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: Bureau of Land Management (BLM) General Support System (GSS)
Bureau/Office: Bureau of Land Management (BLM)
Date: May 23, 2023
Point of Contact
Name: Catherine Brean
Title: BLM Associate Privacy Officer
Email: blm_wo_privacy@blm.gov
Phone: (830) 225-3459
Address: Bureau of Land Management, 1849 C Street NW, Room no. 5644, Washington, DC 20240.

Section 1. General System Information

A. **Is a full PIA required?**
☒ Yes, information is collected from or maintained on
☐ Members of the general public
☒ Federal personnel and/or Federal contractors
☐ Volunteers
☐ All

B. 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) General Support System (GSS) is defined as a common BLM infrastructure consisting of file and print servers, workstations, and wide area network (WAN)/local area network (LAN) services and includes all information resources that are not part of any other GSS or major application. The design and proper operation of the GSS is accomplished using current technology, including switches, routers, firewalls, and other

equipment through which sensitive data may pass or be temporarily retained. Direct access to these devices is restricted to designated personnel authorized to work on select equipment.

The BLM GSS is the infrastructure necessary to facilitate Web and Intranet application hosting, directory services and other network services for the Bureau enterprise network. BLM GSS does not store information or process data directly and any systems hosted have their own security and privacy documentation. The BLM GSS devices are related primarily to network infrastructure and are in strategic areas supporting BLM State, District, Field, and Center offices throughout the United States. This includes approximately 16,000 workstations and 1,500 servers. Access to the BLM GSS is controlled by DOI's Active Directory (AD) user accounts and group membership managed and provisioned through the Enterprise Hosting Infrastructure/Enterprise Directory Services.

The primary end users of applications and services being hosted on the BLM GSS are federal employees and contractors supporting the BLM mission. The BLM GSS functions as a medium for a wide range of major and minor applications to interface with users and possibly share data among applications and other support systems. The BLM GSS principally provides the underlying support infrastructure for the daily business functions of the BLM and is not intended to act as an application or permanent storage medium for any data types.

All major applications, minor applications, and other GSS dependent on the BLM GSS are subject to separate accreditation boundaries and have their own separate accreditations and privacy impact assessments (PIAs). Program managers or system owners complete these PIAs, which undergo review by the assigned Information System Security Officer and the Bureau Associate Privacy Officer Office. The following link has examples of the BLM GSS components with separate PIAs, which can be viewed under the Bureau of Land Management section on the DOI Privacy PIA site Privacy Impact Assessments | U.S. Department of the Interior (doi.gov).

C. What is the legal authority?

- 5 U.S.C. 301, Department Regulations
- 44 U.S.C. Chapter 35, Paperwork Reduction Act
- 40 U.S.C. 1401, Clinger-Cohen Act of 1996
- E-Government Act of 2002 (Public Law 107-347)
- Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

CI. 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*

UII Code: BLM GSS Infrastructure 010-000000120, IT Helpdesk Support 010-000000132;

BLM GSS - System Security and Privacy Plan

☐ No

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

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	

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

☐ Yes:

☒ No

The BLM GSS is not a Privacy Act system of records. It does not collect or use personally identifiable information (PII) to directly retrieve records on individuals. The BLM GSS provides WAN/LAN, local file and print server, and endpoint management support, which consists of workstations, local file storage, and print devices. The PII maintained in the file storage or workstations the BLM GSS supports are covered by applicable published Government-wide, DOI-wide, or DOI bureau/office system of records notices (SORNs). These SORNs may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

Personal Identity Verification (PIV) credentials required to access the BLM GSS and DOI network are covered under INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021).

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

☐ Yes: *Describe*

☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Other: Active Directory (AD) username. The BLM GSS was not designed to collect PII; however, users may store PII on their file shares. Name, username, workstation name, and AD group information are collected to provide support to users. As the primary IT infrastructure used by the BLM to host information systems that collect, process, disseminate, and store information in support of the BLM's mission, the GSS collects, stores, and transmits a large volume of sensitive information of many types, including personally identifiable information (PII). This PII may relate to multiple program areas the BLM is responsible for managing, such as Energy and Minerals, Recreation and Visitor Services, National Conservation Lands, Wild Horses and Burros, Paleontology, Public Safety, Fire and Aviation, Law Enforcement, National Operations Center, Business Management, Human Resources, and Information Technology. See the applicable PIAs for a privacy risk assessment of the PII collected by these systems at https://www.doi.gov/privacy/pia.

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: The BLM GSS was not designed to collect PII; however, users may store PII on their file shares for the purpose of official work duties. The BLM GSS requires multi-factor authentication through a DOI-issued PIV card or network username and password. Access to the BLM GSS is controlled by AD user accounts and group membership managed and provisioned through the Enterprise Hosting Infrastructure/Enterprise Directory Services.

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

For DOI employees and contractors, the information is used to identify and authenticate the user's ability to access the system. Other than logs for auditing purposes, the BLM GSS does not collect sensitive information. If an individual tries to access information via the firewall, his/her IP address is collected, which will enable BLM to identify that person's general location.

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

☒ Within the Bureau/Office:

Information may be shared with BLM information resources, human resources, contract management staff, or other management staff on a need-to-know basis. The primary use of PII is to enable and maintain authorized access to the BLM GSS to accomplish the business-related and mission-related applications used by the BLM. Initially, the information is used to specify a username, user account, and temporary password, which the user is prompted to change at first use. Access to the BLM GSS includes a number of services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the network.

☐ Other Bureaus/Offices:

☒ Other Federal Agencies:

PII may be shared with the Department of Homeland Security for security compliance purposes or to report breaches and with the United States Forest Service (USFS) personnel with whom the BLM has authorized access to BLM intranet resources to support interagency operations.

☐ Tribal, State or Local Agencies:

☒ Contractor:

For DOI contractors, the information is used to identify and authenticate the user's ability to access the system. Information may also be shared with contractors who perform maintenance services or support BLM activities related to the BLM GSS.

☐ 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?

☒ Yes:

Information is voluntarily provided by employees and contractors in order to obtain access to the DOI network and BLM GSS-hosted information systems. Users have the opportunity to consent during the onboarding process, and verification of approval to work is required to enforce access controls across the DOI network. Human Resource staffing forms used to collect the information are required to clearly display a Privacy Act statement that informs individuals that providing the information is voluntary and the consequences of not providing the information may impact employment. If users decline, they will not be issued an AD account and may not be able to perform their official duties.

☐ 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.*

☒ Privacy Notice:

Notice is provided through the publication of this PIA. Users may view the INTERIOR/DOI-47 SORN for use of logical access records on the DOI SORN website at *https://www.doi.gov/privacy/sorn*.

☒ Other:

A pre-login banner that meets the DOI and National Institute of Standards and Technology (NIST) requirements is displayed on the screen at the initial point of login.

☐ 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 BLM's AD access log data is sorted and retrievable by the individual's AD username and the hostname or IP address of the hardware device the individual was attempting to log on/access.

I. Will reports be produced on individuals?

☒ Yes:

The BLM GSS may produce audit logs or reports on user activity in accordance with DOI logging requirements. The logged information is used to ensure the security of the system and for investigative actions associated with cyber security incidents.

☐ No

Section 3. Attributes of System Data

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

The only non-DOI records collected are the AD log-on credentials of United States Forest Service (USFS) personnel whom the BLM has authorized access to BLM intranet resources. Prior to associating a USFS staff member's United States Department of Agriculture (USDA) LincPass log-on credentials to his/her BLM account, the BLM verifies the accuracy directly with the USFS staff member requesting the access.

B. How will data be checked for completeness?

Users are responsible for the completeness of the data provided during the onboarding process and in the user account request form.

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

AD ensures the data is current. If a BLM staff member has left the BLM or changed his/her name, the BLM's on-boarding/off-boarding Remedy ticket process ensures that AD is updated to reflect all personnel changes.

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

Records and data maintained in the BLM GSS are retained in accordance with the Departmental Records Schedule (DRS)/General Records Schedule (GRS)/BLM Combined Records Schedule, Schedule 24 - Information Technology Operations and Management Records, Item 6.b., User Identification, Profiles, Authorizations, and Password Files, Excluding Record Relating to Electronic Signature. System access records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate system access by users and may include records such as user profiles, log-in files, password files, audit trail files and extracts, and system usage files. Disposition is temporary, and cutoff is when the BLM determines they are no longer needed for administrative, legal, audit, or other operational purposes. Destruction occurs no later than three years after cutoff.

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

The BLM GSS uses the dispositions procedures as defined in the DRS/GRS/BLM Combined Records Schedule. Cutting off files involves breaking or ending files at regular intervals, usually at fiscal or calendar year end, to permit their disposal or transfer. All temporary records are scheduled for destruction, either at their cutoff date, or after a specific time period after cutoff. BLM-approved disposition of paper records includes shredding, and electronic records are deleted in accordance with NARA guidelines and DOI policy.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a risk to the privacy of individuals due to the use of user accounts to access the BLM GSS. Only limited PII is used to manage user access to ensure the security of the system. There is an additional risk from users storing PII on their personal file shares. All users are subject to Federal law and regulation and DOI policy to safeguard PII. It is the individual filer's responsibility to follow policy, protect PII, and ensure PII is not inappropriately stored on the individual's personal file share.

There is a risk that PII stored on employee laptops or workstations may be accessed by unauthorized persons. Full disk encryption is enabled on all DOI-issued devices to protect data at rest. BLM employees complete training on using their government-furnished equipment (GFE) for official business only and to avoid storing their personal information on devices. BLM employees must lock their GFE when unattended in a secure environment and follow the DOI's incident reporting procedures in the event of a lost or stolen device. BLM users are also encouraged to employ data minimization practices for PII and the need-to-know for official business only.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties. Transport Layer Security (TLS) technology is employed to protect information in transit using both server authentication and data encryption. Platform- and device-level encryption have been deployed to encrypt data at rest. Other security mechanisms also have been deployed to ensure data security, including, but not limited to, firewalls, virtual private network, and intrusion detection. The BLM GSS has also undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and NIST guidelines. The BLM GSS is rated as a FISMA moderate system, which requires strict privacy and security controls to ensure the confidentiality, integrity, and availability of the data in the system.

There is a risk of unauthorized disclosure or that PII may be misused or used for unauthorized purposes. The BLM GSS limits access to only those persons authorized to use the servers and ensures that they can access only resources for which they have authorization. All BLM authorized personnel sign the DOI Rules of Behavior (ROB) and are subject to monitoring in the system and DOI network. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions, potential termination of employment, and criminal, civil, and administrative penalties. BLM employees must complete Information and Management Technology awareness training, which includes privacy, cyber security, records management, Controlled Unclassified Information (CUI), Section 508, and the Paperwork Reduction Act, and the DOI ROB prior to being granted access to BLM information and information systems, and annually thereafter. Personnel with significant privacy responsibilities, such as human resource staff, IT, financial and law enforcement personnel, must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy.

There is a risk that data on the BLM GSS will be maintained for longer than necessary to support the Department's mission or that records may not be properly destroyed. These risks are mitigated by managing records in accordance with a NARA-approved records schedule and providing extensive training to users on IT security, Privacy, Records Management, and CUI. In addition, there are assigned organization-defined frequencies established for the maintenance of an information system's access and audit records, which are part of the continuous monitoring process of security and privacy controls.

There is a risk of inadequate notice for individuals. Notice is provided to users through the publication of this PIA and the DOI-47 SORN and other applicable SORNs that cover PII that users may have placed on file shares. Users are also provided notice of security monitoring in the warning banner and ROB.

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:

The BLM ACIO operates and maintains the necessary Information Technology (IT) services to support the multiple BLM missions, including the network, servers, applications, databases, computers, and communication facilities. The BLM's use of the data is both relevant and necessary for the purpose of enforcing access control, generating logs, and supporting the auditing process.

☐ 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 --- Not applicable based on the response in Section 4, Question B.

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

☐ Yes: *Explanation*

☒ No --- Not applicable based on the response in Section 4, Question B.

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

Not applicable based on the response in Section 4, Question B.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are 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
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: BLM IT Security team for support, incident response, and compliance purposes.

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

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee requests to access network applications and specify the appropriate user role and level

of access privileges. Network and application access is based on: (1) a valid access authorization, (2) intended system usage, and (3) other attributes based on the system's business function. All network and application access are based on the least-privilege and need-to-know security models. Federal government information is managed and safeguarded by following FISMA, NIST guidelines, and DOI security and privacy policies.

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

The BLM GSS may use contractors to help support the design, development, or maintenance of the system. Contractors are subject to the same authorization and access controls as BLM employees, as described in Section 4.H. above. Privacy Act contract clauses are required and included in all contractor agreements in accordance with, and subject to, the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable DOI regulations.

☐ 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.

The BLM GSS uses AD usernames to help enforce access control, generate logs, support the auditing process, and monitor system use. The BLM GSS does not locate individuals.

☐ No

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

The BLM GSS collects the BLM staff member's AD username, the time of his/her attempted log-on, and the action(s) he/she took.

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

Only BLM staff members with proper authorization and need-to-know (e.g., system administrators, BLM IT Security team) are able to access log data. In addition, users with

Significant Information Security Responsibilities (SISR) are provided, and required to complete, the DOI Role-Based Security Training (RBST) and Role-Based Privacy Training (RBPT) additional training requirements in accordance with 5 CFR § 930.301 (2004), FISMA, OMB Circular A-130, NIST guidance, and DOI Security and Privacy Control Standards.

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. The physical controls are inherited from local sites where the users are located. The system inherits those controls which are in compliance with NIST SP 800-53.

(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. AD user groups, AD elevated accounts for BLM staff members with need-to-know, and group policy objects (GPOs).

(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*

N. 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 BLM Deputy Associate Chief Information Officer (DACIO), as the BLM GSS Information System Owner (ISO), and the BLM Associate Privacy Officer (APO) are responsible for protecting the privacy rights of the public and employee data within the BLM GSS designated boundary and for the systems/applications operating within the BLM GSS boundary that are designated as Privacy Act SORs. The applicable system manager is also responsible for protecting privacy rights of the data under their control. The ISO is the official responsible for oversight and management of the BLM GSS security and privacy controls and the protection of BLM GSS data processed and stored within the BLM GSS. The ISO, Information System Security Officer (ISSO), and the Division Chief of the Enterprise Engineering and Infrastructure Operations Division, in collaboration with the BLM Cybersecurity Management Team, are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data processed, used, or stored within the BLM GSS. Although the BLM GSS is not designated as a Privacy Act System of Records, some of the hosted systems are, and DOI does provide a process for individuals to seek records about themselves that are maintained in any DOI system of records, which is described on the DOI Privacy Program webpage (Privacy Act Requests | U.S. Department of the Interior (doi.gov)). An individual may make a request under the Privacy Act for access to information maintained by the DOI about themselves in any of the Privacy Act systems, which may include systems that are hosted on the BLM GSS. For a list of Government-wide, DOI, and BLM systems of records, visit the DOI Privacy Act Systems of Records Notices webpage (Privacy Act Systems of Records Notices | U.S. Department of the Interior (doi.gov)). Additionally, individuals may contact the BLM APO with any complaints, questions, or concerns via phone or email as identified on the DOI Privacy Officers Contact webpage (Privacy Officers | U.S. Department of the Interior (doi.gov)).

O. 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 GSS ISO 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 BLM GSS ISO, ISSO, and authorized users are responsible for ensuring the proper use of data; for reporting any loss, compromise, unauthorized access, or disclosure of PII to DOI-

CIRC, DOI's incident reporting portal, within one hour of discovery in accordance with Federal policy and established DOI procedures; and for working with the BLM'S APO to ensure appropriate remedial activities are taken to mitigate any impact to individuals.