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: General Web Services (GWS)
Bureau/Office: Bureau of Land Management, National Operations Center (NOC)
Date: May 24, 2023
Point of Contact
Name: Catherine Brean
Title: Bureau Associate Privacy Officer
Email: blm_wo_privacy@blm.gov
Phone: 830-225-3459
Address: BLM, 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

☐ 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 Web Services (GWS) utilizes web application and content management tools such as Drupal and database servers to provide web publishing services for various entities and programs within the BLM. The GWS provides hosting and publishing services for content owned by other systems, offices, programs, and entities defined by Platform Areas. GWS is responsible for the application and platform software such as PHP

(Hypertext Preprocessor) and Drupal, management of the physical, virtual and operating system (OS) layers is done by the BLM General Support System (GSS).

The GWS does not own, test, nor maintain the content hosted users post; it only maintains backups of the hosted providers data. There are multiple websites hosted on the GWS, but only one which collects, uses, or maintains personal identifiable information (PII) and it is the BLM Public Help Desk (PHD).

The PHD is an application that enables public users of BLM systems to submit help tickets that are routed to an internal application support team for resolution. No login is required to submit a help ticket for external users. The requestor is asked to identify the application they are experiencing an issue with from a dropdown field; provide a description of the issue, request or comments; upload any relevant attachments; and provide their full name, phone number, email address, and business or organization name. An internal user can track and respond to tickets after logging into the application with their active directory credentials. An external user receives a ticket number assigned during submittal which can be used to track the issue and status.

BLM has developed multiple applications to support the management of outdoor recreation, livestock grazing, mineral development, and energy production on public lands. If a member of the public experiences any issues with the use of these applications, they can contact the BLM PHD and submit a help ticket for assistance. A list of the current BLM applications that PHD may receive calls on for help, or to provide information are listed below:

- Automated Fluid Mineral Support System (AFMSS)
- Communication Sites
- ePlanning
- eSF299 – Communication Use Application
- General Land Office (GLO)
- LR2000 Public Reports
- Mineral and Land Records System (MLRS)
- National Fluid Lease Sale System (NFLSS)
- Recreation and Permit Tracking Online Reporting (RAPTOR)
- Rangeland Application System (RAS) Public Reports
- National Interagency Fire Center (NIFC)
- Science in Practice Portal (SPP)

A complete list of the hosted GWS websites is identified in Appendix A of this PIA.

C. What is the legal authority?

- 40 U.S.C. 1401, Clinger-Cohen Act of 1996
- E-Government Act of 2002 (Public Law 107-347)
- Memorandum on Transparency and Open Government, January 21, 2009

- Presidential Memorandum on Building a 21st Century Digital Government, May 23, 2012
- OMB Open Government Directive, December 8, 2009
- OMB Memorandum Guidance for Use of Agency Third-Party Websites and Applications, June 25, 2010
- Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

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?

The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

☒ Yes:

General Web Services (GWS) System Security and Privacy Plan. GWS has been registered within the Department of the Interior (DOI) Governance, Risk and Compliance (GRC) tool.

☐ 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.*
See Appendix A			

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)*

☒ No

GWS is not a Privacy Act system of records. It does not collect or use PII to directly retrieve records on individuals. The GWS acts as a service provider, enabling the tools and mechanisms for other entities to publish their content and applications on their platforms. BLM PHD is the only GWS hosted website that collects, uses, or maintains PII and does not retrieve information by a personal identifier, but uses a help support ticket process which documents interaction between the requesting user and the BLM PHD team to resolve reported issues in a timely manner. When the issue is resolved, the ticket is closed. The only information collected is that which may be needed to research and resolve a user's request as it pertains to the applications identified in 1.B. above, which are supported by applicable published DOI bureau/office system of records notices (SORNs) and Privacy Impact Assessments (PIAs). These SORNs and PIAs may be viewed on the DOI SORN website at https://www.doi.gov/privacy.

PIV credentials required to access GWS and the 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:

☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Other:

The only module (sometimes referred to as a platform or subsystem) that collects PII is PHD. This information is collected to research and resolve a requestor's reported issue. PHD public users provide their name, personal or business phone number, personal or business email address, and business or organization name is used for contact purposed to resolve the ticket.

BLM employees and contractors use their government issued Personal Identity Verification (PIV) authenticated through the Enterprise Active Directory (AD). The system collects the user's name, official email address, username, date of last login, and role or access levels for authorized users.

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:

When internal users log on to PHD it is through ADFS (active directory federation services) however the information collected from external users requiring problem resolution is e mail, phone number and name. They are issued a ticket number for issue follow up reasons.

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

PII collected only for PHD

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☒ Telephone Interview
☒ Information Shared Between Systems: When a person logs into the application the Active Directory Federation Services receives either the username and password or the PIV card identification and the PIN which is used for authentication.
☐ Other: *Describe*

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

For the PHD, the intended uses of the PII collected is to contact the caller and inform them on whether the technical issues they were experiencing with a particular BLM application has been resolved or to gather more information regarding the nature of the issue. PII is only collected for the PHD module in support of the web publishing services provided by GWS.

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

☒ Within the Bureau/Office: The PII information is entered into the PHD application which is accessed by the BLM help desk support staff to assist in resolving issues presented from request submitted.

☐ Other Bureaus/Offices:

☐ Other Federal Agencies:

☐ Tribal, State or Local Agencies:

☒ Contractor: Contractor personnel service the help desk for GWS application issues. For PHD, the full name, email address and phone number of the caller will be entered into the PHD software by the contractor. The information will be used to communicate and resolve technical

☐ 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?

If "Yes," describe the method by which individuals can decline to provide information or how individuals consent to specific uses. If "No," state the reason why individuals cannot object or why individuals cannot give or withhold their consent.

☒ Yes:

The BLM PHD website has required items identified by a red asterisk that must be completed if the individual would like the BLM PHD staff to have the ability to contact them regarding the technical issue they are experiencing. Individuals voluntarily provide information when they contact the PHD and a notice of how their information is handled once submitted to the PHD is provided within a posted site disclaimer. If the individual chooses not to complete the asterisked fields, the request cannot be processed. The site disclaimer advises the individual's information will only be used for the PHD records and for contact purposes.

☐ No:

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 this PIA and any related PIAs and SORNs for systems that are supported by GWS and can be viewed at https://www.doi.gov/privacy. A link to the DOI Privacy Policy website is posted on the principal BLM website and the entry point to the PHD .

☒ Other:

A disclaimer has been included on the PHD site where personal information is entered and is shown below. If all the required fields are not completed, the save function will redirect the requestor to the missing fields and the help ticket will not be created until all required fields are populated.

☐ None

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

PHD will use the assigned help desk ticket number to retrieve the information. The help desk ticket number is used to retrieve any information about the issue to resolve or the individual submitting the request. Outside of the PHD application, there is no association between the ticket number and any PII.

I. Will reports be produced on individuals?

☒ Yes:

PHD has a reports section that allows PHD users to manually generate and export information related to tickets, their status, which representative handled the ticket, when tickets were opened and closed, and how many days it took to close the ticket. There is no automated reporting at this time and PHD does not use any external reporting system. No PII information is used in these reports.

☐ No

Section 3. Attributes of System Data

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

.

The PHD individual requesting support will receive either an email or a phone call with a ticket number assigned to their issue. Once the issue has been entered into the PHD, an email is sent or phone conversation is initiated, allowing the individual to verify the accuracy of the information that was provided.

B. How will data be checked for completeness?

Information is obtained directly from individuals who are contacting the PHD during the request process and is presumed to be accurate at the time of submission.

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

The PHD individual requesting support will receive either an email or a phone call with a ticket number assigned to their issue. Once the issue has been entered into the PHD, an email is sent or phone conversation is initiated, allowing the individual to verify the accuracy of the information that was provided.

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

PHD records are covered under the approved Department Records Schedule (DRS)/General Records Schedule (GRS)/BLM Combined Records Schedules which is a combination of schedules developed by the National Archives and Records Administration (NARA), DOI and the BLM.

PHD records are retained in accordance with DRS/GRS/BLM Combined Records Schedule 14 Information Services Records, Item 5e (GRS 6.5-010), IT Customer Service Files. These records are temporary. Cutoff is defined at the end of the fiscal year (EOFY), in which the records would be destroyed one year after resolved, or after being incorporated into program plans and customer feedback mechanisms, whichever is longer, or when no longer needed for business use, whichever is appropriate. The information owner has determined the business use will be 5 years.

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

The DRS/GRS//BLM Combined Records Schedules are a combination of schedules developed and approved by the NARA, DOI and BLM. They constitute the only legal authority the BLM has to dispose of its records. Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA guidelines and Departmental policy. Records schedules authorize, after specified periods of time, the destruction of temporary records that are no longer active or needed and PHD temporary records have established 5 years from the End of Fiscal Year (EOFY) as the cutoff for approved disposition. The procedures for disposition at the end of the retention period are documented in the BLM Manual 1270, Records Management and the DRS/GRS/BLM Combined Records Schedules.

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 when PII is being collected on an existing hosted platform or a new one. This risk is mitigated by the internal standard operating procedures which were developed by the GWS Program Management Team. Each hosted platform must complete a Privacy Threshold Analysis (PTA) prior to receiving approval from GWS to host the application or content. The GWS PTA and PIA are reviewed annually and any new PII elements or applications will be addressed and analyzed for any potential privacy posture changes. If GWS approves any new applications or content changes that contains new PII collection or maintenance, a new PIA will be completed and submitted for approval prior to implementing the new platform or changes to an existing platform.

There is a risk of unauthorized disclosure or that PII may be misused or used for unauthorized purposes. The PHD limits access to only those persons authorized to provide assistance in resolving help tickets and those who support the GWS infrastructure, which acts as a service provider, enabling the tools and mechanisms for other entities to publish their content and applications on their platforms. GWS staff and content/information owners of the hosted systems 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 and potential termination of employment, and criminal, civil, and administrative penalties. This is further reinforced by ensuring BLM employees complete Information and Management Technology awareness training which includes privacy, cybersecurity, records management, Controlled Unclassified Information (CUI), Section 508, and the Paperwork Reduction Act, and the DOI ROB prior to being granted access to DOI information and information systems, and annually thereafter.

There is a risk that data hosted on the GWS will be maintained for longer than necessary to support the Bureau's mission, or that records may not be properly destroyed. This is mitigated by content/information owners identifying the records they are responsible for and managing these records in accordance with NARA-approved retention schedules and providing extensive training to users on IT security, Privacy, Records Management and CUI. In addition, BLM content/information owners are required to follow the BLM Web governance, policies and procedures which ensures internal controls and reviews are completed and appropriate stakeholders are consulted, such as the BLM Associate Privacy Officer, where PII will be collected or BLM Records Officer for disposition guidance.

There is a risk of inadequate notice for individuals. Notice is provided to users at the initial point of collection where a disclaimer notice is provided advising the individual that the use of their data is for contact purposes to resolve their reported issues and for quality control records only. A link to the DOI Privacy Policy is provided in the footer of the landing page where the data is collected. It is also provided through the publication of this PIA and the DOI-47 SORN and other applicable SORNs that cover PII which may reside on the file shares. BLM users are also provided notice of security monitoring in the warning banner and ROBs.

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 use of the information collected is both relevant and necessary for the BLM PHD staff to communicate with individuals and assist in resolving issues they are experiencing within a number of BLM major program areas. If the contact information for the individual is not known, then the technical issue resolution cannot be communicated back to the individual.

☐ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ 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?

N/A. GWS does not derive new data or create previously unavailable data about an individual through data aggregation.

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: *Describe*

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

Access will be restricted for any identified users by roles. Each user will be assigned a role (functions) and permissions. The role will determine what function the user may execute in the system while the permissions will define what records the user can create, read, edit, or delete. The user roles are:

- Site Developer: Administrative access to all site functions and areas.
- PHD Administrator: Accesses all submitted tickets. The PHD Administrator can modify ticket responder fields, generate email replies to tickets, generate and export ticket reports, delete tickets, add/modify/delete ticket queues, modify ticket notification settings, and add/modify/delete users.
- Application Representative (Ticket Access): Assigned specific application(s) within PHD that are authorized for access. These Application Representatives can access submitted tickets only for their assigned application queues, modify ticket responder fields, generate email replies to tickets, and generate and export ticket reports.
- Application Representative (Notifications): Assigned specific application(s) within PHD authorized to receive notifications for incoming tickets. The Application Representatives receive email notifications when a ticket has been added to their assigned application queues.

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.

This is a contractor application and only security cleared personnel may use the system. Contractor employees are required to sign the DOI's ROB and complete security

and privacy training prior to accessing a DOI computer system or network. Information security and role-based security training must be completed on an annual basis as an employment requirement. Contractors are also subject to Federal Acquisitions Regulations (FAR) with regard to PII. BLM contractor staff are required to undergo background checks as defined by DOI policy and procedures. Contractor staff access will be restricted to data on a need-to-know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in published procedures.

The appropriate privacy FAR clauses were included in the contract. The terms and conditions will be added to the contract during its modification.

☐ 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.

☒ No

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

☒ Yes. *Explanation*

The only users who can log into the PHD are security cleared BLM contract employees. Hosted websites on GWS are not intended for monitoring users; however, the PHD system does identify and monitor user activities within the system through audit logs. Audit logs automatically collect and store information about a user's visit, including time/date, verification attempt ID, username, identity verification method, action attempted, status of the attempt, IP address, and location, as well as create/update/delete activities performed by users to support user access controls, troubleshooting, and incident response support. Audit logs may also be used to identify unauthorized access or monitoring.

☐ No

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

Login history collects information for detecting and resolving authentication or login issues. This includes information for assisting users in accessing their accounts or for researching unauthorized access attempts. Information collected may include data such as time, verification attempt ID, username, identity verification method, action attempted, status of the attempt, IP address, and location. For members of the public using the site, the DOI Privacy Policy

describes what information is collected as part of a systems log file that is used internally for technical improvements and site management.

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

Only cleared contract personnel with the appropriate assigned role can access and monitor the logs. Separation of duties, permission restrictions, and audit controls are implemented to prevent unauthorized monitoring. Access can only be attained with either the PIV card or the proper username and password associated with AD.

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. Servers are physically located in the NOC.

(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 GWS Information System Owner (ISO) identified within this document is responsible for protecting the privacy rights of the public and employees affected by the application. The Associate Director, NOC serves as the GWS ISO and the official responsible for oversight and management of the GWS security controls and the protection of customer agency information processed and stored by the GWS system. The ISO 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 GWS and its hosted websites. The ISO, Privacy Act System Managers and data owners for the supported Privacy Act systems are 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.

Data in the systems that are supported by GWS is under the control of each system owner, and the 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.

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 GWS 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 ISO, 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.

Appendix A

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
Air Resource Toolkit (ART)	Only an Internal site currently but will be external displaying public information in the near future. It is under redesign.	No	N/A
BLM.Gov	Main public website for the public and the root page of www.blm.gov. The BLM.Gov website is currently in the operational phase at the Bureau of Land Management (BLM) National Data Center in Denver, Colorado. (https://www.BLM.Gov).	No	N/A
Fire Jobs (NIFC)	Displays information to the public on Fire Jobs. Fire jobs by state and agency is displayed on USA Jobs which is linked to NIFC through hot spots on a map of the USA. The job description, state and DOI agencies for the job are displayed on the USA Job site not NIFC.	No	N/A
Knowledge Resource Center (KRC)	The purpose of this application is to provide essential training resources to the public and BLM. The training content varies from Fire, Forestry, Botany, to internal employee training resources. Many training resources are shared between the public and internal BLM staff. KRC collects no PII.	No	N/A
National Interagency Fire Center (NIFC)	The purpose of the www.nifc.gov website is to provide a web-based information portal of national wildfire information topics to users from the public and the U.S. Government.	No	N/A
National Wildfire Coordinating Group (NWCG)	The National Wildfire Coordinating Group provides the public information on national leadership to enable interoperable wildland fire operations among federal, state, local, tribal, and territorial partners. Primary objectives include the following.	No	N/A
Public Help Desk (PHD)	The purpose of the Public Help Desk application is to provide a ticketing application for the Public to	**Yes: This PIA is for GWS**	Full Name, email,

	interface with BLM staff. Internally, the PHD application provides a simplified interface and Work Order/Request tracking mechanism to provide essential support services to the public.	**however the only website requiring a PIA is PHD within GWS. No other website collects public information.**	phone number, business name and application for which requestor needs technical support.
Science in Practice Portal (SPP)	SPP's purpose is to provide Scientific information and content to be shared amongst the BLM community and Partner Agencies. SPP's mission is to capture this various knowledge from BLM Subject Mater Experts (SME) in their field and provide a portal to capture and share that knowledge with their colleagues across the Agency and partner Agencies. This site is internal to DOI, there is no external public access to the information. https://spp.blm.gov/home	No	N/A