



U.S. Department of the Interior PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our [Privacy Office Support Request Page](#). For further guidance, consult the [DOI PIA Guide](#).

System Information

System or Project Name:	General Land Office Records Automation System
System or Project Acronym:	GLORAS
Date submitted for review:	February 27, 2026
System Operational Status:	Operational

Point of Contact

Name:	Adrienne Brooks-Hill
Title:	Privacy Officer
Office:	Office of the Chief Information Officer
Phone:	202-208-1605
E-mail:	DOI_Privacy@ios.doi.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

- | | |
|--|--|
| ☐ New System | ☒ Significant Modification |
| ☐ New Electronic Collection | ☐ Other: Describe below |

Total modernization [REDACTED]

2. What is the purpose of the system or project?

The General Land Office Records Automation System (GLORAS) provides public online access to historical Federal land records maintained by the Bureau of Land Management. The system allows users to search, view, and download land patent records and related document images, including survey plats, field notes, tract books, master title plats, and control document index records.

This PIA covers only the website application for the land records. Any other connected processes are not covered by this PIA (i.e. the paper records and the process by which members of the public request and are

provided the certified copies of the records).

For additional information on authentication please see the EHI PIA on the DOI Privacy website (<https://www.doi.gov/sites/doi.gov/files/ehi-pia-final-09.29.2021.pdf>).

3. Is the system registered in BisonGRC?

- ☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

UII code: 010-000000111

System Name: General Land Office Records Automation System, BLM-0413SYS-2125

4. What legal authorities authorize the collection and use of data in this system or project?

1 Stat. 464, The Public Land Act of 1796 2 Stat. 716; The General Land Office Act, April 25, 1812, 9 Stat. 395, Establishing Act of March 3, 1849

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

- ☒ Yes: If yes, list the applicable citations below.
☐ No

BLM-42 General Land Office Records Automation System, 79 FR 30158, any information entered into CBS is covered under DOI-86, Accounts Receivable: FBMS - 73 FR 43772 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021). Both SORNs are available for viewing at <https://www.doi.gov/privacy/sorn>.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

- ☐ Yes
☒ No

Answer "Yes" if the project collects the same information from ten (10) or more members of the public in a 12-month period using information technology. If "Yes," provide the OMB Control Number or note that a request for approval is in progress.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

None

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

- | | | |
|--|---|---|
| ☒ Name (full, first or last) | ☐ Home telephone number | ☐ Employment or resume info |
| ☐ Aliases/nickname | ☐ Personal Email | ☐ Full or Truncated SSN |
| ☐ Driver's license | ☐ Mailing or home address | ☐ Physical characteristics |
| ☐ Citizenship | ☐ Religious preference | ☐ Biometrics or facial recognition |
| ☐ Legal Status | ☐ Mother's maiden name | ☐ Vehicle information |
| ☐ Sex | ☒ Marital status | ☐ Passport information |
| ☐ Race or ethnicity | ☒ Spouse Information | ☐ Travel information |
| ☐ Date of birth | ☐ Child or family information | ☐ Parent's name |
| ☐ Place of birth | ☐ Emergency contact info | ☐ Credit card number |
| ☐ Personal cell phone number | ☐ Financial information | ☐ Nationality |
| ☒ Tribal or other ID number | ☐ Education information | ☐ Disability Information |
| ☒ Military records | ☒ Other: Describe below | |

Records in the system include, but are not limited to, information related to historical land documents, homestead certificates, cash patents, military warrants, and railroad grants, including survey plats and field notes, land status records and controlled document indexes. Information not marked above that can be found within these records may include but are not limited to: county, township, range, meridian, section number, Land Office, document number, Indian Allotment number, survey number, authority for the grant, issue date, geographical name of the property, mining claim, survey type, contract/group number, survey approved date, and document type. GLORAS front end allows users to add copies to a shopping cart. Once the user is content with their cart, the user proceeds to generate a print-ready document with the following details: line items of each record being requested, subtotals and totals, [REDACTED]

[REDACTED] Any privacy information (home address, telephone number, financial information, and bank account information) collected for processing payments for purchasing products is not collected through GLORAS, all payments are completely processed through CBS and are covered in the CBS PIA and DOI-86 Accounts Receivable: FBMS SORN. This is provided for informational purposes only. The process by which members of the public purchase certified copies past the initial shopping cart form generation are not covered by this PIA.

2. What is the source for the PII collected? Check all that apply.

- | | |
|--|---|
| ☒ Individual | ☒ DOI Records |
| ☒ Federal Agency | ☐ Third Party Records |
| ☐ Tribal Agency | ☐ State Agency |
| ☐ Local Agency | ☐ Other: <i>Describe Below</i> |

GLORAS maintains records of historical significance related to land records. As such, these records may be originally from federal entities no longer in existence.

3. How will the information be collected? Check all that apply.

- | | |
|--|--|
| ☒ Paper Format | ☐ Fax |
| ☐ Email | ☐ Telephone Interview |

- ☐ Face-to-Face Contact
☐ Website

- ☒ Shared Between Systems: *Describe*
☒ Other: *Describe*

Information that meets the requirements of The General Land Office Act, April 25, 1812, and is collected via the BLM LR2000 (land description records) and Enterprise Geographic Information System (eGIS) (geospatial data related to land records) systems may be downloaded into GLORAS. For additional information regarding MLRS and eGIS, their PIAs may be viewed at <https://www.doi.gov/privacy/pia#BLM>.

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

The system of records contains information collected from publicly available historical Federal land conveyance documents (land patents, survey plats, field notes and land status records) maintained by the BLM General Land Office. The purpose of this system is to maintain, protect and preserve more than five million documents of historical relevance and to make these valuable resources for natural resource agencies, historians, surveyors, title companies, and genealogists available via the General Land Office Records Website.

5. How does this project limit the collection and use of PII to only what is necessary?

The system of records contains information collected from publicly available historical Federal land conveyance documents (land patents, survey plats, field notes and land status records) maintained by the BLM General Land Office (GLO). As new documents are created, they will be added and could contain PII. The GLO system limits data entered into the database to the fields declared above. The new documents digitized in the system could contain PII, the same as historical documents currently in the system.

Section 3: Data Sharing and Individual Rights

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

- ☒ **Within the Bureau/Office:** Describe how the data will be used below.
☐ **Tribal, State or Local Agencies:** Describe how the data will be used below.
☐ **Other Bureaus/Offices:** Describe how the data will be used below.
☒ **Contractor:** Describe how the data will be used below.
☒ **Other Federal Agencies:** Describe the federal agency and how the data will be used
☒ **Other Third-Party Sources:** Describe how the data will be used below.

By federal law, land records are public information. The primary purpose of GLORAS is to make historical land documents-survey plats and field notes, homesteads, patents, military warrants, and railroad grants available to the public, or other organization as authorized and described in the routine uses contained in the BLM-42, General Land Office Records Automation System (GLORAS) system of records notice. Please see <https://www.doi.gov/privacy/sorn>.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with

which it shares information?

- ☐ Yes
☒ No

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

- ☒ 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.*

Individuals voluntarily provide their information when requesting a land record. Any privacy information (home address, telephone number, financial information, and bank account information) collected for processing payments for purchasing GLORAS products is processed through CBS, and individuals can voluntarily consent to providing their information or may decline to provide information to purchase products. Please see the CBS PIA and the FBMS SORN at <https://www.doi.gov/privacy>.

Records on GLORAS are historical documents. Individuals do not have an opportunity to consent as any PII within the system is found on historical land records. By federal law these are public records. GLORAS does not collect or maintain any new PII from individuals within the system.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

- ☒ Privacy Act Statement: ☐ Other: *Describe Below*
☒ Privacy Notice: ☐ None: *Example - law enforcement cases.*

The Privacy Act Statement will be available via a linked web page, as well as a PDF file that can be downloaded and printed.

Additionally, a link to DOI's Privacy Notice is located on the General Land Office Record's website. Notice is also provided through the publication of this privacy impact assessment, the privacy impact assessment for CBS, the BLM-42 General Land Office Records Automation System and the DOI-86, Accounts Receivable: FBMS system of records notice, both of which may be viewed at <https://www.doi.gov/privacy/sorn>.

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

Historical documents may be retrieved by any searchable field to include names of individuals, county, township, range, meridian, section number, Land Office, document number, Indian Allotment number, survey

number, authority for the grant, issue date, militia grant, tribe, geographical name of the property, mining claim, survey type, surveyor name, contract/group number, survey approved date, and document type.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

- ☐ Yes: Describe the use of these reports and who will have access to them.
☒ No

No reports on individuals are produced.

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

Any information collected for payment from the individual is presumed to be accurate upon submission.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

The BLM Records Retention schedule is BLM 4/33a, which has been approved by the National Archives Records Administration (NARA). Records for GLORAS are permanent with a cut off every 5 years for transmission to NARA. Transfer a copy of the master file to NARA upon approval of this schedule, along with the technical documentation, in accordance with 36 CFR 1235.44-50. Thereafter, transfer a copy every 5 years, along with the current technical documentation. (N1-049-09-4, 1a). Payment information is covered under CBS. The records are under permanent retention until transferred per the Departmental Records Schedule, Administrative Schedule, B. [0011] Longterm Financial and Acquisition Records

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

Any information collected for payment from the individual is presumed to be accurate. The data contained in this system consists of electronic reproductions of official land records. No validation is necessary beyond initial quality control check of the image.

3. Does the project include logging capabilities to record and monitor access to PII?

- ☒ Yes
☐ No

[REDACTED] and logs are saved [REDACTED]
[REDACTED] This will allow the GLORAS administrative users to monitor and review the logs weekly as well as security to review the logs. The logs include administrator and user access, performance monitoring, and file conversion processes. [REDACTED] for the retention period above.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

There are minimal risks to the privacy of individuals due to the type of PII contained within GLORAS. There are over 12 million records in the GLO database related to official government survey plats, field notes, and land patents (titles). The data collected in GLO are attributes related to the scanned image of title documents dating back to 1788. Title documents are a matter of public record. Any individual has the right to research and obtain copies of these records from the BLM, most often in a BLM public room. The collection, retention, and processing of the data is secured within the BLM and hosted behind the BLM DMZ (firewall). No user data is actively collected or requested from visitors on the website. GLORAS is classified as low for FISMA and has all the required system security documentation and a current Authority to Operate (ATO).

In accordance with OMB Circulars A-123 and A-130, GLORAS has controls in place to prevent the misuse of the data by those having access. For system administration, GLORAS can only be accessed within the BLM network. Security measures and controls consist of two factor authentication, 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 internal users are authenticated using Government PIV cards for access. All new users receive training on the use of the system. 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 the underlying metadata 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 systems logins.

Additionally, any account that is inactive for more than one year is automatically suspended. All personnel accessing the system 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 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 overrides require that the account manager document the reasoning and the login name with date and time added by the system.

There is minimal risk due to the nature of the records being permanent. Adherence to the records schedule, described in Section 4.1 of this PIA minimizes retention risks. These records are historical in nature and provide valuable insight into how land has been transferred by the US Government. There is moderate risk for the information submitted to purchase land records that are processed within CBS. Please see the CBS PIA for evaluation of privacy risk (<https://www.doi.gov/privacy/pia#BLM>).

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

- ☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
☒ No

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

- ☐ Yes: *Provide explanation below*
☒ No

New data will not be stored in an individual's records.

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

- ☐ Yes: *Provide explanation below*
☒ No

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

N/A

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

- ☒ Yes
☐ No, *Proceed to Section 7.*

2. How are models validated for fairness, accuracy, and transparency?

Human reviewers serve as a "human in the loop," validating all AI-generated recommendations to ensure fairness, accuracy, and transparency. AI is used by GLO to extract text out of the documents and insert the data into the correct fields in the database to reduce labor needs on data collection. The text captured and inserted by the system is reviewed by humans to ensure the correct data is inserted into relevant fields.

For this process, GLORAS uses optical character recognition (OCR), but not machine learning. The OCR is part of a FedRAMP approved software package as a commercial-off-the shelf product [REDACTED] and meets all FedRAMP security requirements.

3. Are individuals notified of AI-based decisions that affect them?

- ☒ Yes
☐ No

Individuals are notified, and a human in the loop reviews and approves all AI-generated recommendations before they are acted upon.

4. Are safeguards in place to prevent bias or unintended consequences?

- ☒ Yes
☐ No

Yes. Human oversight is built into the process to validate and approve all AI-generated recommendations, reducing the risk of bias or unintended outcomes.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

- ☒ Yes
☐ No

Yes. Models undergo periodic review and updates in alignment with their lifecycle and designated end-of-life (EOL) schedules. This ensures continued reliability, relevance, and alignment with current performance and security requirements.

6. Is federated learning used for privacy-preserving model training?

- ☐ Yes
☒ No

No model training is happening.

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

- | | |
|---|--|
| ☒ Users | ☒ System Administrator |
| ☒ Contractors | ☒ Other: <i>Describe below</i> |
| ☒ Developers | |

Users of the systems fall into these four categories: the public, GLO system administrators, contractors, and software agents. Public access is limited to the web interface, which allows only retrieval of land patent metadata and images. No username or password or user email address is required for access. All privacy data accessed by the public is land grant information that is required to be made publicly available under federal law.

GLO system administrators with authorized privileges may use database administration tools, such as Microsoft SQL Management Studio, to access, modify, and update data within the GLO. When required to support

operational responsibilities, system administrators may grant on-site contractors temporary administrator-level privileges. Automated software agents (including engines, services, and scheduled jobs) operate under least-privilege service accounts, meaning they are granted only the specific permissions necessary to perform their assigned tasks.

2. What data protection policies apply to cloud-based PII storage?

FedRAMP authorization, NIST SP 800-53 Rev. 5 controls, DOI Cloud Computing Policy. These are the policies applied to the cloud infrastructure to ensure compliance and monitor the environment [REDACTED].

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

The system monitors and detects unauthorized access, use, or exfiltration of PII by applying policies aligned with FedRAMP Moderate authorization and NIST SP 800-53 Rev. 5 controls. Compliance is enforced through [REDACTED] and platform logging provide ongoing visibility into the cloud environment. All relevant logs are also forwarded to the BLM-managed SIEM for centralized monitoring and threat detection.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.

☐ No

Yes, the application logs all changes and access to the data via logging that [REDACTED]. The logs are secured by Role Based Access Control (RBAC) following DOI requirements so that Zero Trust is followed and only administrators who should be reviewing the logs as part of their duties have access to the logs.

5. Will contractors be involved in the following project activities? Check all that apply.

- ☒ Design
- ☒ Development
- ☒ Maintenance

Contractors are involved with the design, development, and maintenance of the system. Contractors are required to take annual security and privacy training to be granted access to BLM resources. The contract included standard FAR clauses.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

- | | |
|--|---|
| ☒ Security Guards | ☒ Cipher Locks |
| ☒ Key Guards | ☒ Identification Badges |
| ☒ Locked File Cabinets | ☒ Safes |
| ☒ Secured Facility | ☒ Combination Lock |

☒ Closed Circuit Television

☐ Other: *Describe Below*

Technical Controls

☒ Password

☒ Firewall

☒ Encryption

☒ User Identification

☐ Other: *Describe Below*

☒ Intrusion Detection Systems (IDS)

☒ Virtual Private Network (VPN)

☒ Public Key Infrastructure (PKI) Certificates

☐ Biometrics

Describe the other types of controls implemented.

Administrative Controls

☒ Periodic Security Audits

☒ Backups Secured Off-site

☒ Rules of Behavior

☒ Role-Based Training

☐ Other: *Describe Below*

☒ Methods to Ensure Only Authorized Personnel Have Access

☒ Encryption of Backups Containing Sensitive Data

☒ Mandatory Security, Records and Privacy Training

☒ Regular Monitoring of Users' Security Practices

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

The Privacy Officer and GLORAS System Manager are responsible for protecting the privacy rights of the public and employees affected by the interface. The State Director for Eastern States is the GLORAS Information System Owner and the official responsible for oversight and management of the GLORAS security and privacy controls and the protection of agency information processed and stored in the GLORAS application. The Information System Owner and GLORAS Privacy Act System Manager, in collaboration with the BLM Senior Management Team, are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in the GLORAS application. These officials and authorized GLORAS personnel are responsible for protecting individual privacy for the information collected, maintained, and used 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 BLM Privacy Officer.

8. What processes are in place for individuals to access their information?

An individual may file a Privacy Act request to seek records about themselves, request amendment or correction of records. The DOI procedures for filing Privacy Act requests are found at the following website, <https://www.doi.gov/privacy/privacy-act-requests>.

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Follow the steps listed under the Requesting Amendment or Correction of Records under the Privacy Act section at this URL: <https://www.doi.gov/privacy/privacy-act-requests>.

10. 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?

Responsibility rests with the users of the system and the System Owner, the State Director for Eastern States. All users receive system training, and all BLM employees and contractors are required to complete periodic Privacy Act training. All federal employees comply with the requirements in OMB Circulars A-123 and A-130 as well as the Departmental Manual, 383 DM 3, Privacy Act – Bureau Responsibilities. The GLORAS Information System Owner and the BLM Information System Security Officer 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 procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the DOI Privacy Office.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

In the event of a privacy breach involving GLORAS DOI will follow the procedures outlined in the DOI Privacy Breach Response Plan:

1. Immediate Reporting – Any suspected or confirmed breach must be reported within one hour of discovery to the DOI Computer Incident Response Center (DOI-CIRC) and the DOI Privacy Officer.
2. Containment and Mitigation – The ISSO and DOI-CIRC work to secure affected systems, revoke compromised credentials, and prevent further data loss.
3. Risk Assessment – The Privacy Officer and breach response team assess the nature and scope of the breach, the sensitivity of the compromised PII, and the potential risk to affected individuals.
4. Notification – If required, affected individuals will be notified without unreasonable delay, consistent with OMB M-17-12 and DOI policy, providing:
 - a. A description of the incident
 - b. The type of information involved
 - c. Steps individuals can take to protect themselves
 - d. DOI contact information for questions and assistance
5. Oversight Reporting – DOI will report to OMB, Congress, DHS, and other required oversight bodies when thresholds for major incidents are met.
6. Remediation and Prevention – The system team will implement additional controls, update procedures, and retrain personnel to prevent recurrence.

These steps ensure a coordinated, timely, and compliant response to mitigate harm to individuals and uphold DOI's legal obligations.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

The GLORAS PIA will be reviewed every three (3) years, in accordance with the E-Government Act of 2002, or updated whenever major changes occur to the system's technology, data, or operations that could affect privacy risks.