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
Alaska Science Center Beak Deformity Observations

Bureau/Office
USGS Alaska Science Center

Bureau/Office Contact Title
Research Wildlife Biologist

Point of Contact Email
cmhandel@usgs.gov

First Name
Colleen

M.I.

Last Name
Handel

Phone
(907) 786-7181

Address Line 1
4210 University Dr.

Address Line 2

City
Anchorage

State/Territory
Alaska

Zip
99508

Section 1. General System Information

A. Is a PIA required?

Yes

Yes, information is collected from or maintained on
Members of the general public

B. What is the purpose of the system?

Collect observation reports from the public on birds with deformed beaks.

C. What is the legal authority?

16 U.S.C. 742(a)-742d, 742e-742j-2 Fish and Wildlife Act of 1956 authorizes the Secretary of the Interior to

conduct investigations, prepare and disseminate information, and make periodic reports to the public regarding the availability and abundance and the biological requirements of fish and wildlife resources; provides a comprehensive national fish and wildlife policy and authorizes the Secretary of the Interior to take steps required for the development, management, advancement, conservation, and protection of fisheries and wildlife resources through research, acquisition of refuge lands, development of existing facilities, and other means.

D. Why is this PIA being completed or modified?

Existing Information System under Periodic Review

E. Is this information system registered in CSAM?

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	Describe
N/A	N/A	No	

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)

Interior, USGS-18: Computer Registration System

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

Yes

Describe

TBD - pursuing the process.
1028 - NEW

Section 2. Summary of System Data

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

- [x] Name
- [ ] Citizenship
- [ ] Gender
- [ ] Birth Date
- [ ] Group Affiliation
- [ ] Marital Status
- [ ] Biometrics
- [ ] Other Names Used
- [ ] Truncated SSN
- [ ] Legal Status
- [ ] Place of Birth
- [ ] Other
- [ ] Religious Preference
- [ ] Security Clearance
- [ ] Spouse Information
- [ ] Financial Information
- [ ] Medical Information
- [ ] Disability Information
- [ ] Credit Card Number
- [ ] Law Enforcement
- [ ] Education Information
- [ ] Emergency Contact
- [ ] Driver's License
- [ ] Race/Ethnicity
- [ ] Social Security Number (SSN)
- [ ] Personal Cell Telephone Number
- [ ] Tribal or Other ID Number
- [x] Personal Email Address
- [ ] Mother's Maiden Name
- [x] Home Telephone Number
- [ ] Child or Dependent Information
- [ ] Employment Information
- [ ] Military Status/Service
- [x] Mailing/Home Address

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

☒ Individual ☐ Tribal agency ☐ DOI records ☐ State agency
☐ Federal agency ☐ Local agency ☐ Third party source ☐ Other

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

☐ Paper Format ☐ Face-to-Face Contact ☐ Fax ☐ Telephone Interview
☐ Email ☒ Web Site ☐ Other ☐ Information Shared Between Systems

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

To verify observation reports.

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 or office and how the data will be used.

If scientists need to verify any observations, any of the optional PII data entered are used to contact the individual.

☐ Other Bureaus/Offices
☐ Other Federal Agencies
☐ Tribal, State or Local Agencies
☐ Contractor
☐ Other Third Party Sources

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

Yes

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

Although it's extremely helpful to scientists in verifying information, individuals are not required to enter their PII on the web form.

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

☒ Privacy Act Statement ☒ Privacy Notice ☐ Other ☐ None

Describe each applicable format.

In the USGS Footer, a link to Privacy, with more details are offered.

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

Internally, thru the database's ObservationID.

I. Will reports be produced on individuals?

No

Section 3. Attributes of System Data

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

The website has on-screen email and telephone validation tools.

B. How will data be checked for completeness?

It can be verified by the scientists.

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

This will be updated by the individual, only if they are wanting to update their information.

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

Retention periods will vary somewhat by asset but will be done in accordance with DOI, USGS, and federal requirements and guidelines as outlined in USGS GRDS 432-1-S1, Chapter 400, Item #418-01b and any other applicable laws, rules or regulations.

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

Permanent records are determined by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are needed for the agency's administrative, scientific, legal, or fiscal purposes.

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.

The system and the website are secured thru the use of STIGs and A&A process. All of the developers and SA's have yearly security training to ensure the data will be kept secure. This system is in the DMZ and is protected by firewalls. The web server is configured by USGS STIGs and is scanned monthly, as part of our A&A process.

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

To verify individual observation reports.

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

No

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

No

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

No

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

N/A

F. Are the data or the processes being consolidated?

No, data or processes are not being consolidated

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

☐ Users ☒ Developers ☒ System Administrator

☐ Contractors ☒ Other

Describe

System researchers

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

Internal users via Access control list and managed by what role they play in the system; external users can only report into the database.

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

No

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

Yes

Explanation

System is capturing the name, address, and telephone users for verification by researchers and additional questions.

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

Google Analytics is on all our web pages. However, there is not anything specific to the system to monitor an individual's interaction with a system.

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

Website and backend databases are secured via use of USGS STIGs, virus protection; as well as servers are scanned once a month; ESN intrusion detection.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

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

(3) Administrative Controls. Indicate all that apply.

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

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.

System Owner: Marla Hood and add'l ASC IT staff
Asset Owner: Colleen Handel
Privacy Act Officer: Bill Reilly

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?

System Owner: Marla Hood; Asset Owner: Colleen Handel; Information System Security Officer: Larry Roberts
The Asset owner is directly responsible for assuring proper use of the data in conjunction with the information owner and system administrator, who assists with the technical implementation of the controls.