



U.S. Department of the Interior

PRIVACY IMPACT ASSESSMENT

Introduction:

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

System Information

System or Project Name:	Wild Horse and Burro Program ManeFrame
System or Project Acronym:	WHBP MF
Bureau or Office:	Bureau of Land Management
Date submitted for review:	April 3, 2026
System Operational Status:	Development

Point of Contact

Name:	Jamie Huang
Title:	Privacy Officer
Office:	Department Privacy Office
Phone:	(202) 208-1605
E-mail:	DOI_Privacy@ios.doi.gov
Address:	U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1: System Overview

1. What triggered this PIA? (Check one)

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

The Wild Horse and Burro Program ManeFrame system is being assessed because it represents a significant modernization of the existing Wild Horse and Burro Program System (WHBPS). ManeFrame is intended to replace the legacy WHBPS application and provide a modernized web-based environment for supporting Wild Horse and Burro Program business processes, including animal management, adoption, sale, transfer, compliance, reporting, user access management, and program oversight.

The modernization changes the technical environment, system architecture, user experience, and supporting platform used to collect, maintain, use, retrieve, share, and protect personally identifiable information (PII). This PIA is being completed to document the modernized system boundary, updated data flows, continued use of PII,

applicable SORN coverage, records retention requirements, privacy risks, safeguards, and access controls before the system is approved for full operational use.

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

The Wild Horse and Burro Program ManeFrame system is a Bureau of Land Management (BLM) web-based application that supports the Department of the Interior's responsibilities for managing wild horses and burros under the Wild Free-Roaming Horses and Burros Act of 1971. ManeFrame replaces and modernizes the legacy Wild Horse and Burro Program System (WHBPS) and serves as the primary program system for managing animal, herd, adoption, sale, transfer, compliance, facility, and program operational records.

ManeFrame supports BLM's ability to manage wild horses and burros on public lands; document the removal, care, adoption, sale, transfer, and title status of animals; monitor compliance with adoption, sale, transfer, and private care requirements; support program reporting; and provide program management information to authorized BLM personnel and partner agencies involved in the management of wild horses and burros.

ManeFrame collects and maintains PII necessary to identify applicants, adopters, purchasers, transferees, foster care providers, contractors, veterinarians, volunteers, service providers, BLM personnel, and other individuals involved in Wild Horse and Burro Program activities. The system also maintains records needed to assign and manage authorized system access. The PII maintained in ManeFrame may include sensitive PII such as Social Security numbers, driver's license numbers, dates of birth, personal contact information, addresses where animals are maintained, and compliance-related records.

ManeFrame supports the WHBP mission while protecting PII through role-based access controls, need-to-know restrictions, audit logging, encryption, training, Rules of Behavior, privacy and security controls, and records management requirements.

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 legacy Wild Horse and Burro Program System (WHBPS) is registered in BisonGRC under UII Code 010-000000171. ManeFrame is the modernized replacement for WHBPS and will use the applicable BisonGRC system registration and authorization record as determined through the DOI security authorization process. The BisonGRC record, system security documentation, and privacy documentation must be updated to reflect the ManeFrame modernization, including the current system name, hosting environment, system boundary, data flows, interfaces, access roles, and applicable privacy controls.

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

The collection, maintenance, use, and sharing of information in ManeFrame is authorized by the following authorities:

The Wild Free-Roaming Horses and Burros Act of 1971, as amended, 16 U.S.C. §§ 1331–1340, authorizes BLM to manage and protect wild free-roaming horses and burros on public lands and to administer activities related to the removal, care, adoption, sale, transfer, and management of excess animals.

The Federal Land Policy and Management Act of 1976, as amended, 43 U.S.C. §§ 1701–1787, provides BLM with land management authorities relevant to the administration of public lands and resources.

43 CFR Part 4700, Protection, Management, and Control of Wild Free-Roaming Horses and Burros, establishes regulatory requirements for the management, adoption, sale, transfer, care, and control of wild horses and burros.

31 U.S.C. § 7701, Taxpayer Identifying Number, authorizes collection of taxpayer identifying numbers where needed for Federal debt collection and related financial accountability purposes.

Section 208 of the E-Government Act of 2002 requires Federal agencies to assess privacy risks associated with information technology systems that collect, maintain, or disseminate PII.

The Privacy Act of 1974, 5 U.S.C. § 552a, governs the collection, maintenance, use, retrieval, and disclosure of records about individuals that are maintained in a system of records.

OMB Circular A-130, Managing Information as a Strategic Resource, establishes Federal agency responsibilities for privacy risk management, information governance, and the protection of PII.

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

☒ Yes: If yes, list the applicable citations below.

☐ No

ManeFrame retrieves records by personal identifiers, including individual name, Social Security number, driver's license number, address, organization name, and other identifiers associated with applicants, adopters, purchasers, transferees, foster care providers, contractors, volunteers, service providers, and program personnel. Therefore, ManeFrame is covered by a published Privacy Act System of Records Notice.

The applicable SORN is INTERIOR/BLM–37, Wild Horse and Burro Program (WHBP), 89 FR 25648, April 11, 2024. It covers records used to identify individuals who apply to obtain custody of wild horses or burros through adoption, sale, or transfer; document the rejection, suspension, or granting of those requests; monitor compliance with laws and regulations concerning adopted and fostered animals; identify contractors, employees, volunteers, and service providers; provide program management information to FS and APHIS; and identify and assign system access levels for BLM employees, contractors, and program personnel.

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

☒ Yes

☐ No

ManeFrame supports information collections associated with the Wild Horse and Burro Program, including applications and agreements used for adoption, sale, transfer, private maintenance and care, and related program activities. The applicable OMB Control Number is 1004-0042, Protection, Management, and Control of Wild Horses and Burros, 43 CFR Part 4700, currently approved through January 31, 2028.

Information collected from members of the public through WHBP forms and related collection instruments must display a valid OMB control number where required and must be consistent with the approved information collection, Privacy Act Statement, and applicable Paperwork Reduction Act requirements.

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

ManeFrame does not currently host separate minor applications or subsystems within the system boundary. However, ManeFrame receives, uses, or exchanges information with related WHBP processes and systems, including the BLM Online Corral, where adoption, sale, and private maintenance and care information may be collected or initiated.

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/facial recognition |
| ☐ Legal Status | ☐ Mother's maiden name | ☒ Vehicle information |
| ☐ Sex | ☐ Marital status | ☐ Passport information |
| ☐ Race or ethnicity | ☐ Spouse Information | ☐ Travel information |
| ☒ Date of birth | ☐ Child or family information | ☐ Parent's name |
| ☐ Place of birth | ☐ Emergency contact info | ☐ Credit card number |
| ☒ Personal cell phone number | ☐ Financial information | ☐ Nationality |
| ☒ Username / user ID / acct ID | ☒ IP address / network ID | ☒ Device ID / online ID |
| ☐ Geolocation / GPS / location | ☒ Photos / video / audio | ☐ Health / medical information |
| ☐ Tribal or other ID number | ☐ Education information | ☐ Disability Information |
| ☐ Criminal / disciplinary info | ☐ Military records | ☒ Other: Describe below |

ManeFrame collects, uses, and maintains PII necessary to administer WHBP activities. PII may include information submitted by applicants, adopters, purchasers, transferees, foster care providers, contractors, veterinarians, volunteers, service providers, BLM personnel, and other individuals involved in WHBP activities, including contact information, identity verification information, program participation records, animal custody or care information, compliance-related records, and system access information, as authorized by the applicable SORN and program requirements.

For BLM employees, contractors, volunteers, veterinarians, service providers, and other program personnel, ManeFrame may maintain work contact information, role or qualification information, certifications, services supplied, system access roles, approval authorities, usernames, user IDs, audit log information, and other access-related records necessary to administer system permissions and program responsibilities.

ManeFrame also maintains animal and herd records that may be linked to individuals, including animal freeze mark numbers, adoption or sale records, transfer records, care facility information, compliance records, and disposition information.

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

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

PII in ManeFrame is primarily collected directly from individuals who apply to adopt, purchase, transfer, foster, or maintain wild horses or burros, as well as from individuals who support WHBP operations, including contractors, veterinarians, volunteers, service providers, and program personnel.

Information may also come from BLM program records, legacy WHBPS records, BLM Online Corral records, field office records, compliance inspection records, correspondence, payment or fee-related records, program personnel, contractors, veterinarians, service providers, law enforcement entities, State, local, or Tribal agencies, the U.S. Forest Service, APHIS, and other sources related to WHBP services or program support.

Program officials may verify applicant information, facility information, address information, compliance status, or other eligibility-related information using available program records, address validation tools, field inspections, background or compliance checks, and other authorized sources.

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

- | | |
|--|---|
| ☒ Paper Format | ☐ Fax |
| ☒ Email | ☒ Telephone Interview |
| ☒ Face-to-Face Contact | ☒ Shared Between Systems: <i>Describe</i> |
| ☒ Website | ☒ Other: <i>Describe</i> |

Information is collected through paper forms, online forms, BLM Online Corral submissions, in-person interactions, telephone interviews, email communications, field inspections, program correspondence, data entry by authorized BLM personnel, and authorized system interfaces or data migration from legacy WHBPS records. Field personnel may collect information directly from individuals during application, adoption, sale, transfer, compliance, inspection, title, or private care processes and enter that information into ManeFrame.

ManeFrame may also receive information from the BLM Online Corral and other authorized WHBP sources to support adoption, sale, transfer, private maintenance and care agreements, compliance monitoring, and program management. Any electronic transfer of information must be documented in system security and privacy documentation and protected through approved technical and administrative safeguards.

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

ManeFrame uses PII to support the administration of the Wild Horse and Burro Program. The intended uses include:

1. Identifying and verifying individuals and organizations that apply to adopt, purchase, transfer, foster, or maintain wild horses or burros.
2. Documenting the approval, denial, rejection, suspension, cancellation, or completion of adoption, sale,

transfer, private care, or title-related requests.

3. Monitoring compliance with laws, regulations, agreements, and program requirements concerning the care and maintenance of adopted, fostered, transferred, or privately maintained animals.
4. Documenting facility information, inspection results, corrective actions, compliance records, and animal disposition information.
5. Supporting the care, movement, preparation, transport, training, adoption, sale, transfer, and disposition of wild horses and burros.
6. Identifying contractors, veterinarians, employees, volunteers, service providers, and other personnel required to perform WHBP functions.
7. Providing necessary program management information to agencies involved in WHBP-related activities, including the U.S. Forest Service and APHIS, as authorized.
8. Assigning and managing system access roles for authorized BLM employees, contractors, and program personnel.
9. Supporting audit logging, security monitoring, incident response, breach response, records management, reporting, and oversight activities.
10. Supporting authorized disclosures consistent with the Privacy Act, INTERIOR/BLM-37, and applicable law.

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

ManeFrame limits the collection and use of PII to the information necessary to administer WHBP functions, verify identity and eligibility, manage adoption, sale, transfer, private care, compliance, title, animal disposition, and system access processes, and meet legal, regulatory, records management, and program oversight requirements.

The system uses role-based access controls and need-to-know restrictions to limit access to PII based on assigned duties. Sensitive identifiers, including Social Security numbers and driver's license numbers, are used only for authorized program purposes such as identity verification, distinguishing individuals with similar names, supporting taxpayer identification or debt-related requirements where applicable, and administering adoption, sale, transfer, and compliance processes. Where full SSN display is not required, the program should use masking, restricted display, or limited-access controls to reduce unnecessary exposure.

ManeFrame does not collect PII unrelated to WHBP business needs. Any new collection, use, interface, report, or data element involving PII must be reviewed to ensure it is authorized, necessary, documented, and consistent with the applicable SORN, Privacy Act Statement, records schedule, security documentation, and privacy compliance requirements.

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.

PII in ManeFrame is shared within BLM with authorized personnel who require access to perform WHBP duties, including program staff, field office personnel, compliance personnel, Washington Office personnel, system administrators, system developers, database administrators, records personnel, FOIA personnel, security personnel, and other authorized users with an official need to know.

PII may be shared with other DOI bureaus or offices when necessary for authorized program, security, privacy, records management, FOIA, legal, audit, oversight, or incident response purposes. Contractors and service providers may access PII only when required to perform services on behalf of DOI or BLM and only under applicable contract requirements, access controls, Rules of Behavior, background investigation, training, and need-to-know restrictions.

PII may be shared outside DOI only when authorized by the Privacy Act, INTERIOR/BLM-37, applicable routine uses, applicable law, and DOI policy. Authorized external recipients may include the U.S. Forest Service, APHIS, other Federal agencies, State, local, territorial, or Tribal agencies, law enforcement entities, NARA, DOJ, OMB, Treasury, congressional offices, courts, contractors, consultants, grantees, shared service providers, and other entities as authorized by the SORN and applicable law.

Public disclosures must be limited to information authorized under INTERIOR/BLM-37, such as information about government operations and the disposition of wild horses and burros, including adoption, sale, transfer, death, or specific facility, and must be reviewed to ensure the disclosure does not constitute an unwarranted invasion of personal privacy.

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

No formal MOU, MOA, or ISA is currently in place for ManeFrame information sharing with external Federal, State, local, or Tribal agencies. ManeFrame is currently being modernized, and planned or future information exchanges will be reviewed to determine whether a written agreement, ISA, MOU, MOA, contract provision, or other documented authorization is required. Any future recurring external data sharing will be documented in the applicable system security documentation, privacy compliance documentation, and information sharing agreement, as required.

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 generally provide information voluntarily when they apply to adopt, purchase, transfer, foster, or maintain wild horses or burros, or when they participate in WHBP-related activities. However, the requested

information may be necessary for BLM to determine eligibility, verify identity, approve or deny an application, complete an agreement, transfer title, monitor compliance, or administer other WHBP requirements.

Individuals may decline to provide requested information, but failure to provide required information may result in denial, rejection, suspension, delay, cancellation, or inability to complete an adoption, sale, transfer, title, agreement, or related program action. Individuals are informed of the authority, purpose, routine uses, and consequences of not providing information through Privacy Act Statements on applicable forms, posted privacy notices, the applicable SORN, and this PIA.

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

☒ Privacy Act Statement:

☒ Other: *Describe Below*

☒ Privacy Notice:

☐ None: *Example - law enforcement cases.*

Notice is provided through Privacy Act Statements on applicable WHBP forms and collection instruments, privacy notices on relevant websites or online collection points, the published INTERIOR/BLM–37 SORN, this PIA, and DOI/BLM privacy policy notices. Where information is collected through BLM Online Corral or other online collection methods, the applicable Privacy Act Statement or privacy notice must be available to the individual before information is submitted.

The Privacy Act Statement must identify the authority for collection, the principal purpose of the collection, routine uses, whether disclosure is mandatory or voluntary, and the consequences of not providing the requested information.

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

Records in ManeFrame may be retrieved by personal identifiers and program identifiers, including name, Social Security number, driver's license number, address, organization name, user ID, role or certification, application or case information, and animal freeze mark number. Records may also be retrieved by adoption, sale, transfer, title, facility, compliance, or animal-related identifiers when those identifiers are linked to an individual or organization.

Because ManeFrame retrieves records by personal identifier, the system is subject to the Privacy Act and is covered by INTERIOR/BLM–37, Wild Horse and Burro Program (WHBP).

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

ManeFrame may generate reports that include PII when necessary for WHBP operations, compliance monitoring, program management, oversight, records management, or authorized disclosure. Reports may include information about applicants, adopters, purchasers, transferees, foster care providers, contractors, service providers, or other individuals associated with animal custody, facility information, compliance status,

title status, adoption or sale history, transfer activity, or program participation.

Access to reports containing PII is limited to authorized personnel with an official need to know. Reports must be protected according to DOI privacy, security, and records management requirements. Reports used for public release, FOIA, program transparency, or external sharing must be reviewed to ensure that PII is redacted or withheld when required and that any disclosure is authorized by law, the applicable SORN, and DOI policy.

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

Information collected directly from individuals is presumed to be accurate when submitted, but BLM may verify information as needed to determine eligibility, support program compliance, or administer WHBP requirements. Verification may include review by BLM program personnel, comparison with program records, address validation tools, contact with the individual, field inspection, review of supporting documentation, confirmation with authorized external sources, or other authorized validation methods.

Addresses submitted through adoption, sale, transfer, private maintenance and care, or title-related processes may be validated using address verification tools to determine whether the address is complete, valid, and deliverable. Compliance-related information may be verified through inspections, program review, documentation, correspondence, and follow-up with the individual or facility.

Section 4: Data Management and Retention

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

ManeFrame records are retained in accordance with the Departmental Records Schedule, General Records Schedule, and BLM Records Retention Catalog, as applicable. WHBP records may be temporary or permanent depending on the specific record type.

The WHBP master file is permanent and is retained under BLM Records Retention Catalog Schedule 4, Property Use and Disposal Records, Item 4/8j(1), approved by NARA under N1-049-09-4. WHBP master file records are cut off every five years and transferred to NARA with current technical documentation in accordance with applicable records management requirements.

Other WHBP records, including adoption records, applications, animal preparation records, shipping records, facility case files, duplicate files, and related operational records, may be temporary and must be retained and disposed of in accordance with the applicable approved records schedule. Destruction of temporary records must be performed using approved methods, including shredding or pulping for paper records and approved deletion, erasure, or sanitization methods for electronic records.

The system owner must coordinate with the BLM Records Officer to confirm the applicable records schedules for each record category maintained in ManeFrame and ensure retention requirements are documented in the system records management plan and security/privacy documentation.

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

ManeFrame uses both manual and automated processes to support data accuracy and completeness. Information submitted by individuals is reviewed by authorized BLM personnel and may be verified through address validation tools, required form fields, supporting documentation, program review, field inspection, compliance follow-up, and comparison with existing program records.

When information is received from external sources or related systems, authorized personnel review the information for completeness and consistency before it is used for program decisions or added to the official record. Data received through system interfaces or migration processes must be validated through testing, reconciliation, quality checks, and user acceptance review before operational use. Any identified inaccuracies may be corrected through program procedures, direct contact with the individual, or formal Privacy Act amendment procedures, as applicable.

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

☒ Yes

☐ No

ManeFrame includes logging and monitoring capabilities to record and monitor access to PII. The system uses Power Platform and Dataverse audit logging, administrative monitoring, access logs, security logs, and related enterprise monitoring capabilities to track user activity, system access, administrative activity, and access to data tables, including tables that contain PII.

Audit logs support security monitoring, incident response, access control, accountability, and detection of unauthorized access, use, modification, or disclosure of PII. Access to audit logs is restricted to authorized administrators, security personnel, and other officials with an official need to know. Logs are reviewed and maintained in accordance with DOI security, privacy, and records management requirements.

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?

ManeFrame presents a moderate privacy risk because it maintains sensitive PII and a large volume of program records associated with applicants, adopters, purchasers, transferees, foster care providers, contractors, volunteers, veterinarians, service providers, BLM personnel, and other individuals involved in WHBP activities. Sensitive PII may include Social Security numbers, driver's license numbers, dates of birth, personal contact information, physical facility addresses, compliance records, and other information linked to individuals.

Collection risk: There is a risk that more PII could be collected than necessary or that individuals may not understand why their information is required. This risk is mitigated through approved forms, Privacy Act Statements, PRA-approved collection instruments, data minimization, required-field review, program procedures, and publication of the applicable SORN and PIA.

Use risk: There is a risk that PII could be used for unauthorized purposes or accessed by personnel without a need to know. This risk is mitigated through role-based access controls, least privilege, need-to-know restrictions, user provisioning approvals, Rules of Behavior, privacy and security training, annual access reviews,

and audit logging.

Retention risk: There is a risk that records could be retained longer than necessary or disposed of before authorized. This risk is mitigated through use of NARA-approved records schedules, coordination with records officials, documented retention requirements, and records management procedures for temporary and permanent WHBP records.

Disclosure risk: There is a risk that PII could be improperly shared within DOI, with external agencies, with contractors, or with the public. This risk is mitigated by limiting disclosures to those authorized by the Privacy Act, INTERIOR/BLM-37, routine uses, FOIA, records management requirements, and DOI policy. Public disclosures are reviewed to prevent unwarranted invasions of personal privacy.

Security risk: There is a risk of unauthorized access, modification, exfiltration, or compromise of PII. This risk is mitigated through encryption, multi-factor authentication, role-based access, audit logging, network monitoring, access reviews, incident response procedures, background checks, contractor controls, and DOI/BLM security controls.

Accuracy risk: There is a risk that inaccurate information could affect an adoption, sale, transfer, compliance action, title action, or other program outcome. This risk is mitigated through collection from individuals where practicable, address validation, program review, supporting documentation, inspections, correction processes, and Privacy Act amendment procedures.

Breach risk: There is a risk that PII could be lost, compromised, or disclosed without authorization. This risk is mitigated through mandatory reporting to DOI-CIRC, coordination with the BLM Privacy Officer and Department Privacy Office, preservation of logs and evidence, breach risk assessment, containment, mitigation, notification analysis, corrective action, and post-incident review.

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

ManeFrame does not use artificial intelligence or machine learning to generate predictions or automated determinations about individuals. However, the system may aggregate program information about individuals, organizations, animals, facilities, adoption history, sale history, title status, transfer activity, and compliance records to support WHBP operational decisions and reporting.

For example, ManeFrame may aggregate information to determine how many animals an adopter or purchaser has obtained, whether legal or program limits apply, whether compliance requirements have been met, whether title may be issued, or whether additional review is needed. These aggregations are based on program records maintained in the system and are reviewed by authorized personnel before being used for program action.

Risks associated with aggregation include inaccurate matching, incomplete records, or overreliance on system-generated summaries. These risks are mitigated through human review, validation against source records, role-based access controls, audit logging, correction procedures, and Privacy Act access and amendment rights.

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

- ☒ Yes: *Provide explanation below*
☐ No

To the extent ManeFrame produces or records program determinations, compliance status, title status, adoption or sale history, transfer information, facility information, inspection results, or other official program information about an individual, that information may become part of the individual's program record. Any such information must be based on authorized program data, reviewed by authorized personnel, and maintained in accordance with applicable records schedules, access controls, and Privacy Act requirements.

ManeFrame does not create AI-generated records or automated predictive determinations about individuals.

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

- ☒ Yes: *Provide explanation below*
☐ No

ManeFrame supports program determinations by consolidating and organizing WHBP records that allow authorized personnel to evaluate adoption, sale, transfer, title, facility, and compliance information. The system may help personnel determine whether an individual has met program requirements, exceeded applicable limits, is eligible for title, requires compliance follow-up, or is associated with specific animals, facilities, or prior program actions.

These determinations are not fully automated and are made by authorized program personnel based on program records, applicable law, regulation, policy, and supporting documentation. The system supports decision-making by making relevant information available to authorized users, but final program determinations remain subject to human review and applicable procedural requirements.

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

New or aggregated program information is verified through review by authorized WHBP personnel, comparison with source records, validation of required data fields, address validation, supporting documentation, inspection results, correspondence with the individual, compliance review, and other program procedures. Where an individual believes information is inaccurate, the individual may seek correction through BLM program procedures or submit a Privacy Act amendment request in accordance with DOI regulations and the applicable SORN.

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. ManeFrame does not use AI, machine learning, generative AI, federated learning, or AI-based decision-making. Any future AI capability or AI use case must be reviewed before implementation.

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

- ☐ Yes
☐ No

N/A. ManeFrame does not use AI, machine learning, generative AI, federated learning, or AI-based decision-making. Any future AI capability or AI use case must be reviewed before implementation.

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

- ☐ Yes
☐ No

N/A. ManeFrame does not use AI, machine learning, generative AI, federated learning, or AI-based decision-making. Any future AI capability or AI use case must be reviewed before implementation.

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

- ☐ Yes
☐ No

N/A. ManeFrame does not use AI, machine learning, generative AI, federated learning, or AI-based decision-making. Any future AI capability or AI use case must be reviewed before implementation.

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

- ☐ Yes
☐ No

N/A. ManeFrame does not use AI, machine learning, generative AI, federated learning, or AI-based decision-making. Any future AI capability or AI use case must be reviewed before implementation.

Section 7: Security and Access Controls

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

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

Access to ManeFrame is limited to authorized personnel with an official need to know. Users may include BLM WHBP program staff, field office personnel, Washington Office personnel, compliance personnel, system administrators, developers, database administrators, contractors, security personnel, records personnel, FOIA personnel, Privacy Officers, Privacy Analysts, and other authorized officials who require access to perform assigned duties.

Access is determined based on job duties, role, need to know, and system authorization requirements. Access privileges are approved by authorized program or system officials before account creation or modification. ManeFrame uses role-based access controls to limit users to the data and functions necessary to perform their duties. Higher-privilege access, including administrator or developer access, is restricted, documented, reviewed, and monitored.

Accounts are reviewed periodically to confirm that access remains appropriate. Accounts are modified or disabled when users change roles, leave the program, no longer require access, or fail to meet access requirements. Users must complete required privacy, security, records management, and role-based training, and must acknowledge DOI Rules of Behavior before accessing the system.

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

ManeFrame is hosted within a DOI/BLM-approved Microsoft cloud environment using Power Platform, Dataverse, and related Azure capabilities, as applicable. PII stored or processed in the cloud is protected through Federal, Departmental, bureau, contractual, and system-specific security and privacy requirements.

Applicable requirements include the Privacy Act of 1974, E-Government Act Section 208, OMB Circular A-130, Federal Information Security Modernization Act requirements, NIST SP 800-53 Rev. 5 security and privacy controls, FIPS 199 security categorization requirements, FedRAMP requirements for applicable cloud services, DOI cloud security policies, DOI Rules of Behavior, DOI incident response requirements, contract clauses governing protection of Federal information, and system-specific security authorization requirements.

Controls include encryption in transit and at rest, role-based access, multi-factor authentication, least privilege, audit logging, privileged access restrictions, data loss prevention policies, backup protection, continuous monitoring, vulnerability management, incident response procedures, and access reviews. Contractors and administrators with access to cloud-hosted PII must meet applicable background investigation, training, Rules of Behavior, and access authorization requirements.

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

ManeFrame uses Power Platform, Dataverse, Azure, and DOI/BLM enterprise security monitoring capabilities to detect and respond to unauthorized access, use, modification, or exfiltration of PII. Monitoring may include authentication logs, access logs, administrative activity logs, Dataverse audit logs, data table access logs, security alerts, system usage analytics, anomaly detection, and enterprise network/security monitoring.

Audit logs support accountability by recording user and administrative activity, including access to records, changes to data, authentication activity, and system events. Logs are available to authorized administrators, security personnel, and other officials with a need to know. Suspected unauthorized access, use, or disclosure is reported and handled through DOI incident response and privacy breach response procedures.

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

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

ManeFrame monitors authorized user activity for security, audit, access control, operational support, and incident response purposes. Monitoring includes user authentication, system access, administrative activity, access to data tables, changes to records, and other activity necessary to protect the system and PII.

This monitoring is not used to track members of the public for behavioral profiling or surveillance. Monitoring information is used to protect the system, detect unauthorized access or misuse, support investigations of suspected incidents, support audit requirements, and ensure accountability. Access to monitoring data is limited to authorized administrators, security personnel, and officials with an official need to know. Monitoring is governed by DOI security policies, privacy requirements, Rules of Behavior, and applicable NIST controls.

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

- ☒ Design
☒ Development
☒ Maintenance

Contractors may support ManeFrame design, development, maintenance, testing, technical administration, user support, or other system support activities. Contractor access to PII is limited to personnel with an official need to know and must be authorized, documented, and monitored.

Contractors must meet applicable background investigation requirements, complete required DOI privacy, security, records management, information management, and role-based training, sign applicable Rules of Behavior, and comply with contract requirements for protecting PII and Federal information. Contractors with elevated privileges or access to the cloud environment must meet applicable privileged access, administrator, and cloud security requirements before access is granted.

Contractor access is removed when no longer required, when duties change, or when contract support ends.

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

Physical Controls

- | | |
|---|--|
| ☒ Security Guards | ☐ Cipher Locks |
| ☐ Key Guards | ☒ Identification Badges |
| ☒ Locked File Cabinets | ☐ Safes |
| ☒ Secured Facility | ☐ Combination Lock |
| ☒ Closed Circuit Television | ☒ Other: <i>Describe Below</i> |

Restricted access areas for paper records, controlled office access, visitor controls, and secure storage procedures.

Technical Controls

- | | |
|--|--|
| ☒ Password | ☒ Intrusion Detection Systems (IDS) |
| ☒ Firewall | ☐ Virtual Private Network (VPN) |
| ☒ Encryption | ☒ Public Key Infrastructure (PKI) Certificates |
| ☒ User Identification | ☐ Biometrics |
| ☒ Other: <i>Describe Below</i> | |

Multi-factor authentication, Role-based access control, Audit logging, Data loss prevention controls, Privileged access restrictions, Power Platform/Dataverse/Azure monitoring and security controls.

Administrative Controls

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

ManeFrame protects PII through layered physical, technical, and administrative controls. Physical controls include secured facilities, identification badges, security guards, locked file cabinets, controlled access areas, and visitor controls. Technical controls include multi-factor authentication, user identification, role-based access control, encryption, firewall protections, intrusion detection, audit logging, data loss prevention controls, privileged access restrictions, and monitoring through DOI/BLM enterprise security capabilities and Power Platform/Dataverse tools. Administrative controls include Rules of Behavior, mandatory privacy/security/records training, role-based training, background investigation requirements, access approval procedures, access reviews, incident response procedures, privacy breach response procedures, contractor requirements, and records management controls.

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

Individuals who believe their Privacy Act rights have been violated may contact the Department Privacy Office. Privacy Act complaints are reviewed, coordinated, and addressed in accordance with DOI Privacy Act regulations, DOI privacy policy, and applicable Department procedures.

Individuals may contact the Department Privacy Office at DOI_Privacy@ios.doi.gov. Complaints involving ManeFrame records will be coordinated with the appropriate program office, system owner, Privacy Officer, Privacy Analyst, and other officials as needed.

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

Individuals may request access to records about themselves in ManeFrame by submitting a Privacy Act request in accordance with 43 CFR Part 2, Subpart K, and the Records Access Procedures in INTERIOR/BLM-37, Wild Horse and Burro Program (WHBP). Requests must reasonably describe the records sought and include the requester's full name, current address, and sufficient identifying information to verify identity, such as date of birth or other information needed to locate the record.

Requests must be signed and dated and either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. § 1746. Requests submitted by mail should be clearly marked as a Privacy Act request for access. DOI forms and instructions for submitting Privacy Act requests are available through DOI's Privacy Act request process.

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

Individuals may request amendment of records about themselves in accordance with 43 CFR Part 2, Subpart K, and the Contesting Record Procedures in INTERIOR/BLM–37, Wild Horse and Burro Program (WHBP). A request for amendment must identify the specific record to be corrected, explain why the record is inaccurate, irrelevant, untimely, or incomplete, and provide the proposed correction.

The request must include the requester's full name, current address, sufficient identifying information to verify identity, and a signed and dated verification of identity, notarized or submitted under penalty of perjury. Where appropriate, individuals may also work with BLM program personnel to correct operational information submitted through WHBP processes, but formal Privacy Act amendment requests must be handled under DOI's Privacy Act procedures.

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?

The ManeFrame Information System Owner, Program Manager/Product Owner, Information System Security Officer, and authorized BLM program officials are responsible for ensuring proper use of ManeFrame data and for enforcing access, security, privacy, and records management requirements. Users are responsible for using information only for authorized official purposes and for protecting PII in accordance with DOI policy, training, Rules of Behavior, and applicable law.

Any suspected or confirmed loss, compromise, unauthorized access, unauthorized use, or unauthorized disclosure of PII must be reported immediately to DOI-CIRC and the appropriate Privacy Officer. The System Owner, ISSO, Program Manager/Product Owner, BLM Privacy Officer, Privacy Analyst, and Department Privacy Office coordinate as needed to assess the incident, preserve evidence, determine affected records and individuals, support breach risk analysis, and implement mitigation and corrective actions.

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 suspected or confirmed privacy incident involving ManeFrame, the discovering party, System Owner, Program Manager/Product Owner, ISSO, or other responsible official must immediately report the incident to DOI-CIRC and notify the appropriate Privacy Officer and Department Privacy Office. The ManeFrame team will preserve relevant logs, records, and technical evidence; identify the affected system components, data elements, users, and individuals; and support immediate containment actions.

Containment actions may include disabling compromised accounts, limiting access, isolating affected components, suspending data processing, correcting permissions, removing improperly exposed records, or

taking other steps necessary to prevent further exposure. The Department Privacy Office, in coordination with BLM, DOI-CIRC, the ISSO, the System Owner, program officials, legal counsel, communications officials, and other stakeholders as appropriate, will assess the likelihood and risk of harm, determine whether affected individual notification or other mitigation is required, and coordinate any required reporting.

Mitigation may include notification to affected individuals, credit or identity monitoring where appropriate, correction of access controls, user retraining, technical remediation, disciplinary or administrative action where warranted, documentation of corrective actions, and post-incident review to prevent recurrence.

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

This PIA will be reviewed at least annually as part of the system's privacy, security, and FISMA review cycle and must be updated whenever there is a significant change to ManeFrame's technology, system boundary, hosting environment, data collection, data sharing, interfaces, access controls, use of PII, records retention, SORN coverage, reporting, or privacy risk posture.

The PIA must also be reviewed and updated before deployment of any new AI, machine learning, automated analytics, scoring, ranking, recommendation, inference, generative AI, new public-facing collection, new external data sharing arrangement, new cloud service, major interface, or material change in how records are collected, maintained, used, retrieved, disclosed, or disposed of.