U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Wild Horse and Burro Program System (WHBPS)

Bureau/Office: Bureau of Land Management
Date: August 16, 2018
Point of Contact:
Name: Suzanne S Wachter
Title: BLM Associate Privacy Officer
Email: swachter@blm.gov
Phone: 202-912-7178
Address: 20 M Street SE, Washington DC 20003

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Bureau of Land Management (BLM) Wild Horse and Burro (WH&B) Program manages land designated as Herd Areas (HAs) and Herd Management Areas (HMAs), as well as the horses, burros, and mules on that land. These animals are considered cultural resources by law; therefore, the BLM must manage the animals and the land they roam as a resource. The WH&B Program also tracks these

types of animals on lands managed by other agencies (for example, the U.S. Forest Service), under agreements with those agencies.

WHBPS provides data input, storage, and retrieval capabilities for the WH&B Program, with users across the entire BLM. It supports data for monitoring the wild herds and their habitat, as well as removing some of the animals from the wild, caring for them, and finding responsible owners for them through adoptions and sales. WHBPS contains histories and detailed records for over 300,000 animals and over 100,000 adopters, buyers, and suppliers.

WHBPS is an internal BLM web application. It is accessed via BLM Application Security System (BASS) by authorized users who are logged into the BLM intranet via a web-based user interface that is supported by an application server and a database server, as well as non-essential interfaces to other systems.

WHBPS uses BASS for authentication which links to the DOI Active Directory (AD) for authentication. AD authentication for user access is covered under the DOI Enterprise Hosted Infrastructure (EHI) privacy impact assessment. For additional information on authentication please see the EHI PIA on the DOI Privacy website (www.doi.gov/privacy/pia).

C. What is the legal authority?

The Wild Free Roaming Horses and Burros Act of 1971
The Federal Land Policy and Management Act
The Public Rangelands Improvement Act
43 CFR 4700
16 U.S.C. 1333 and 31 U.S.C. 7701

D. Why is this PIA being completed or modified?

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

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name* The UII Code for WHBPS is 010-000000171. The System Security Plan (SSP) for Wild Horse & Burro Program System covers this system.
☐ No

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

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

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

☒ Yes: *List Privacy Act SORN Identifier(s)* BLM-37, Wild Horse & Burro Program System, 72 FR 67956, 3 Dec 2007, and BLM-28, Adopt-A-Horse, 51 FR 25111, 10 July 1986. Both SORNs may be viewed at https://www.doi.gov/privacy/blm_notices. BLM-37 is currently being revised to provide updated content for the system and incorporate new Federal government-wide requirements in accordance with OMB Circular A-108. The records form BLM-28 will be incorporated into BLM-37 during this revision to create a SORN that covers the program area and BLM-28 will be rescinded.

☐ No

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

☒ Yes: *Describe* The BLM Application for Adoption of Wild Horse(s) or Burro(s) obtained OMB approval, OMB Control Number is 1004-0042, title "Protection, Management, and Control of Wild Horses and Burros (43 CFR part 4700)." Expiration Date is February 29, 2020.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Birth Date
☒ Personal Email Address
☒ Home Telephone Number

☒ Mailing/Home Address
☒ Driver's License
☒ Other: *Specify the PII collected.* Facility Address where the animal is kept.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☐ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe* Program officials may verify applicants' information or conduct background checks on applicants.

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

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Web site
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems
☐ Other: *Describe*

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

The primary uses of the information are to:

1. Identify and verify individuals who have applied to obtain custody of a wild horse or burro through adoption or sale;
2. Document the rejection, suspension or granting of the request for adoption or sale;
3. Monitor compliance with laws / regulations concerning maintenance of adopted animals;
4. Identify contractors / employees / volunteers/ service providers required to perform program functions;
5. Provide necessary program management information to other agencies involved in management of wild horses and burros on public lands, i.e., the U.S. Forest Service (FS) and the Animal and Plant Health Inspection Service (APHIS);
6. Identify and assign level of system access required by BLM wild horse and burro program personnel; and
7. Authorize the disclosure of records to individuals involved in responding to a breach of Federal data.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

The information is shared throughout the BLM with personnel who are involved in the Wild Horse and Burro program, the Washington Office personnel who perform oversight of Wild Horse and Burro Program, BLM Law Enforcement, and with system developers and database administrators who assist in maintaining this system. Additionally, information is shared with Freedom of Information Act (FOIA) officers as required in response to FOIA requests.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Office of the Inspector General and other authorized auditors. Information may also be shared with other Bureaus and offices as authorized and described in the routine uses contained in the BLM-37, Wild Horse & Burro Program System (WHBPS) and BLM-28, Adopt-A-Horse system of records notices.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Information may also be shared with the General Accounting Office and other Federal Agencies as authorized and described in the routine uses contained in the BLM-37, Wild Horse & Burro Program System (WHBPS) and BLM-28, Adopt-A-Horse system of records notices.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Information may also be shared with Tribal, State or Local Agencies, such as Law Enforcement Agencies, as authorized and described in the routine uses contained in the BLM-37, Wild Horse & Burro Program System (WHBPS) and BLM-28, Adopt-A-Horse system of records notices.

☒ Contractor: *Describe the contractor and how the data will be used.*

Information may also be shared with contractors who provide program support or IT system administration support.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Disclosures may be made to organizations or members of the general public as to the disposition of wild horses or burros, or other Federal agencies as authorized and described in the routine uses contained in the BLM-37, Wild Horse & Burro Program System (WHBPS) and BLM-28, Adopt-A-Horse system of records notices.

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

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Submission of the requested information on the Application for Adoption of Wild Horses or Burros, Application to Purchase Wild Horses and Burros, the Private Maintenance and Care Agreement for Wild Horses or Burros, and the Bill of Sale for Wild Horses and Burros is voluntary, but necessary, to obtain or retain a benefit. Individuals can decline to provide the information, however, failure to submit all of the requested information or to complete one of these forms may result in the rejection and/or denial of the application.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

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

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is included on all the relevant forms used by the program to collect information. The Privacy Act Statement will be available via a linked web page on the official BLM Wild Horse and Burro Online Corral website, as well as a PDF file that can be downloaded and printed.

☒ Privacy Notice: *Describe each applicable format.*

The Wild Horse & Burro website contains a link directing individuals to the DOI privacy policy. Notice is also provided through the publication of this privacy impact assessment and the BLM-37, Wild Horse & Burro Program System (WHBPS) system of records notice, which may be viewed at https://www.doi.gov/privacy/sorn. BLM-28, Adopt-A-Horse system of records notice, which may be viewed at https://www.doi.gov/ocio/policy-mgmt-support/privacy/BLM_28.

☐ Other: *Describe each applicable format.*

☐ None

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

Personal information is likely to be retrievable by (1) name; (2) driver's license; (3) SSN; (4) Address; (5) Role/Certification; (6) animal freeze mark number. These are the minimum identifiers by which the Wild Horse and Burro program can uniquely distinguish specific adopters and personnel, especially where records are stored about several members of the same family.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Reports that include information on individuals are based on the numbers of animals adopted or sold by year; animals maintained at a private care facility; numbers of animals titled to an individual; and compliance records. Access to reports containing identifiable personal information is limited to those with a "need to know" to complete program management responsibilities.

☐ No

Section 3. Attributes of System Data

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

Information is obtained directly from individuals through the application process and is presumed to be accurate when provided by the applicant. Addresses submitted by individuals on the Application for Adoption of Wild Horses or Burros, Application to Purchase Wild Horses and Burros, the Private Maintenance and Care Agreement for Wild Horses or Burros and the Bill of Sale for Wild Horses and Burros are verified using Commercial off the Shelf software that determines if an address is complete, valid, and deliverable by the U.S. Postal Service.

B. How will data be checked for completeness?

Information is obtained directly from individuals through the application process and is presumed to be complete when provided by the applicant. WHBPS includes automated edit checks for completeness and valid domain values. Automated business processes include checks for information completeness at each step of every transaction. For example, when filling out a multi-page electronic application on the Web, it will automatically roll back incomplete transactions. Address information is checked using COTS software that determines if an address is complete, valid, and deliverable by the U.S. Postal Service.

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

Information is obtained directly from individuals through the application process and is presumed to be current when provided by the applicant. Data in the system is historical in nature, for example, the date when an adoption took place, or the date certain vaccinations were performed. All records are accompanied by audit information, including date of update. The Project Management Office monitors the data, providing reports and communication to data stewards to help ensure that the data is current.

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

The BLM Records Retention schedule is BLM 4/8j(1), which has been approved by the National Archives Records Administration (NARA). Records for WHBPS are permanent, with a cut off every 5 years for transmission to NARA.

Transfer a copy of the master file to NARA upon approval of this schedule, along with the technical documentation, in accordance with 36 CFR 1235.44-50. Thereafter, transfer a copy every 5 years, along with the current technical documentation. (N1-049-09-4, 1a).

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

The procedures for the WHBPS files are documented in BLM 4/8j(1). This system contains no temporary records.

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

There is a moderate privacy risk due to the type and volume of personal information maintained in the system. WHBPS manages land designated as Herd Areas (HAs) and Herd Management Areas (HMAs), as well as the horses, burros, and mules on that land. WHBPS also supports data for monitoring the wild herds and their habitat, as well as removing some of the animals from the wild, caring for them, and finding responsible owners for them through adoptions and sales. WHBPS contains histories and detailed records for over 300,000 animals and over 100,000 adopters, buyers, and suppliers. Information collected and used is limited to the minimum required to perform the purpose and functions of the system.

There is a risk that individuals may gain unauthorized access to the information in the system. System security controls are in place to prevent access by unauthorized individuals to sensitive information. WHBPS is classified as moderate for FISMA and has all of the required system security documentation and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, WHBPS has controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions and software controls. All employees including contractors must meet the requirements for protecting Privacy Act information.

Business rules and guidelines, as well as rules of behavior, have been established to prevent inadvertent disclosure to individuals not authorized to use the system or those who do not have a direct "need to know" certain information contained in the system. All end-users have an individual password and ID that is issued by the WHBPS application steward. All new users will receive training on the use of the system. All DOI employees must complete mandatory privacy, security and records management training annually, and acknowledge the DOI Rules of Behavior.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting and sharing information with unauthorized recipients. This risk is mitigated by limiting access to the system to only those personnel who have an official need to perform their job duties. Access to information is role-based and is only granted on a need-to-know basis, and requires DOI credentials. Accounts are reviewed annually to ensure that only authorized personnel have systems logins. Additionally, any account that is inactive for more than one year is automatically suspended. All personnel accessing the system must acknowledge the rules of behavior prior to each login. The System Security Plan describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data via User ID, IP Address, etc. Audit trails are also captured within the system to determine who has added, deleted or changed the data within the system. Any qualification overrides require that the account manager document the reasoning and the login name with date and time is added by the system.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored has intentionally been limited; only the minimal amount of data needed for identification purposes is maintained and used by the system. Records are maintained in accordance with Department Records Schedules that were approved by NARA. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

There is a risk that an application may be denied based on the submission of inaccurate information. All information is obtained directly from the applicant so is presumed to be complete and accurate. Any inaccurate information provided by the applicant may be corrected during user validation procedures or by the applicant themselves.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA and the BLM Wild Horse and Burro Program System notice, and the Privacy Act statements provided on the applications and the official BLM website.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation* The use of data is automated to serve specific business process needs. The SSN is used to identify potential adopters and for debt collection purposes. We use it to track all of our adopters and prevent applicants with violations, such as animal abuse, from adopting using a different name and address.

☐ No

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

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

WHBPS does not derive new data. The system provides the capability to aggregate information about an adopter to determine how many animals the adopter has obtained, since there are legal limitations on that number.

Reports are compiled but not stored in the system and hard copies are managed per existing BLM guidance for protecting basic personal information records, to protect them from unauthorized access or disclosure. System access to reports is controlled as documented in the National Applications System Security Plan. Other aggregations are produced for program progress reporting, but do not identify individuals. Where no Privacy Act issue is concerned, reports ordinarily are releasable to the public.

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

Not applicable

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

The system operates under a formal system security plan, and is subject to security C&A requirements. The current design segregates functions that may involve Privacy Act information so that role-based security restrictions can be implemented more confidently.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

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

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

Roles and associated access privileges are established as part of the System Security Plan. Access is controlled by assignment of roles and is limited to necessary access. Individual access to the system and authorizations within the system require signed documentation from the program prior to creation or modification. Access is controlled by assignment of roles and specific discrete authorizations and is limited to necessary access. Therefore, individuals have limited access to the data. For example, there is a role for volunteers which hides the PII in the system.

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

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

The Privacy Act clauses are included in the Information Technology Support Services contract, which is the contract supporting the system.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

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

☐ Yes. *Explanation*

☒ No

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

Not applicable

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

Not applicable

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits

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

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Privacy Officer and WHBPS System Manager is responsible for protecting the privacy rights of the public and employees affected by the interface. The Assistant Director for Renewable Resources and Planning (WO-200), is the WHBPS Information System Owner and the official responsible for oversight and management of the WHBPS security and privacy controls and the protection of agency information processed and stored in the WHBPS application. The Information System Owner and WHBPS Privacy Act System Manager, in collaboration with the BLM Senior Management Team, are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in the WHBPS application. These officials and authorized WHBPS personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with BLM Privacy Officer.

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

Responsibility rests with the users of the system and the System Owner, the Assistant Director for Renewable Resources and Planning (WO-200). All users receive system training and all BLM employees and contractors are required to complete periodic Privacy Act training. All federal employees comply with the requirements in OMB Circulars A-123 and A-130 as well as the Departmental Manual, 383 DM 3, Privacy Act – Bureau Responsibilities. The WHBPS Information System Owner and the BLM Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the BLM Privacy Officer.