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: Legacy Rehost 2000 (LR2000)
Bureau/Office: Bureau of Land Management (BLM)
Date: March 5, 2020
Point of Contact:
Name: Suzanne S. Wachter
Title: BLM Associate Privacy Officer
Email: blm_wo_privacy@blm.gov
Phone: 202-912-7178
Address: 20 M Street SE, Washington DC

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 Bureau of Land Management (BLM) has the responsibility for maintaining the land and mineral records for the United States. LR2000 is a business-essential national system that provides internal and external customers with Intranet/Internet access to land status data. Land status data includes land and mineral use authorizations (permits, O&G leases, Rights of Ways, mineral leases, etc.), land title,

(exchanges, acquisition, conveyances, etc.), and segregation (withdrawals, classifications) data extracted from the BLM's case files that support the BLM land, mineral and resources programs. Information in the system has been collected for the purpose of establishing a public record of transfers of title to and from the Federal Government, authorized and unauthorized uses of public land. All trespass cases, unauthorized use cases, cultural resource cases, and paleontology cases are restricted from public viewing.

C. What is the legal authority?

Federal Land Policy and Management Act (43 U.S.C.1701)
The Uniform Relocation Act (42 U.S.C 4601)
The Act of April 25, 1812 (2 Stat 716)

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*

010-000000158; System Security and Privacy Plan for Legacy Rehost 2000

☐ No

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

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Case Recordation	Abstracted data from land and mineral, title, use authorization, and withdrawal cases	Yes	Names and addresses of customers

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Mining Claims	Abstracted data from more than three million mining claim cases	Yes	Names and addresses of customers
Status	Contains historic data abstracted from title cases that transferred surface and/or mining rights to or from the U. S., and restriction of U.S. rights	Yes	Names and addresses of customers
Historic Index	Abstracted data from use authorization cases and withdrawal cases that were closed prior to the implementation of Case Recordation	No	n/a
LLD/Land	Contains land descriptions in accordance with the cadastral or special survey	No	n/a
Customer/Master Name	Contains, names, address, name entity identification numbers (NIDS) and the category of name entities.	Yes	Names and addresses of customers
Bond/Surety	Contains bond and surety information for each office of the BLM	Yes	Names and addresses of customers
Cadastral Survey/Fiche	Provides an online index to the survey field notes maintained throughout BLM	Yes	Names and addresses of customers

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

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

This system is covered by the BLM - 32, Land & Minerals Authorization Tracking System 56 FR 5014, 7 February 1991, which may be viewed at https://www.doi.gov/privacy/blm_notices. The BLM-32 SORN is currently being revised to provide updated content for the system and incorporate new Federal government-wide requirements in accordance with OMB Circular A-108.

☐ No

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

☒ Yes: *Describe*

OMB Control Number 1004-0009, Land Use Application and Permit (43 CFR 2920), Expiration 31 March 2020

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Financial Information
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address
☒ Other: Case number, Interests relationships (the type of interest held), trespass, unauthorized access or use records and other information used to determine authorized use of lands.

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
☒ Web site
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems
☐ Other: *Describe*

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

Information in the system is collected for the purpose of establishing a record of transfers of title to and from the Federal Government and authorized uses of public lands. The LR2000 system contains the names, addresses, interest relationships and percent interest for individual, government entities, entrepreneurs, and other business entities holding permits, leases, or other authorizations to use public lands. All trespass cases, unauthorized use cases, cultural resource cases, and paleontology cases are restricted from public viewing and will be referred to organizations and maintained in those systems of records (e.g., IMARS).

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 in LR2000 is used to determine land status. Land status is defined as the availability of a given tract of land for use (government or private) or the disposal or lease of the land (or its resources) into non-federal ownership or tenure. Status results from actions recorded in the cumulative set of documents and records that define ownership and interest in lands and authorized uses on, and limitations to, use and ownership transfers. It is the BLM's responsibility to maintain the land and mineral data and it this data that is used to determine ownership and use of Federal lands and minerals. The agencies below have access to external data which does not contain PII.

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

The status of the land use may also be shared with other bureaus and offices as authorized and described in the routine uses contained in the BLM-32, Lands and Minerals Authorization Tracking system of records notice.

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

Information may also be shared with other Federal agencies as authorized and described in the routine uses contained in the BLM-32, Lands and Minerals Authorization Tracking 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 tribal, state or local agencies as authorized and described in the routine uses contained in the BLM-32, Lands and Minerals Authorization Tracking system of records notice.

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

Contractors perform maintenance and enhancements on the system and provide customer support to BLM personnel. The data is used as part of the routine operations and maintenance to validate system performance. Contractors do not have access to PII stored on the system.

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

Limited information from LR2000 released under a Freedom of Information Act (FOIA) request may be posted on a public website. It is the policy of the BLM to make records available to the public to the greatest extent possible, in keeping with the spirit of FOIA, while at the same time protecting sensitive information.

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.*

Individuals and corporations voluntarily provide information when applying to use, lease or permit on federally managed lands. The LR2000 system contains the names, addresses, interest relationships and percent interest for individuals, government entities, entrepreneurs, and other business entities holding permits, leases or other authorizations to use public lands. If the information is not provided the application process cannot be completed.

☐ 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:

A Privacy Act Statement is included on the Land Use Application and Permit form used by the program to collect information, and is posted on the official BLM website.

☒ Privacy Notice: *Describe each applicable format.*

Notice is also provided through the publication of this privacy impact assessment and the BLM-32, Land and Minerals Authorization Tracking system of records notice, which may be viewed at https://www.doi.gov/privacy/blm_notices.

☒ Other: *Describe each applicable format.*

When users access the system the following privacy act notice is displayed.

**** WARNING **** WARNING **** WARNING **** WARNING ****

PUBLIC LAW 99-474 PROHIBITS UNAUTHORIZED USE OF THIS U.S. GOVERNMENT COMPUTER AND/OR SOFTWARE. PUNISHMENT INCLUDES FINES AND UP TO 10 YEARS IN PRISON. REPORT SUSPECTED VIOLATIONS TO THE INSTALLATION IT SECURITY MANAGER. ALL USE OF THIS SYSTEM IS SUBJECT TO MONITORING.

NOTICE

Certain portions of this system are part of a Privacy Act System of Records (LLM-32).
ACCESS: Access to this information is limited to only those officers and employees of the Bureau of Land management who have a need for the information in the performance of their duties. Disclosure without the consent of the subject of the information is restricted unless required by the Freedom of Information Act, to those listed in the Federal Register Notice under the "routine use" section, for the purposes identified in that section, and to those identified in 43 CFR 2.56.

These records may not be altered or destroyed except as authorized by 43 CFR 2.52. Please contact your office's Privacy Act Coordinator for advice on disclosure restrictions.

CRIMINAL PENALTIES FOR DISCLOSURE: The Privacy Act contains provisions for criminal penalties for knowingly and willfully disclosing information from this file unless properly authorized. Fines shall not exceed more than $5,000.

ACCESS GUIDANCE: This system contains sensitive information including home addresses (street, city, and zip code) of private individuals for certain case types (e.g., acquisitions, donations, condemnations, road rights-of-way, and other agency rights-of-way), and trespass case file information, which must not

be released to the public, except as authorized under the Freedom of Information Act.

☐ None

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

The data can be retrieved by individual name and case number.

I. Will reports be produced on individuals?

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

BLM employees can generate ad hoc and annual reports on land use when logged in to the internal system, which may contain names and addresses of individuals with interest in a case. For reports that are produced for external use, case types that contain sensitive data are flagged, and the sensitive data is suppressed from the data results.

☐ No

Section 3. Attributes of System Data

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

BLM Field Office land mineral adjudication staff verifies the accuracy of data extracted from application forms prior to entry into LR2000 System.

B. How will data be checked for completeness?

BLM Field Office land and mineral adjudication staff verifies completeness of data extracted from application forms prior to entry into LR2000 System.

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

BLM Field Office land and mineral adjudication staff is responsible for entering designations and data updates from lessees/permittees into LR2000 action records.

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

Records maintained in LR2000 are covered by BLM records retention schedule 4/34 under disposition authority DAA-0049-2013-0004-0001, which was approved the National Archives and Records Administration (NARA). The LR2000 records are permanent and 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 retention period set forth by NARA on the LR2000 system records are PERMANENT and covered by disposition authority DAA-0049-2013-0004-0001. Per the DRS/GRS/BLM Combined Records Schedule, the LR2000 system is scheduled under Schedule 4 item 34, LEGACY REHOST SYSTEM (LR2000) and Schedule 4/34(a), Master File. The content of the LR2000 system and its modules includes land survey information and documentation of actions taken, abstracted from BLM case files, including case files information from ownership and authorization records, property rights and use permits affecting public lands, survey information, federal land and mineral ownership information, withdrawals, classifications and determinations, and bonding information. The database contains the names, addresses, interest relationships and percent interest for individuals, government entities, entrepreneurs, and other business entities holding permits, leases, or other authorizations to use public lands.

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

The LR2000 records are permanent and 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 disposition procedures set forth by NARA for LR2000 are as follows; LR2000 records 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 applicableat the time of transfer. Thereafter, transfer a copy every 5 years to NARA along with public use version that fully supersedes the previous accession". These disposition instructions can be found in the Combined Records Schedule under Schedule 4, Item 34(a), LEGACY REHOST SYSTEM (LR2000) Master File.

The procedures used to electronically transfer the records in LR2000 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 LR2000 conform to the Office of Management and Budget (OMB) Circular A-130 and Department guidelines reflecting the implementation of the Computer Security Act of 1987 (40 U.S.C.759). LR2000 data is protected through user identification, strong passwords, database permissions and software controls. Such security measures establish different access levels for different types of users. For example, access rights for non-BLM users will allow them to query portions of the database, but will not permit them to modify the data or to view personal information protected under the Privacy Act, such as names and home addresses or private non-entrepreneurial individuals. Specific BLM employees will have a level of access that will allow them to enter new case information. Higher levels of access will allow authorized Bureau employees to grant or remove passwords, correct or update the software, and impose of remove security controls.

There is a moderate privacy risk due to the type and volume of personal information maintained in LR2000. Information collected and used is limited to the minimum required to perform the purpose and functions of LR2000. To mitigate privacy risk, BLM has restricted access to personally identifiable information within LR2000 to a limited number of users.

There is a risk that individuals may gain unauthorized access to the information in the system. System security controls are in place to prevent access by unauthorized individuals to sensitive information. LR2000 is classified as a high value asset for FISMA and has all of the required security documentation and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, LR2000 has controls in place to prevent the misuse of 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 LR2000. All end-users have an individual password and ID that is issued by the LR2000 application steward. All new users will receive a user guide detailing the appropriate use of LR2000. All DOI employees must complete mandatory privacy, security and records management training annually, and acknowledge the DOI Rules of Behavior.

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. Accounts are reviewed annually to ensure that only authorized personnel have LR2000 logins. Additionally, any account that is inactive for more than one year is automatically suspended. All personnel accessing LR2000 must acknowledge the rules of behavior prior to each login. The System Security Plan describes the practice of audit trails. Audit trails maintain a record of activity and user activity including invalid logon attempts and access to data via User ID, IP Address, etc. Audit trails are also captured within LR2000 to determine who has added, deleted or changed the data within LR2000. Any qualification overrides require that the account manager document the reasoning and the login name with date and time is added by LR2000. The website uses https secure data transmissions.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the consent received by the individual when providing information, by the publication of this PIA and the Legacy Rehost 2000 notice, and the Privacy Act statement provided on the application and the official BLM website.

There is minimal risk due to the nature of the records being permanent. These records provide valuable insight into how public lands are managed by the US Government.

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*

LR2000 provides Bureau employees and customers with a centralized source of land status information such as ownership (agency, State, etc.), use authorizations (permits, rights-of-way, mining claims, mineral leases, bond & surety, etc.), and segregation (withdrawals, classifications, etc.). Information in the system has been collected for the purpose of establishing a public record of transfers of title to and from the Federal Government and authorized uses of public lands.

☐ 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.

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 dataor will access be restricted?

User access for LR2000 is determined based upon the role of the BLM employee and the level of access necessary to complete the user's functions. The LR2000 Legacy Transaction Processing Data Base (LTPDB) provides authorized BLM users, access to create, read, update, and delete data, and provide Serial Register Page reports on a case-by-case basis. The LR2000 Legacy Reporting Data Base (LRDB)

provides access for BLM users to all reports and access for External users to various publicly available reports. The data in the LRDB is updated from the LTPDB on a nightly basis. LR2000 Reports are web enabled. BLM DOI Office of Natural Resource Revenue, Bureau of Reclamation and U.S. Forest Service personnel access the LR2000 Public reports via the internet. Public versions of the LR2000 reports, minus sensitive and proprietary information, are accessible to the public via the Internet. The records shown on the BLM LR2000 public site are all classified as Category 1 Records. It is the policy of the BLM to make records available to the public to the greatest extent possible, in keeping with the spirit of FOIA, while at the same time protecting sensitive information.

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

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

Contractors who work at the BLM have access to the system. FAR clauses are included in the contracts.

☐ 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*

The Assessment and Authorization (A&A) process requires a system security plan (SSP) outlining the implementation of the technical controls associated with identification and authentication. The LR2000 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.

☐ No

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

The logs contain the user ID, date/time of access, invalid logon attempts, user activity, and asidentified in the previous response, IP address for the employee who entered or modified the database record, but does not link it to any other PII information.

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

Violations of the following Rules of Behavior are considered IT security incidents. According to the Department of Interior Manual 375 DM 19.11B, all suspected actual or threatened incidents involving the destruction, physical abuse or loss of technological resources shall be reported to the appropriate authorities. BLM employees shall report observed security incidents to their supervisors or the local Information System Security Officer (ISSO). The ISSO may recommend the removal of any individual User ID and password from any BLM computer system in the event of a security incident. Other controls include access controls, least privileges, training, and monitoring user activities.

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 redressor amendment of records.

The BLM Assistant Director for WO-300, Energy, Minerals, and Realty Management, serves as the LR 2000 Information System Owner and the official responsible for oversight and management of the LR 2000 security controls and the protection of customer agency information processed and stored by LR 2000. 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 LR 2000. 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 BLM Assistant Director for WO-300, Energy, Minerals, and Realty Management, 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 LR 2000 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.