Introduction:

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

System Information

System or Project Name:	ePlanning
System or Project Acronym:	EPL
Date submitted for review:	December 12, 2025
System Operational Status:	Operational

Point of Contact

Name:	Dianna Tayllor
Title:	Privacy Officer
Office:	Office of the Chief Information Officer, Departmental Privacy Office
Phone:	(703)787-1763
E-mail:	dianna_taylor@ios.doi.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

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

This PIA is being conducted due to a significant modification of the ePlanning (EPL) system. The system has been migrated to a Microsoft Cloud Service Provider (CSP) environment as part of a technical modernization effort. This change affects the system's hosting and security architecture but does not introduce new categories of PII, new data sources, expanded data sharing, changes to authentication, or new retrieval methods. The purpose, collection, use, sharing, and retention of PII remain unchanged.

This PIA evaluates cloud migration and associated data security considerations to ensure continued compliance with applicable privacy and cloud security requirements.

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

ePlanning is an operational web-based application that supports the Bureau of Land Management's (BLM) implementation of the National Environmental Policy Act (NEPA) by enabling the tracking, review, and public

commenting of environmental planning documents through integrated text and mapping tools.

The system is used by BLM personnel, interdisciplinary project teams, and members of the public to track, manage, review, and comment on NEPA documents. It facilitates public participation by allowing individuals to voluntarily submit comments and limited contact information to receive updates or responses related to specific projects and supports the development and maintenance of official project records in accordance with the BLM Planning Manual ensuring transparency, collaboration, and informed decision-making in the NEPA process.

3. Is the system registered in BisonGRC?

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

The ePlanning (EPL) system is registered in BisonGRC, DOI's official system inventory and Authorization to Operate (ATO) tracking system, under UII BLM-0006-SYS-1033. The system record includes current security categorization, privacy compliance documentation, and supporting materials for the Authorization and Assessment (A&A) process. The BisonGRC record is reviewed and updated during annual FISMA reporting and whenever significant changes are made to the system.

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

The collection and use of data within ePlanning is authorized under the following authorities:

- **Privacy Act of 1974, 5 U.S.C. § 552a** – Governs the collection, maintenance, use, and disclosure of records containing personally identifiable information (PII) about individuals retrieved by personal identifiers.
- **E-Government Act of 2002, Section 208, 44 U.S.C. § 3501** – Requires federal agencies to conduct Privacy Impact Assessments for systems that collect, maintain, or disseminate PII.
- **OMB Circular A-130, Managing Information as a Strategic Resource** – Establishes federal requirements for managing information resources, including privacy and security controls for federal information systems.
- **National Environmental Policy Act (NEPA), 42 U.S.C. § 4321 et seq.** – Requires federal agencies to evaluate environmental impacts and consider public input in decision-making processes. ePlanning facilitates public participation under NEPA.
- **Federal Land Policy and Management Act (FLPMA), 43 U.S.C. § 1701 et seq.** – Provides BLM authority to manage public lands and conduct planning activities that require public engagement.
- **Taylor Grazing Act, 43 U.S.C. §§ 315–316** – Authorizes BLM land management activities that may involve public notice and comment.
- **Government Performance and Results Act (GPRA) Modernization Act of 2010, Pub. L. 111-352** – Establishes federal performance management and reporting requirements. ePlanning supports tracking and reporting of land management activities.
- **Federal Acquisition Streamlining Act (FASA) of 1994, Pub. L. 103-355** – Governs federal acquisition and contracting processes relevant to the procurement and management of system services supporting ePlanning operations.

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

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

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

The ePlanning system does not currently require a separate Privacy Act System of Records Notice because records are not retrieved by name, email address, telephone number, mailing address, protestor name, submitter ID, user ID, or any other personal identifier. Records are organized and retrieved by project name, project ID, NEPA document, planning action, or associated project record.

Although members of the public may voluntarily provide contact information in comments, and individuals submitting Land Use Planning protests may be required to provide limited contact information to establish standing, ePlanning does not use those personal identifiers as the method of retrieval for Privacy Act purposes. If BLM enables or uses any functionality to retrieve, search, sort, report, or manage comment or protest records by personal identifier, the Privacy Office will reassess SORN applicability before that functionality is used.

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

☐ Yes
☒ No

The ePlanning system supports public comment and Land Use Planning protest submissions. Public comments are generally submitted in free-text format and do not require individuals to provide personal information to participate in the NEPA comment process.

Land Use Planning protest submissions may require limited contact information to establish standing under applicable planning requirements. BLM will coordinate with the appropriate Information Collection Clearance Officer to confirm whether the protest submission process is covered by an existing OMB-approved information collection, requires an OMB Control Number, or is otherwise exempt from PRA clearance requirements. If an OMB Control Number applies, it will be documented in this PIA and displayed with the applicable collection notice.

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

None.

Section 2: Data Description and Use

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

☒ Name (full, first or last)	☒ Home telephone number	☐ Employment or resume info
☐ Aliases/nickname	☒ Personal Email	☐ Full or Truncated SSN
☐ Driver's license	☒ Mailing or home address	☐ Physical characteristics
☐ Citizenship	☐ Religious preference	☐ Biometrics or facial recognition
☐ Legal Status	☐ Mother's maiden name	☐ Vehicle information

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

☐ Sex
☐ Race or ethnicity
☐ Date of birth
☐ Place of birth
☐ Personal cell phone number
☐ Tribal or other ID number
☐ Military records
☐ Marital status
☐ Spouse Information
☐ Child or family information
☐ Emergency contact info
☐ Financial information
☐ Education information
☒ Other: Describe below
☐ Passport information
☐ Travel information
☐ Parent's name
☐ Credit card number
☐ Nationality
☐ Disability Information

The ePlanning system collects, uses, stores, or logs the following categories of PII:

- Full name, email address, telephone number, and mailing address voluntarily provided by members of the public when submitting comments or required, where applicable, for Land Use Planning protest submissions.
- Free-text public comments and protest narratives, which may contain unstructured PII or sensitive PII if voluntarily submitted by the individual.
- BLM employee and contractor names, user IDs, account identifiers, work contact information, role assignments, and project assignments used for system access, project management, and accountability.
- Authentication and audit-related data, including successful and failed login events, user activity logs, IP address or network identifiers where captured, and other system metadata linked to authorized users.

The system does not intentionally solicit Social Security numbers, financial account information, biometric information, health information, or other highly sensitive personal information. Users are advised not to include sensitive PII in public comments or protest narratives unless specifically required by the applicable process.

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

☒ Individual
☐ Federal Agency
☐ Tribal Agency
☐ Local Agency
☒ DOI Records
☐ Third Party Records
☐ State Agency
☒ Other: *Describe Below*

PII is collected directly from individuals through the ePlanning (EPL) system's web-based comment submission interface, as well as through paper and fax submissions that may be manually entered into the system by authorized personnel. Members of the public may voluntarily provide limited contact information, such as name, telephone number, email address, and mailing address.

PII is also obtained from DOI records. BLM employee names are retrieved from the Department's Active Directory (AD) to identify personnel involved in project management.

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

☒ Paper Format
☐ Email
☐ Face-to-Fact Contact
☒ Website
☒ Fax
☐ Telephone Interview
☒ Shared Between Systems: *Describe*
☐ Other: *Describe*

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

PII within the ePlanning (EPL) system is collected through the following methods:

- **Website** – Members of the public submit comments through a secure web-based interface. Individuals may voluntarily provide limited contact information. Data is transmitted using HTTPS encryption, and users are provided with a privacy notice at the time of submission.
- **Paper Format** – Public comments may be submitted in paper form and are manually entered into the system by authorized personnel in accordance with DOI information handling procedures.
- **Fax** – Public comments may be submitted via fax and are manually entered into the system by authorized personnel in accordance with DOI information handling procedures.
- **Information Shared Between Systems (Active Directory)** – BLM employee names are retrieved from the Department's Active Directory (AD) system through internal system integration. Access is restricted to authorized users and managed in accordance with DOI access control policies.

All collection methods use DOI-approved security protocols, and users are provided with Privacy Notice at the point of data submission when applicable.

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

The ePlanning (EPL) system collects PII to support public participation in the National Environmental Policy Act (NEPA) and Land Use Planning process, project management, and communication related to BLM planning activities.

- **Public Comment Attribution** – Names and any voluntarily provided identifying information are used to associate submitted comments with an individual, when provided, and to maintain the administrative record for NEPA projects.
- **Communication and Follow-Up** – Email addresses, telephone numbers, and mailing addresses, when voluntarily provided, are used to respond to comments, provide project updates, or request clarification related to submissions.
- **Project Management and Accountability** – BLM employee names, retrieved from Active Directory, are used to identify personnel responsible for managing projects, reviewing submissions, and maintaining official records within the system.
- **Recordkeeping and Compliance** – PII contained within comment submissions is maintained as part of the official project record to support transparency, documentation, and compliance with NEPA and federal records management requirements.
- **Collection of Protests –** The ePlanning system is used to collect and identify protests on Land Use Planning actions in accordance with BLM's Planning regulations.

All uses of PII are limited to supporting NEPA and Land Use Planning processes and related administrative functions. PII is not used for profiling, marketing, or any unrelated purposes.

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

The ePlanning (EPL) system limits the collection and use of PII to what is necessary to support public participation in the NEPA and Land Use Planning process and related project management activities.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

- **Limited and Voluntary Collection** – PII is limited to basic contact information and is provided voluntarily when individuals submit comments. Personal information is not required to participate.
- **Purpose-Based Use** – PII is used only for comment attribution, communication, and project recordkeeping, consistent with the system's purpose.
- **No Collection of Sensitive PII** – The system does not intentionally collect sensitive PII such as Social Security numbers, financial information, or biometric data.
- **System Design and Controls** – Data fields are limited to only what is necessary, and changes to data collection require review and approval.
- **Access Controls** – Access to PII is restricted to authorized users based on role and project assignment.
- **Periodic Review** – PII collection and use are reviewed periodically to ensure continued alignment with operational needs and DOI privacy requirements.

Through these measures, ePlanning ensures that PII collection and use are limited to what is directly relevant and necessary to support NEPA processes.

Section 3: Data Sharing and Individual Rights

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

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

The ePlanning (EPL) system shares PII only as necessary to support NEPA comment management, administrative record development, and project tracking functions.

- **Within the Bureau/Office (Bureau of Land Management)** – PII is accessible to authorized BLM project team members through the secure back-office module for purposes of reviewing and managing public comments, developing responses, and monitoring the progress of NEPA projects. Access is limited to personnel with a need to know and governed by role-based access controls.

- **Public Disclosure (NEPA Administrative Record)** – Public comments submitted through ePlanning may be made available to the public as part of the official NEPA and Land Use Planning administrative record and may be incorporated into final Interactive Digital Documents. Individuals are informed at the time of submission that comments may be publicly available and that any information voluntarily provided may be subject to disclosure in accordance with the Privacy Act and the Freedom of Information Act (FOIA).

- **Contractors and Developers** – Authorized contractor personnel may access limited system data, including PII, only as necessary to perform approved design, development, testing, troubleshooting, operations, maintenance, and security support functions. Contractor access is limited by role-based access controls, least privilege, contract requirements, DOI Rules of Behavior, privacy and security training, and applicable Federal Acquisition Regulation privacy and information security clauses.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

- **Public Disclosure / NEPA Administrative Record** – Public comments and representative comments may be made publicly available as part of the NEPA or Land Use Planning administrative record, final planning documents, or related public transparency materials. Individuals are advised at the point of submission that comments and information voluntarily included in comments may be made publicly available or subject to release under FOIA.

All sharing is limited to what is necessary to support NEPA processes and is conducted in accordance with DOI privacy and security policies, including role-based access controls and secure handling requirements.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

☐ Yes
☒ No

The ePlanning (EPL) system does not have a MOU, MOA, or ISA for external PII sharing. All PII is maintained within BLM for NEPA comment management and administrative record purposes.

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

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Individuals submitting comments through the ePlanning (EPL) system may choose whether to provide PII and may decline to provide personal information.

- **Comment Submission** – Individuals may voluntarily provide limited contact information (e.g., name, email, telephone number, mailing address) when submitting comments on a NEPA action. These fields are optional, and individuals may submit comments anonymously.
- **Notice and Transparency** – Users are informed through a Privacy Notice at the point of submission regarding how their information will be used, including the potential public disclosure of comments.
- **Impact of Declining to Provide PII** – Declining to provide personal information does not prevent participation in the NEPA process; however, it may limit the ability of BLM to provide responses or updates related to submitted comments.
- **Voluntary Submission** –Providing contact information, such as name, mailing address, email address, and telephone number, is optional when submitting public comments on NEPA actions. Individuals may submit comments without providing this information; however, BLM will be unable to contact them regarding their submission or provide updates or responses related to the project.
- **Land Use Planning Protests -** During the protest period, individuals are required to provide limited PII, including first and last name, street address, city, state or territory, ZIP/postal code, and phone number, to establish standing in accordance with applicable land use planning regulations.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

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

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

The ePlanning system provides notice to individuals at the point of collection through a Privacy Notice displayed on the public-facing website and within the comment submission interface. The notice informs individuals of the purpose of the collection, the authority supporting the collection, how the information will be used in support of the NEPA process, and any applicable routine uses or disclosures.

The Privacy Notice informs individuals of the purpose of the collection, the authority supporting the collection, how the information will be used in support of the NEPA and Land Use Planning processes, whether providing information is voluntary or required for the applicable submission type, and the potential public disclosure of comments or protest materials as part of the administrative record or in response to FOIA.

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

The ePlanning system retrieves records using the following identifier:

- **Project Name or Project ID** – Used to retrieve all comments and associated records for a specific NEPA project.

Retrieval occurs through search functions within the ePlanning interface. The system does not retrieve records using personal identifiers; therefore, it does not meet the definition of a Privacy Act System of Records based on retrieval practices.

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

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

The ePlanning system does not generate reports on individuals whose PII is contained in the system. Reporting is limited to aggregated, project-level data based on project name or project ID. The system does not produce reports organized, retrieved, or disseminated by personal identifiers. While limited PII may be contained within individual public comments, it is not used for reporting purpose.

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

The ePlanning system receives limited PII directly from members of the public through voluntary comment submissions. The system does not receive PII from external authoritative sources. The verification process includes:

- **Automated Field Validation** – The submission interface applies required field checks and basic format

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

validation at the time of data entry.

- **User Responsibility** – Individuals are responsible for ensuring the accuracy and completeness of the information they provide at the time of submission.
- **Manual Review** – BLM personnel may review submissions to identify inappropriate or irrelevant content; however, PII is not independently verified against external data sources.

Because the information is voluntarily provided and not used to make determinations about individuals, no direct follow-up or confirmation process is conducted. These measures support maintaining data that is reasonably accurate, relevant, timely, and complete, consistent with Privacy Act requirements.

Section 4: Data Management and Retention

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

The ePlanning system retains records in accordance with applicable NARA-approved Department of the Interior (DOI) and General Records Schedules (GRS) governing administrative, operational, and information system security records. Temporary administrative and operational records are retained in accordance with DOI Departmental Records Schedule DAA-0048-2013-0008, which covers policy, administrative, and program support records. These records include system support documentation, routine correspondence, and operational tracking materials and are generally destroyed up to 8 years after cutoff in accordance with approved disposition authorities.

System audit logs and technical records are retained in accordance with General Records Schedule (GRS) 3.2, Information Systems Security Records (DAA-GRS-2013-0006-0001). These records include system access logs, monitoring data, and user activity records and are retained in accordance with operational and security requirements and destroyed when no longer needed for administrative, legal, audit, or security purposes.

If new data elements or record categories are introduced that are not covered under existing schedules, the ePlanning program will coordinate with the appropriate Records Officer to ensure a NARA-approved records schedule is applied or developed prior to retention or disposal.

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

The ePlanning system does not receive PII from external data sources; all information is voluntarily submitted by members of the public, verification and validation measures include:

- **Automated Data Handling** – Data is automatically managed within the ePlanning system, with basic system controls supporting data entry.
- **User-Provided Information** – Individuals entering comments may provide name and location information (city, state, country); however, accuracy and completeness are not verified and are not required for submission.

The system does not include processes to independently verify, update, or maintain PII, as it is designed to collect public comments on BLM NEPA activities rather than maintain records about individuals. These practices

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

are consistent with the limited use of PII within the system.

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

☒ Yes
☐ No

The ePlanning system includes logging capabilities to record and monitor access to the application and associated tables, including records that may contain PII.

- **Types of Logs** – System logs capture user authentication events (successful and failed logins), user access to the application, and interactions with system tables and records.
- **Security of Logs** – Logs are stored within the secure system environment and are accessible only to authorized system administrators. Log data is protected from unauthorized modification through role-based access controls and system-level safeguards.
- **Retention** – Logs are retained in accordance with the applicable DOI IT security and audit records schedule.
- **Review Process** – Designated system administrators and/or the Information System Security Officer (ISSO) review logs in accordance with the System Security Plan (SSP) and DOI continuous monitoring requirements. Logs are reviewed periodically and in response to suspected security or privacy incidents.

These measures support DOI's ability to detect, investigate, and respond to potential unauthorized access or misuse of records maintained within ePlanning.

Section 5. Privacy Risks and Mitigation Strategies

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

The ePlanning system collects, uses, retains, and discloses limited PII in support of BLM NEPA and Land Use Planning public participation and protest processes. Privacy risks have been identified at each stage of the information lifecycle, with mitigations applied.

Collection Risks – Potential over-collection of PII, submission of unnecessary or sensitive personal information in public comments, or collection without sufficient understanding that information may be publicly available.

- **Mitigation:** PII collection is voluntary under the NEPA commenting process and limited under the Land Use Planning protest process. A Privacy Notice is presented at the point of collecting, advising individuals not to include sensitive information and informing them that comments may be publicly available. Electronic submissions occur over secure HTTPS connections in accordance with DOI security requirements.

Use Risks – Unauthorized access to PII or use of information beyond the purpose of supporting NEPA documentation and public participation.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

- **Mitigation:** Access to PII is controlled through role-based permissions and project-level access assignments. The principle of least privilege is applied, and user activity is monitored consistently with DOI security controls.

Retention Risks – Retaining PII longer than necessary or maintaining outdated or irrelevant information.

- **Mitigation:** Records are maintained in accordance with NARA-approved record schedules for NEPA project records and managed in accordance with DOI records management policies.

Disclosure Risks – Unauthorized sharing or public disclosure of PII submitted within comments.

- **Mitigation:** Comments submitted through ePlanning are part of the public record. Individuals are advised not to include sensitive PII. Disclosures are limited to project-related purposes and protected through DOI security controls.

Residual Risks – Individuals may voluntarily include sensitive PII in public comments, which may be publicly disclosed.

- **Mitigation:** This risk is mitigated through clear notice and user advisories; however, it cannot be fully eliminated due to the nature of public participation systems.

These administrative and technical safeguards support compliance with the Privacy Act and DOI privacy and security requirements while maintaining transparency required under NEPA.

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

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

The ePlanning system does not generate new data or inferences about individuals through aggregation or analytics. It functions solely as a repository for public comments and project documentation, and information is not used to create profiles or inform decisions about individuals.

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

☐ Yes: *Provide explanation below*
☒ No

The ePlanning system does not create or add derived data to individual records, as it does not generate new data or maintain individual-level records beyond submitted public comments.

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

☐ Yes: *Provide explanation below*

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

☒ No

The ePlanning system does not create or add derived data to individual records, as it does not generate new data or maintain individual-level records beyond submitted public comments.

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

Not Applicable, the ePlanning system does not generate or derive new data. It stores information as submitted and does not perform validation or analysis to create new data elements.

Section 6: Automated Decision-Making and AI Risk Management

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

☐ Yes
☒ No, *Proceed to Section 7.*

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

N/A. The ePlanning system does not use artificial intelligence, machine learning, automated decision-making, model-based analytics, or federated learning."

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

☐ Yes
☐ No

N/A. The ePlanning system does not use artificial intelligence, machine learning, automated decision-making, model-based analytics, or federated learning.

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

☐ Yes
☐ No

N/A. The ePlanning system does not use artificial intelligence, machine learning, automated decision-making, model-based analytics, or federated learning.

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

☐ Yes
☐ No

N/A. The ePlanning system does not use artificial intelligence, machine learning, automated decision-making,

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

model-based analytics, or federated learning.

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

☐ Yes
☐ No

N/A. The ePlanning system does not use artificial intelligence, machine learning, automated decision-making, model-based analytics, or federated learning.

Section 7: Security and Access Controls

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

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe below*

BLM authorized employee users, managers, system administrators, developers, and contractors have access to data in the system based on assigned roles. Final BLM NEPA documents may include representative public comments and are available to the public. Use of an individual's comments in final documents is contingent upon consent provided during submission.

User Roles and Access Levels

- **System Administrators** – Administrative access to manage system configuration, user accounts, and system functionality, in accordance with the System Security Plan (SSP).
- **Project Leads** – Responsible for assigning user roles for individual projects, which determine the level of access granted to each user.
- **Back Office Federal Employees and Authorized DOI Staff** – Access is restricted to assigned project roles and limited to the minimum necessary to perform official duties.
- **Contractors and Developers** – Limited access required for system development, operations, and maintenance, consistent with contract requirements and DOI policies.

Authorization and Restrictions

- Access is granted based on documentation and approved through project-level role assignments by authorized personnel.
- All users must authenticate using DOI-managed credentials (Entra ID), with unique user IDs and multi-factor authentication.
- Role-Based Access Controls (RBAC) restrict access to data based on assigned project roles.
- User activity is logged and monitored in accordance with the System Security Plan (SSP).
- All users must comply with DOI Rules of Behavior and required privacy and security training.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

This tiered access structure ensures that only authorized users with a legitimate operational need can access system data, and that access is controlled and monitored in accordance with DOI security requirements.

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

The ePlanning system stores PII within a DOI-approved cloud environment that meets federal and Departmental security requirements as documented in the system's approved Authority to Operate (ATO). Cloud-based PII storage complies with:

- **DOI Cloud Computing Policy** – Requires use of FedRAMP-authorized cloud services and adherence to DOI security and privacy requirements.
- **FedRAMP Authorization (Impact Level documented in the ATO)** – Ensures implementation of NIST SP 800-53 Rev. 5 security controls appropriate to the system's categorization.
- **NIST SP 800-53 Rev. 5** – Establishes required security and privacy controls for federal information systems.
- **NIST SP 800-144** – Provides guidance for cloud computing security and risk management.

PII is protected through encryption in transit using TLS and encryption at rest using FIPS-validated cryptographic standards. Access is restricted through role-based access controls and authenticated user accounts with multi-factor authentication. System activity is logged and monitored in accordance with the System Security Plan (SSP).

The cloud service provider operates within a FedRAMP-authorized environment, and security controls are assessed to ensure compliance with DOI and federal requirements.

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

The ePlanning system uses DOI-managed monitoring capabilities to detect and respond to unauthorized access, use, or potential exfiltration of data:

- **Automated Monitoring Tools** – System and security logs are captured and monitored within DOI-managed logging and monitoring solutions, which analyze activity and identify anomalous behavior such as repeated failed login attempts or unusual access patterns.
- **Access Audit Logs** – User authentication and system activity are logged, including access events and system interactions. Logs are maintained in accordance with the System Security Plan (SSP) and DOI security requirements.
- **Alert and Incident Response** – Suspicious activity is identified through automated monitoring and reviewed by authorized personnel, including system administrators and security staff. Potential incidents are reported and handled in accordance with DOI incident response policies and procedures.

These controls support continuous monitoring and enable timely detection, investigation, and response to unauthorized access or misuse, consistent with DOI security policies and NIST SP 800-53 Rev. 5 control requirements.

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

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.
☐ No

The ePlanning system includes monitoring of user activity to support system security, maintain data integrity, and meet federal audit requirements.

Monitored Activities:

- User authentication events, including successful and failed login attempts
- System access and general user activity within assigned projects

Controls for Appropriate Use:

- Monitoring data is accessible only to authorized personnel, including the ISSO, system administrators, and designated security staff with a documented need-to-know.
- All monitoring activities are logged and reviewed in accordance with DOI security policies and the System Security Plan (SSP).
- The DOI Rules of Behavior and required privacy and security training inform users that their activity is monitored and define acceptable use.

Any use of monitoring data for investigations follows DOI incident response procedures and is documented for accountability.

Monitoring is limited to authorized system, security, and audit activity for workforce and contractor users. ePlanning does not use monitoring to track members of the public across unrelated websites, build profiles, or make determinations about individuals.

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

☒ Design
☒ Development
☒ Maintenance

Contractors are involved in the design, development, and maintenance of the ePlanning system.

- **Design**- Contractors support system design and enhancements to improve functionality and user experience.
- **Development** – Contractors develop system features, updates, and integrations.
- **Maintenance** – Contractors provide ongoing system support, including troubleshooting, updates, and performance monitoring.

Contractor personnel may have access to system data, including limited PII, only as necessary to perform authorized functions such as troubleshooting, testing, or system validation. Access is restricted to the minimum necessary in accordance with the principle of least privilege and is governed by the System Security Plan (SSP), Authority to Operate (ATO), and applicable DOI policies.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

All contractor personnel are required to comply with Federal Acquisition Regulation (FAR) Privacy Act clauses (FAR 52.224-1 and 52.224-2), complete DOI-approved privacy and security training, and adhere to DOI Rules of Behavior and non-disclosure requirements.

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

Physical Controls

☐ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☒ Safes
☒ Combination Lock
☐ Other: *Describe Below*

Describe the other types of controls implemented.

Technical Controls

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Other: *Describe Below*
☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

Describe the other types of controls implemented.

Administrative Controls

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☐ Other: *Describe Below*
☒ Methods to Ensure Only Authorized Personnel Have Access
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Records and Privacy Training
☒ Regular Monitoring of Users' Security Practices

Describe the other types of controls implemented

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

Individuals may file a Privacy Act complaint regarding the ePlanning system through the Department of the Interior's established Privacy Act complaint process.

- **Submission Methods** – Complaints may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240, or through the DOI FOIA/Privacy Act request portal.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

- **Responsible Office** – The DOI Chief Privacy Officer receives all Privacy Act complaints and assigns them to the appropriate Bureau Privacy Officer and Privacy Analyst for review and coordination with program officials.
- **Review Process** – The assigned reviewer evaluates the complaint, coordinates with the ePlanning System Owner and Information System Security Officer (ISSO) and determines whether a Privacy Act violation or policy issue occurred. If a potential breach is identified, DOI breach response procedures are initiated in accordance with the DOI Privacy Breach Response Plan.
- **Resolution and Response** – DOI provides a written response to the complainant outlining findings and any corrective action taken. Responses are generally issued within the timeframes established under 43 CFR Part 2, Subpart K.
- **Notice to Individuals** – Information on the right to file a Privacy Act complaint is provided through Privacy Notices at the point of collection and is available through the DOI Privacy Program website.

Describe how individuals can submit a Privacy Act complaint, including points of contact, mailing or email addresses, and any forms or procedures used. Note how complaints are logged, reviewed, and addressed by the DOI Privacy Office or responsible officials.

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

Individuals may access their records in ePlanning by submitting a written Privacy Act request in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and DOI regulations at 43 CFR Part 2, Subpart K.

- **Request Methods** – Requests may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, or through the DOI FOIA/Privacy Act request portal. The request must include sufficient identifying information and verification of identity (e.g., signed declaration under penalty of perjury or notarized statement).
- **Processing and Review** – Upon receipt, the DOI Privacy Office verifies the requester's identity and coordinates with BLM and the ePlanning System Owner to locate responsive records.
- **Response** – DOI responds within the timeframes established under 43 CFR Part 2, Subpart K, providing access to records unless subject to lawful exemptions or redactions.
- **Notice to Individuals** – Information on the right to file a Privacy Act complaint is provided through Privacy Notices at the point of collection and is available through the DOI Privacy Program website.

This process ensures compliance with Privacy Act access provisions while protecting the integrity and security of the records.

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

Individuals may request correction of inaccurate or erroneous information submitted through the ePlanning system in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and DOI regulations at 43 CFR Part 2, Subpart K.

- **Request Methods** – Requests for amendment may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, or through the DOI FOIA/Privacy Act request portal. The request must include sufficient identifying information, a description of the information to be corrected, and verification of identity.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

- **Processing and Review** – Upon receipt, the DOI Privacy Office reviews the request and coordinates with BLM and the ePlanning System Owner to determine whether the information can be corrected or amended.
- **Response** – DOI responds in accordance with applicable regulations, either making the requested correction or providing an explanation if the request is denied.
- **Limitations** – Because ePlanning primarily maintains public comment submissions associated with NEPA projects, individuals may also submit revised or updated comments; however, previously submitted comments that are part of the official project record may not be altered.

This process ensures compliance with Privacy Act amendment provisions while maintaining the integrity of official NEPA records.

10. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

Responsibility for assuring proper use of ePlanning data and reporting privacy incidents is shared among designated roles to ensure accountability, compliance, and timely incident response in accordance with DOI policy and NIST SP 800-53 Rev. 5.

- **BLM Assistant Director for WO-200 Renewable Resources Planning** – Provides operational oversight of system security and privacy controls, ensures data is properly managed, approves access based on mission need-to-know, and enforces implementation of controls in a secure and auditable manner.
- **Information System Security Officer (ISSO)** –Monitors technical safeguards, reviews audit logs, and coordinates incident response actions in collaboration with the Privacy Officer.
- **Bureau Privacy Officer / DOI Privacy Officer** – Provides oversight of Privacy Act compliance, advises on authorized uses of PII, and leads coordination of privacy breach response efforts, including risk assessment and mitigation activities.
- **Authorized Users** –Must comply with DOI Rules of Behavior, complete required privacy and security training, use data only for authorized purposes, and report suspected or confirmed incidents.

All DOI personnel and contractors with access to ePlanning data are required to report the loss, compromise, unauthorized disclosure, or unauthorized access of information to the DOI Computer Incident Response Center (DOI-CIRC) and the DOI Privacy Officer within one hour of discovery, in accordance with the DOI Privacy Breach Response Plan.

This shared responsibility model ensures proper data use, continuous monitoring, and timely reporting of incidents in accordance with DOI policy and NIST SP 800-53 Rev. 5 requirements.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

Section 8: Incident Response and Review

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

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

1. **Immediate Reporting** – Any suspected or confirmed breach must be reported within one hour of discovery to the DOI Computer Incident Response Center (DOI-CIRC) and the DOI Privacy Officer.
2. **Containment and Mitigation** – The ISSO and DOI-CIRC coordinate to contain the incident, secure affected systems, and prevent further unauthorized access or disclosure.
3. **Risk Assessment** – The Privacy Officer, in coordination with system and security officials, assesses the scope of the breach, the type of information involved, and the potential risk to individuals.
4. **Notification** – When required, affected individuals will be notified without unreasonable delay in accordance with DOI policy and OMB guidance, including information about the incident and recommended protective actions.
5. **Oversight Reporting** – DOI will report the incident to appropriate oversight entities, including OMB, DHS, and Congress, when required by federal policy.
6. **Remediation and Prevention** – Corrective actions are implemented, including updates to controls, procedures, and user training to prevent recurrence.

These steps ensure a timely, coordinated, and compliant response to mitigate harm and protect individuals' information.

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

The ePlanning Privacy Impact Assessment (PIA) will be reviewed and updated at least once every three years, in accordance with DOI policy and OMB requirements.
Interim updates will be conducted as needed when changes occur that may impact privacy risk, including:

- Significant modifications to system functionality, architecture, or hosting environment
- Changes in the type or use of information collected
- New data sharing practices or external integrations
- Implementation of new technologies that may affect privacy risk
- Changes to applicable laws, regulations, or DOI policies

The System Owner is responsible for initiating the review in coordination with the DOI Privacy Officer. Updated PIAs will undergo the appropriate review and approval process and will be made publicly available as required.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.