U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires a Privacy Impact Assessment (PIA) 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: Recreation and Permit Tracking Online Reporting (RAPTOR)
Bureau/Office: Bureau of Land Management, National Conservation Lands
Date: November 30, 2022
Point of Contact:
Name: Catherine Brean
Title: BLM Associate Privacy Officer
Email: blm_wo_privacy@blm.gov
Phone: (830) 225-3459
Address: IRM, DOI National Operations Center, Bldg. 50, Denver, Colorado 80224

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?

Recreation and Permit Tracking Online Reporting (RAPTOR) is a permit and tracking system for members of the public to apply for Special Recreation Permits (SRPs), Paleontological Resource Use Permits, and Scientific Research Authorizations on public lands managed by the Bureau of Land Management (BLM). RAPTOR provides an online interface with the public to apply for more easily, and view, the status of an application for a permit as required by Department of the Interior Secretarial

Orders 3356 and 3366. The use of permits allows the BLM to coordinate and track recreational and research uses of public lands and provides resource protection measures to ensure the future enjoyment of those resources by the public. The RAPTOR system also ties together administrative, information and knowledge, and data management activities. RAPTOR interacts with BLM's Enterprise Geographic Information System for supporting spatial locality information and creating maps of project areas. Geospatial information is directly integrated to permit applications and issuance. Paleontological or other scientific research specimens or data collected, and accomplishments after issuance of the permit or authorization is later reported by the externals users and annual requirements are collected to validate Special Recreation Permits via RAPTOR.

SRPs are authorizations for commercial use, competitive events, group activities, recreation events, and providing vending services or supplies associated with recreation events. These permits include conditions of use (stipulations) that ensure that the permitted recreation use meets BLM's goals of providing opportunities for recreation experiences and ensure that the use is consistent with other resource management objectives. SRPs also ensure that the public receives a fair-value return for certain recreational uses of the public lands, by charging fees for permitted activities, and provides for economic development in surrounding communities through sustainable recreation uses.

In addition, the BLM is committed to offering outstanding recreation opportunities to the public while ensuring good stewardship of public lands and resources. SRPs are issued to ensure public health and safety, protect natural and recreational resources, reduce user conflicts, achieve recreation and other resource management objectives, and enhance the public's opportunity for quality recreation experiences.

Scientific projects, paleontology, and other disciplines, inform the decision-making process of BLM managers and help address conservation needs on public lands using the best available science. Close working relationships between scientists and BLM managers and staff lead to mutually beneficial outcomes. RAPTOR is a permit and tracking system for members of the public to apply for Paleontological Resource Use Permits or Scientific Research Authorizations on public lands managed by the BLM. The RAPTOR system addresses a need to document scientific research work occurring systematically and consistently on National Conservation Lands units, and other BLM lands, over time. Documentation allows managers to have early access to scientific findings so that management decisions can incorporate the best available science.

C. What is the legal authority?

Federal Land Policy and Management Act, Pub.L. 94-579
Paleontological Resources Preservation Act, Pub.L. 111-11
Federal Lands Recreation Enhancement Act, Pub.L. 108-447

D. Why is this PIA being completed or modified?

☐ New Information System
☒ New Electronic Collection

☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes

UII Code: 010-000003803 SSP Title: System Security and Privacy Plan for Recreation and Permit Tracking Online Reporting (RAPTOR)

☐ 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	**n/a**	n/a	**n/a**

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

☒ Yes

This is a new electronic collection of information which streamlines and improves the BLM permitting process which will allow the public to electronically apply for, and view, the status of an application for a permit. A new Special Recreation Permit SORN is currently under review and once finalized, an Interior/BLM number will be assigned and a notice of a new system of records will be published in the Federal Register.

INTERIOR/DOI-20, Paleontological Resources Preservation System, 84 FR 52530, October 2, 2019. BLM, Bureau of Reclamation (BOR), National Park Service (NPS) and US Fish and Wildlife Service (FWS) have developed a standardized application for paleontological resources use permits. This system of records assists the bureaus in managing, tracking, and reporting activities under permits.

INTERIOR/DOI-86, Accounts Receivable: FBMS, 73 FR 43772, July 28, 2008; Modification published 86 FR 0156, September 7, 2021. BLM's Collections and Billings System (CBS) sends collection and billing files to DOI's Financial and Business Management System (FBMS)to ensure that all collections,

bills, adjustments, and reversals posted in CBS are also posted in the FBMS ledger of record and the two systems are kept in sync.

DOI SORNs may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☐ No

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

☒ Yes

The information collected specific to the Special Recreation Permits Application under 43 CFR 2930 has been approved by OMB under 44 U.S.C. 3501 and assigned clearance number 1004-0119, which expires April 30, 2023.

- Form 2930-1, Special Recreation Permit Application

The information collected specific to Application and Reports for Paleontological Permits, 43 CFR 49 has been approved under OMB under 44 U.S.C. 3501 and assigned clearance number 1093-0008, which expires September 30, 2025.

- DI- 9002 (07/2019) Paleontology Permit Application
- DI- 9003 (07/2019) Paleontology Permit
- DI- 9004 (07/2019) Paleontology Locality Record
- DI- 9005 (07/2019) Notice to Proceed (Paleontology)
- DI- 9006 (07/2019) Paleontology Permit Report
- DI- 9007 (07/2019) Repository Receipt of Collections (Paleontology)

☐ 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
☒ Group Affiliation
☒ Home Telephone Number
☒ Employment Information
☒ Education Information
☒ Mailing/Home Address

☒ Financial
☒ Driver's License
☒ Other

Financial information including, but not limited to, fees, bills, payments, and receipts. Payments may be collected for special recreation permit applications, cost recovery, post use, and annual fees. Any payments are processed through the Department of the Treasury, Bureau of Fiscal Service, utilizing the Pay.gov website. Individuals logging on through RAPTOR are redirected to the Pay.gov website to make payment. Payment data provided by users through Pay.gov is presumed to be current and accurate, and data verification processes are managed by the Department of the Treasury. Information received from Pay.gov consists of accounting and financial data which is forwarded to DOI FBMS for payment processing. Only a confirmation of receipt of payment is returned from Pay.gov to the system, which includes information such as merchant confirmation number. Pay.gov then sends information to the BLM's CBS, which generates a receipt once the funds are deposited. CBS then sends the information to FBMS. BLM staff access CBS to download the receipt and then upload the receipt into RAPTOR for the applicant/permittee to view. BLM staff may also create bills within CBS to send to applicant/ permittee through a US mail service and upload the bills into RAPTOR for applicant/permittee viewing. CBS receipts and bills include the applicant's name, mailing address, amount paid, the fund the amount went to, and any text the BLM inserted to describe the fee, including fee calculation.

On rare occasions, applicants may be requested to provide a driver's license if the BLM has questions about historical activity. These licenses will be used by law enforcement to run background checks on individuals to help the BLM determine if there were previous violations and if a permit should be issued.

Many special recreation permit applications will include proprietary business or operating plans. Insurance information will be collected prior to a Final Decision. We ask for a certificate of insurance for our records and the BLM needs to be listed as additional insured. Additional information includes website, Fax Number, maps/GIS data, proposal details (location, dates, purpose), previous permit history, unresolved/criminal/civil/administrative actions relating to permit or activities plan to conduct with application, bond or security history/forfeiture, conviction/fine history for violations regarding natural resources, cultural resources, or any activity related to proposal, price list/fees/rates, waivers/liability release/acknowledgement of risk forms/client-outfitter contracts, documentation of business contracts/agreements, bonding, documentation of arrangement to cross or access private or other agency land, proposed trip itineraries, fees, employee lists, vehicle lists (including equipment and livestock), list of third parties, and other required federal, state or local licenses/registrations/permits After permit issuance, financial history (bills, fees and payments/receipts), trip logs (including, but not limited to, number of clients/participants, number of staff/volunteers, dates of trips/events, gross receipts collected, amount of time/miles on BLM, number of vehicles/equipment/boats, location, and number of items sold), post use reports, evaluations, monitoring documentation, decision letters, and annual validation requirements (requirements listed above needed for permit issuance) may be required.

Information regarding in-kind contributions from other sources for paleontological permits and scientific authorizations, Online Contributor Identification (researcher proxy identification), other permit numbers.

Information on the general composition of research teams, such as number of participants by age range, and number of total volunteer and staff hours contributed.

Open Researcher and Contributor ID (ORCID) is optional information that could be collected for each researcher (https://orcid.org). This ID allows for tracking of research and publications more easily.

Aircraft operators certificate ID and aircraft identification numbers for drone operators.

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:

Applicants may provide information about their employees, volunteers, subcontractors for purposes of applying for a permit or validating their permit as a third-party source

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: Via text message or instant message

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

Special recreation permit application information is used to:

- Determine whether proposed recreation use is environmentally acceptable and acceptable under the current Land Use Plan.
- Calculate the amount of fees that will be assessed for processing fees (application fees), cost recovery, post use fees, and annual fees and if the activity or event is authorized.
- Determine qualifications and capability of the applicant to offer the proposed services.
- Tabulate number of permits or Letters of Authorization issued for the Triennial Report to Congress required by the Federal Lands Recreation Enhancement Act.
- BLM needs this information to approve or reject the application.
- Administer the permit after issuance, including monitoring the permit, calculating fees and tracking financials, evaluations, and annual validation of the permit.

Paleontology permit application information is used to:

- Determine whether proposed activity is scientifically sound.
- Identify the designated museum repository that will receive the material collected.
- Determine qualifications and capability of the applicant to conduct the proposed paleontology research.
- Tabulate paleontology actions on BLM-managed land, and track BLM museum property and permit compliance.

Scientific research authorization application information is used to:

- Determine whether proposed activity is scientifically sound and complies with laws and regulations.
- Determine qualifications and capability of the applicant to conduct the proposed scientific research.

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

☒ Within the Bureau/Office:

BLM authorized users and approval authorities will use this information to approve or reject applications and administer permits. Information may be shared at the District, State or National Operations Center/Headquarters level within BLM to help staff process applications or administer permits. PII may also be shared with internal BLM law enforcement and solicitors.

☒ Other Bureaus/Offices:

The BLM CBS sends collection and billing files to DOI's FBMS to ensure that all collections, and all bills, adjustments and reversals posted in CBS are also posted in the FBMS ledger of record, and the two systems are kept in sync. FBMS is an enterprise-wide application centrally managed by the DOI Business Integration Office. Each DOI Bureau/Office has assigned Account Controllers and other administrators that grant access to employees who have a need to know in order to perform their official

duties. BLM only has access to its own information. BLM users access FBMS via the FBMS Portal. FBMS Transnational access is restricted only to users who have been granted authorized access. Also, information could be shared with National Park Service (NPS), US Fish and Wildlife Service (USFWS) and Bureau of Reclamation (BOR) if activities cross jurisdictions, or if an applicant is applying or has historical activity with other Bureaus. BLM may also share with DOI Interior Board of Land Appeals (IBLA) who is an appellate review body that exercises the delegated authority of the Secretary of the Interior to issue final decisions for the Department of the Interior.

☒ Other Federal Agencies:

In the event of a forest fire, drone crash or other emergency, the appropriate federal agency such as Federal Emergency Management Agency, would be notified. Also, information could be shared with US Forest Service, Army Corps of Engineers, and National Oceanic Atmospheric Administration (NOAA) if activities cross jurisdictions, or if an applicant is applying with other agencies or has historical activity with other agencies. BLM also interacts with the Department of Treasury's, Bureau of Fiscal Service Pay.gov system to allow applicants/permittees to pay fees online. Using a RAPTOR assigned code, Pay.gov sends the amount to BLM's CBS, which creates a receipt once funds have been deposited.

☒ Tribal, State or Local Agencies:

Information related to a permit may be released to law enforcement for any valid law enforcement action. Also, information could be shared if the activity crosses jurisdiction, or if an applicant is applying with other agencies or has historical activity with other agencies.

☒ Contractor:

BLM authorized contractors working on the system may be able to access this information in the performance of their duties. In addition, BLM may share information with contracted certified public accountants for the purpose of conducting periodic audits of their SRP programs. Periodic audits will help BLM ensure it has collected fees in accordance with the terms and conditions of the SRP, to evaluate the SRP holder's accounting system, and to determine the adequacy of BLM recordkeeping processes, procedures and actions pertaining to SRP administration.

☒ Other Third-Party Sources:

Names and group affiliation may be provided to the repository. BLM may share information about paleontology resources and localities with data aggregating websites such as https://www.idigbio.org/. Such websites facilitate access to scientific data from numerous institutions. Potential PII, such as name and professional affiliation, may be associated with records of localities or specimens collected.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes:

Submission of the requested information on the special recreation permit application, scientific research authorization application, and paleontological permit application is necessary to obtain or retain the benefit of a permit or authorization. Individuals can decline to provide the information, however, failure to submit all of the requested information or to complete one of these forms may result in the rejection or denial of the application.

☐ No:

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

☒ Privacy Act Statement:

The applicable BLM forms identified in 1.H above contains a Privacy Act statement. After an individual successfully submits a request to register for a RAPTOR account, they will be directed to a new page which explains what is needed to proceed to the electronic application process and provides a Privacy Act statement.

☒ Privacy Notice:

Notice is provided through the publication of this privacy impact assessment, the SORNs identified in Section 1.G above, and the new system of records notice, Special Recreation Permits, that is currently being developed and coordinated for approval. Once the SORN is ready for final approval, an INTERIOR/BLM SORN number will be assigned prior to being published in the Federal Register. DOI PIAs and SORNs may be viewed at https://www.doi.gov/privacy/pia and https://www.doi.gov/privacy/sorn.

☒ Other:

The BLM RAPTOR site where the public can submit applications to BLM for Special Recreation Permits, Paleontological Resource Use Permits and Scientific Research Permits and Authorization and the BLM Electronic Forms site, where applicable forms are available for download, contain a hyperlink to the DOI Privacy Policy page.

☐ None

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

An external user (public) can only access their data. First filter is by USER ID. If the external user has multiple applications, the selection can be by application name or application number. The number is associated to a key - APPLICATION ID. This ID is how the information is retrieved.

For a BLM field user, the first filter is by office. Each field user is assigned to an office (multiple offices are allowed). They can only update records that are a part of their office. A list of applications belonging to the office are displayed. The field user will select the desired application by application name or application number. The number is associated to a key - APPLICATION ID. This ID is how the information is retrieved.

BLM reports are based on specific criteria. For example, an office wants all applications for their office that are not complete. All records are retrieved based on the search criteria. The primary field return in the search is APPLICATION ID. Based on the ID all secondary fields are collected. All reports are view only - no updating or deleting is allowed.

I. Will reports be produced on individuals?

☒ Yes:

Prior to close out of the permit, BLM will produce a report of permit status to ensure the requirements of the permit have been fulfilled and follow up on any outstanding issues. A query would also be used to determine eligibility for a new permit. A report may also be produced showing what applications or permits are associated with an individual or organization.

☐ No

Section 3. Attributes of System Data

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

Information is obtained directly from applicants during the application process and is presumed to be accurate at the time of submission. The application form requires the applicant to certify the information in the application and supporting documents are true, complete, and correct to the best of their knowledge and belief and is given in good faith.

B. How will data be checked for completeness?

RAPTOR includes automated edit checks for completeness and valid domain values. Automated business processes include checks for information completeness at every step of every transaction, as, for example, when filling out a multi-page electronic application on the website and roll back of incomplete transactions.

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

The RAPTOR data model is set up so the data is updated in a table and is then linked to the corresponding data elements. The data model ensures the same data does not need to be entered in

multiple fields. Data is collected real time via point of access to the application, i.e., desktop, tablet, phone, etc. via a web browser. Data accuracy and integrity are ensured via standard physical and logical data model development practices outlined in the BLM data standards. Data model development techniques ensure the data that is collected is useful to the business and is named in such a way that it is clear what the data element represents.

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

RAPTOR 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), the Department of the Interior (DOI) and the Bureau of Land Management (BLM).

Scientific research and paleontological records in RAPTOR are retained and disposed in accordance with DRS/GRS/BLM Combined Records Schedule 4, item 11a; Resources Inventory, Study, Survey and Mapping Files. These records are scheduled as PERMANENT.

Special recreation permit records in RAPTOR are retained and disposed in accordance with DRS/GRS/BLM Combined Records Schedule 4 item 14b; Grazing and Other Land-Use Lease and Permit Files. These records are TEMPORARY. Cutoff is defined at the end of the fiscal year (EOFY), in which permit terminates and appeal rights are exhausted.

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

The scientific research and paleontological records in RAPTOR are retained and disposed in accordance with DRS/GRS/BLM Combined Records Schedule 4, item 11a; Resources Inventory, Study, Survey and Mapping Files. These records are scheduled as PERMANENT. Permanent records are never destroyed and are always identified for transfer to NARA at a specific time after cutoff. Permanent records are transferred to the Federal Records Center (FRC) and then later transferred by the FRC to National Archives during NARA's annual move process. Permanent records may be transferred directly to the National Archives if they have met their disposition.

Special recreation permit records in RAPTOR are retained and disposed in accordance with DRS/GRS/BLM Combined Records Schedule 4 item 14b; Grazing and Other Land-Use Lease and Permit Files. These records are TEMPORARY. Cutoff is defined at the end of the fiscal year (EOFY), in which the permit terminates, and appeal rights are exhausted. Records are then transferred to a FRC 3 years after the cutoff. The Federal Records Center destroys 30 years after cutoff as authorized under Disposition Authority (N1-49-90-1, 4/14b).

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.

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 moderate privacy risk due to the type and volume of personal information maintained in the RAPTOR. Users submit applications for special recreation and paleontological permits as well as applications for scientific research authorizations in RAPTOR, which a program designated user reviews. Information collected and used is limited to the minimum required to perform the purpose and functions of RAPTOR. To mitigate privacy risk, BLM has restricted access to personally identifiable information within RAPTOR to a limited number of BLM employees and contractors.

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. RAPTOR is classified as moderate for FISMA and has all of the required security and privacy documentation, and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, RAPTOR 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 and sign DOI Rules of Behavior.

Business rules and guidelines, as well as rules of behavior, have been established to prevent inadvertent disclosure to individuals not authorized to use RAPTOR or those who do not have a direct "need to know" certain information contained in RAPTOR. All end-users from the public have an individual password and ID that is created by the user in RAPTOR. All new internal users will receive a user guide detailing the appropriate use of the RAPTOR. 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 RAPTOR logins. Additionally, any account that is inactive for more than one year is automatically suspended. All BLM personnel accessing the RAPTOR 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 activity and user activity including invalid logon attempts and access to data via User ID, IP Address, etc. Audit trails are also captured within RAPTOR to determine who has added, deleted, or changed the data within RAPTOR. Any qualification overrides require that the account manager document the reasoning and the login name with date and time is added by RAPTOR.

There is a risk that an application may be denied based on the submission of inaccurate information. All information is obtained directly from the applicant so is presumed to be complete and accurate. Any

inaccurate information provided by the applicant may be corrected during user validation procedures or by the applicant themselves. 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 publication of this PIA, BLM applicable notices, and the Privacy Act statements provided on the applications submitted on the official BLM RAPTOR website.

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: RAPTOR provides Bureau employees and customers with a system to apply for and maintain paleontology, special recreation, and scientific research authorizations. Use of the information collected in the RAPTOR system is both relevant and necessary for the purpose of approving or rejecting the submitted application and administrating the permit.

☐ 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:

☒ No

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

Not applicable

F. Are the data or the processes being consolidated?

☒Yes, data is being consolidated. RAPTOR operates under a formal system security plan and is subject to security certification and accreditation requirements. The current design segregates functions that may involve Privacy Act information so that role-based security restrictions can be implemented more confidently.

☐ 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:

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

Roles and associated access privileges are established as part of the System Security Plan. Access is controlled by assignment of roles and specific discrete authorizations and is limited to minimum necessary access. Individual access to RAPTOR and authorizations within RAPTOR require signed documentation from the program prior to creation or modification. Therefore, individuals have limited access to the data. It is the responsibility of information system owners to ensure no unauthorized access is granted.

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

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

BLM authorized contractors are involved with the development and maintenance of the RAPTOR System. The contractors working on the RAPTOR system can access information in the performance of their official duties. Required Privacy Act clauses are included in the Information Technology Support Services contract, which is the contract supporting RAPTOR.

☐ 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 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 RAPTOR 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 audit logs contain the user ID, date/time of access, invalid logon attempts, user activity, and as identified 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?

RAPTOR has the ability to audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. In accordance with applicable DOI guidance, unauthorized activity will be included in the audit logs and alerts are being continuously updated to improve security. Logs are ingested by the BLM's SPLUNK tool. The audit trail includes system user username, logon date and time, number of failed login attempts, and user actions or changes. The principle of least privilege is applied to ensure the system operates at privilege levels no higher than necessary to accomplish organizational missions or business functions. Authorized personnel may include security administrators, system administrators, system security officers, system programmers, and other privileged users. In addition, all internal users must complete annual Information Management Training, which includes, privacy, security, records management, and CUI, as well as role-based privacy and security training, prior to being granted access to the DOI network or any DOI system, and annually thereafter. All internal users are required to acknowledge and sign DOI ROBs which provides the guidance needed for users to fully understand the rules and their responsibilities. Also, embedded within the ROBs is the warning banner which is displayed upon logging into any Department of the Interior computer system. The warning banner clearly states all agency computer systems may be

monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. It further states, by logging into an agency computer system, the user acknowledges and consents to monitoring of this system.

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.

(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.

(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 RAPTOR System Manager is responsible for protecting the privacy rights of the public and employees affected by the interface.

The Assistant Director for National Conservation Lands and Community Partnerships Directorate (WO-400) is the RAPTOR Information System Owner and the official responsible for oversight and management of RAPTOR security controls and the protection of agency information processed and stored in the RAPTOR application. The Information System Owner and RAPTOR Privacy Act System Manager, in collaboration with the DOI 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 RAPTOR application. These officials, DOI bureau and office emergency response officials, and authorized RAPTOR personnel are responsible for protecting individual privacy for the information collected, maintained, and used in RAPTOR, 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 RAPTOR System Owner is responsible for oversight and management of RAPTOR security and privacy controls, and for ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of agency PII is reported to DOI-CIRC within one hour of discovery in accordance with Federal policy and established DOI procedures.