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: Collections and Billings System
Bureau/Office: Bureau of Land Management
Date: November 7, 2019
Point of Contact:
Name: Suzanne S. Wachter
Title: BLM Associate Privacy Officer
Email: swachter@blm.gov
Phone: 202-912-7178
Address: 20 M Street SE, Washington D.C. 20003

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 purpose of the Bureau of Land Management (BLM) Collections and Billings System (CBS) is to maintain accounting and financial information associated with the normal accounting procedures of the BLM. The CBS application uses Enterprise Active Directory authentication, and provides a single electronic database containing standard and consistent data on payments made by the BLM's customers. The system can be used to prepare bills for the use of public lands and other goods and services that the BLM offers and then make collections against these and other bills. This data provides BLM employees with a centralized source for financial, collections, and billings information.

Specifically, the system will be used for the billing of uses of public lands (such as collection of payments for recreation sites, sand and gravel extraction, and timber harvesting). It is also used for the billing of other goods and services received from BLM (such as declining deposit accounts in BLM public rooms), follow-up, updating program files when payments are made, and accounting for monies. It will also include money which BLM employees owe the Bureau. Records in this system may be subject to use in approved computer matching programs authorized under the Privacy Act of 1974, as amended, for debt collection purposes.

C. What is the legal authority?

Federal Managers Financial Integrity Act (31 U.S.C. 3512; 31 U.S.C. 3711 through 3719; 41 CFR 301-304)
The Debt Collection Act of 1982 (Public Law 97-365, 96 Stat. 1749, as amended by Public Law 98-167, 97 Stat. 1104)
The Debt Collection Act of 199, (Public Law 104-134, 110 Stat. 1321 (6) 26 U. S.C. 6103 (m)(2) and U.S.C. 5514)

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: *UII Code - 010-000000094 00-04-01-07-01-00 and the System Security Plan (SSP) - CBS System Security Plan_20170721_mkl*
☐ 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.*
Management Information System (MIS)	The Management Information System (MIS) provides web-	No	N/A

	enabled reports and data entry systems for business, financial, program, and workload & performance measurement information.		

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)*

CBS is covered under DOI-86, Accounts Receivable: FBMS - July 28, 2008, 73 FR 43772. Both SORNs are available for viewing at https://www.doi.gov/privacy/sorn. Previously, CBS was under Interior/BLM-35, Collections and Billings System, 65 FR 502 (January 5, 2000). BLM-35 is being rescinded as it is redundant to DOI-86.

☐ 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
☒ Spouse Information
☒ Financial Information
☒ Credit Card Number
☒ Mailing/Home Address
☒ Social Security Number (SSN) of sole proprietors

Other: Tax identification numbers, reasons for payment and debt, method of payment (including checking account number, check number, or credit card information), amounts owed, routine billing and payment information used in accounting and financial processing, and purchase transaction information from purchases made via the BLM website through Pay.gov, a secure Department of Treasury website.

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*

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

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

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

The PII is used to record customer payment information or billing information required for processing payments and billing. It is also obtained when purchasing a lease, right-of-way, horse and burro purchases, certified copies of General Land Office records and any other BLM services or products. This is an Accounts Receivable system required for accounting of all financial transactions.

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.*

The data will be used in the creation of Bills and Transactions/Orders for customers doing business with BLM. Information may also be shared with other Bureaus/Offices as authorized and described in the routine uses contained in the DOI-86, Accounts Receivable: FBMS system of records notice.

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

Information may also be shared with other Bureaus/Offices as authorized and described in the routine uses contained in the DOI-86, Accounts Receivable: FBMS system of records notice.

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

Information is shared with the Department of Treasury for the purpose of collecting debts. Information may also be shared with other Federal agencies as authorized and described in the routine uses contained in the DOI-86, Accounts Receivable: FBMS system of records notice.

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

Information may also be shared with other Tribes, State or Local Agencies as authorized and described in the routine uses contained in the DOI-86, Accounts Receivable: FBMS system of records notice.

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

Information is shared with the Department of Treasury for the purpose of collecting debts. Information may also be shared with other Federal agencies as authorized and described in the routine uses contained in the DOI-86, Accounts Receivable: FBMS system of records notice.

☐ 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:

Customers have the opportunity to choose to provide information when making a purchase or conducting transactions with BLM, and may decline to provide requested information. However, without the requested program information they will not be able to complete transactions or purchase the requested item.

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

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

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

Individuals are provided a copy of a Privacy Act statement on various forms used by this system. A copy of the Privacy Act statement is also available upon request.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is also provided by publication of this privacy impact assessment and the DOI-86 Accounts Receivable: FBMS system of records notice.

☒ Other: *Describe each applicable format.*

BLM users are presented with a Security Warning Banner when logging into the CBS that informs them the system is protected and there is no expectation of privacy.

☐ None

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

Data can be retrieved primarily through a transaction number, bill number or vendor/customer name. A vendor code is also available, and if known, can be used to retrieve data.

I. Will reports be produced on individuals?

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

☒ No

Section 3. Attributes of System Data

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

BLM personnel are responsible for verifying that the information is correct. A product named "Dataflux" is used to standardize address information. The system has multiple edits to ensure required fields are populated. BLM personnel are responsible for verifying that the information is correct.

B. How will data be checked for completeness?

The system has multiple edits to insure required fields are populated. BLM personnel are responsible for verifying that the information is correct. A product named "Dataflux" is used to standardize address information.

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

The CBS data is governed by the Federal Financial Laws and Regulations that provide guidance on permanent and temporary records disposition. Financial auditors review the financial records on an annual basis for compliance with Federal laws and regulations.

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

The CBS data is governed by the Federal Financial Laws and Regulations that provide guidance on permanent and temporary records disposition. Financial auditors review the financial records on an annual basis for compliance with Federal laws and regulations. The National Archives and Records Administration's (NARA) approved records schedule is what determines retention for BLM records.

Records maintained in CBS are under permanent retention until transferred to NARA. Currently, there is no approved BLM records schedule for the records contained in CBS. However, it is in the process of being placed in a record schedule but will still be considered permanent records due to their financial nature.

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

This system contains no temporary records. CBS retains all transaction data since its implementation. No data has ever been archived or disposed of since implementation. CBS contains the detail level of every transaction while FBMS contains summary information.

The disposition procedures set forth by NARA for CBS are as follows; records for unscheduled systems are PERMANENT with cutoff every 5 years. The disposition authority states to "transfer a copy along with a public use version to NARA immediately, in accordance with NARA transfer instructions applicable at the time of transfer. Thereafter, transfer a copy every 5 years to NARA along with public use version that fully supersedes the previous accession".

The procedures used to electronically transfer the records in CBS are in accordance with NARA Bulletin 2012-03, issued August 21, 2012. This Bulletin informed Federal agencies that, beginning October 1, 2012, NARA will use Electronic Records Archives (ERA) for scheduling records and transferring permanent records to the National Archives. The procedures documented to electronically transfer data can be found in the Electronic Records Archive Agency User Manual.

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.

Safeguards for the CBS conform to the Office of Management and Budget (OMB) and DOI guidelines reflecting the implementation of the Computer Security Act of 1987 (40 U.S.C. 759). Only those employees who have been identified as collections agents and billing clerks have read/write access. The system is protected through user identification, passwords, database permissions, and software controls. The CBS security measures establish different access levels for different types of users.

CBS is classified as moderate for FISMA and has all of the required system security documentation and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, CBS has controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions and software controls. All employees including contractors must meet the requirements for protecting Privacy Act information.

Business rules and guidelines, as well as rules of behavior, have been established to prevent inadvertent disclosure to individuals not authorized to use the system or those who do not have a direct "need to know" certain information contained in the system. All end-users must complete the CBS Access Request Form (1372-8) to request a CBS account and access. The request must include the user's legal name including middle initial, organization code, email address, approval signatures and the level of CBS access required. The CBS State Lead will review the form to ensure that the requested roles are appropriate and adhere to proper separation of duties. The Lead will submit the form to the CBS Customer Service Staff. The CBS Customer Service Staff will review the CBS Access Request Form for signatures and role appropriateness. All new users will receive training on the use of the system. All DOI employees and contractors must complete mandatory privacy, security and records management training annually, and acknowledge the DOI Rules of Behavior.

The NOC Security Review Coordinator will conduct a security review of user accounts and appropriateness once each quarter during the fiscal year. The first three quarters require a full validation of all CBS users and a review of only new role assignments since the last review. The fourth quarter review will consist of a complete verification of all users and all roles currently assigned. The CBS management feels that any risks associated with this schedule are minimal and acceptable, and that the costs far outweigh the benefits of a full role review each quarter. Each quarter, the NOC Security Review Coordinator will send Security Reports to the Lead for review. The Lead will review the reports for inaccuracies and annotate findings in the appropriate field provided on the report. After review and notations, the Lead will complete and sign the CBS User Account Review Concurrence Section of the CBS User Account Management Review Form and forward it to their supervisor or manager. The Lead's supervisor or manager verifies that the Lead has performed the user account review, reviews the Lead's account, and annotates any corrections needed on the report. Then signs the CBS User Account Review Verification Section of the CBS User Account Management Review Form. This signature also grants the Lead authority to conduct the security review. The signed documents are returned to the Lead. The Lead will return the Security Reports, along with the signed CBS User Account Management Review Form to the BLM NOC CBS Security Review Coordinator by the due date for each quarter. The due date will be thirty days after the day the Security Reports are provided to the Lead.

The CBS SSP describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data via User ID, IP Address, etc. Audit trails are also captured within the system to determine who has added, deleted or changed the data within the system. Any qualification over-rides require that the account manager document the reasoning and the login name with date and time is added by the system. The CBS Security Review Coordinator will forward requests to inactivate accounts or remove roles to the CBS Customer Service Staff utilizing the BLM National Help Desk Remedy Ticket application. Please note that new users added and additional roles cannot be assigned through the Security Review process. New users and new roles must be requested through the process described in section I paragraph C, Requesting User Accounts and User Access. 6. The CBS Security Review Coordinator will maintain the returned Security Reports and CBS User Account Management Review Forms, along with any other pertinent documentation.

The CBS also has an audit trail that identifies and logs a specific user whenever data is added or modified.

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*
The CBS application provides a single electronic database containing standard and consistent data on payments made by the BLM's customers. The system can be used to prepare bills for the use of public lands and other goods and services that the BLM offers. This data provides BLM employees with a centralized source for financial, collections, and billings information. Only personal data essential to maintaining accounting and financial information associated with normal accounting functions of the BLM are in the system.

☐ 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?

No new data is derived by this system.

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

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

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

The CBS application is restricted to only BLM employees and its contractors. Roles are assigned by supervisors based on an employee's job responsibilities. The user's access to the CBS is restricted by the assigned role as stated by the supervisor.

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 involved in the design, development, and maintenance of the CBS. Privacy Act clauses are contained in their contracts and a nondisclosure statement has been signed by the contractor.

☐ 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*
CBS also has an audit trail that identifies and logs a specific user whenever data is added or modified.

☐ No

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

The only individuals identified and monitored are BLM employees and contractors who add, modify or delete data in the system. An audit trail, noting what data was changed when and by whom, is recorded within the system. CBS does register a complete audit trail that tracks all modifications and deletions by user, date, and time.

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

Safeguards for the CBS conform to the Office of Management and Budget (OMB) and DOI guidelines reflecting the implementation of the Computer Security Act of 1987 (40 U.S.C. 759). Only those employees who have been identified as collections agents and billing clerks have read/write access. The system is protected through user identification, passwords, database permissions, and software controls. The CBS security measures establish different access levels for different types of users.

The CBS also has an audit trail that identifies and logs a specific CBS user whenever data is added or modified within a transaction.

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 CBS Application Manager identified within this document is responsible for protecting the privacy rights of the public and employees affected by the application.

The Associate Director, National Operations Center (NOC) serves as the CBS Information System Owner and the official responsible for oversight and management of the CBS security controls and the protection of customer agency information processed and stored by the CBS system. The Information System Owner is 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 CBS. The Information System Owner 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, in consultation with the BLM Associate Privacy Officer.

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 CBS application is restricted to only BLM employees and its contractors. Roles are assigned by supervisors based on an employee's job responsibilities.

The CBS Information System Owner has responsibility for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner, the Information System Security Officer and any authorized users are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the BLM Associate Privacy Officer.