No

State the reason why individuals cannot object or why individuals cannot give or withhold their consent.

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information, please see the FBMS Cloud PIA.

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

☐ Privacy Act Statement ☐ Privacy Notice ☐ Other ☒ None

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

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information, please see the FBMS Cloud PIA.

I. Will reports be produced on individuals?

No

Section 3. Attributes of System Data

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

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information, please see the FBMS Cloud PIA

B. How will data be checked for completeness?

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. For

further information, please see the FBMS Cloud PIA

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

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information, please see the FBMS Cloud PIA

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

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information, please see the FBMS Cloud PIA

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

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. All data has been migrated from the legacy infrastructure to the FBMS Cloud infrastructure. For further information, please see the FBMS Cloud PIA.

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 minimal risk to individual privacy as all FBMS data has been migrated to the FBMS Cloud system and the legacy hardware will be sanitized and disposed of. No personally identifiable information remains on the legacy infrastructure. The FBMS software is not being decommissioned; it has been migrated/converted to a new infrastructure provided by a Cloud Infrastructure As a Service (IaaS) provider in June 2015. The FBMS Cloud based systems and software are supported by a tested replication disaster recovery solution, so the legacy DOI FBMS infrastructure is no longer used and will be decommissioned. Please see the FBMS Cloud PIA for the description of the privacy risks and how the data is handled at each stage of the information lifecycle.

Server hard drives will remain within the Data Center organizational control until destroyed on site. The Data Center Manager has property custody of the servers until custody is transferred to a property officer within the Office of Facilities and Services(OFAS), Property Management Office. The entire storage hardware will be professionally sanitized (scrubbed) in accordance with standard DoD 5220.22-M specifications because it is being decommissioned. The hardware vendor will provide sanitization, verification, and certification. Backup tapes will remain within the data center's organizational control, and tapes will be recirculated in the tape library and FMBS data will be overwritten.

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?

No

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

No

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

No

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

No

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

Not applicable as this legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information, please see the FBMS Cloud PIA.

F. Are the data or the processes being consolidated?

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 ☐ Developers ☐ System Administrator

☐ Contractors ☒ Other

Describe

This legacy system is no longer used to collect or maintain PII. The FBMS and its subsystems and data were successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned. For further information, please see the FBMS Cloud PIA.

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

This legacy system is no longer used to collect or maintain PII. The FBMS and its subsystems and data have been successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned. For further information, please see the FBMS Cloud PIA.

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?

Privacy Act contract clauses are included in all contractor agreements.

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

No

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

No

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

This legacy system is no longer used to collect or maintain PII. The FBMS and its subsystems and data have been successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned. For further information, please see the FBMS Cloud PIA.

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

This legacy system is no longer used to collect or maintain PII. The FBMS and its subsystems and data have been successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned. For further information, please see the FBMS Cloud PIA.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

Describe

The FBMS legacy system and hardware are hosted in secured DOI facilities. This legacy system is no longer used to collect or maintain PII. The FBMS and its subsystems and data have been successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned. For further information, please see the FBMS Cloud PIA.

(2) Technical Controls. Indicate all that apply.

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

Describe

The FBMS legacy system and hardware are hosted in a secured DOI environment with appropriate security controls. This legacy system is no longer used to collect or maintain PII. The FBMS and its subsystems and data have been successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned. The entire storage hardware will be professionally sanitized (scrubbed) in accordance with standard DoD 5220.22-M specifications. For further information, please see the FBMS Cloud PIA.

(3) Administrative Controls. Indicate all that apply.

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

Describe

The FBMS legacy system and hardware are hosted in a secured DOI environment with appropriate security controls. This legacy system is no longer used to collect or maintain PII. The FBMS and its subsystems and data have been successfully migrated to an Infrastructure as a Service (IaaS) hosting provider in the Federal Cloud in 2015. As a result, the legacy FBMS infrastructure is no longer used or needed and will be decommissioned. The entire storage hardware will be professionally sanitized (scrubbed) in accordance with standard DoD 5220.22-M specifications. For further information, please see the FBMS Cloud PIA.

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, serves as the FBMS Information System Owner and the official responsible for oversight and management of the FBMS security and privacy controls and the protection of customer agency information processed and stored by the FBMS system. The Information System Owner and the FBMS 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 FBMS. Customer agency data in FBMS 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 processing complaints.

The legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information,

please see the FBMS Cloud PIA.

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 customer agency and agency data is properly managed and that all access to customer agency and agency 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 customer agency and agency PII is reported to the customer agency and US-CERT within 1-hour of discovery in accordance with Federal policy and established procedures. The customer agency data in FBMS 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.

The legacy system is being decommissioned and is no longer used to collect or maintain PII. For further information, please see the FBMS Cloud PIA.