Appendix A: DI-4001 PIA Form

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.

Name of Project: Contact Information
Bureau/Office: Fish and Wildlife Service
Date: TBD
Point of Contact: Associate Privacy Officer
Name: Jennifer L. Schmidt
Title: Associate Privacy Officer
Email: Jennifer_Schmidt@fws.gov
Phone: 703/358-2291
Address: Falls Church, VA

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 U.S. Fish and Wildlife Service (FWS or the Service) mission is to work with others to conserve, protect and enhance fish, wildlife, and plants and their habitats for the continuing benefit of the American people. To accomplish this mission the Service regularly interacts with members of the public: employees of non-Federal government

agencies such as state or Canadian wildlife federations; representatives from non-profit institutions like museums and universities, and individual hobbyists or wildlife enthusiasts seeking general FWS information; data from a FWS database; partnering with FWS on an initiative or providing coordinated emergency response; or interested in participating in a FWS study or project. As part of these interactions, FWS may collect minimal Personally Identifiable Information (PII); i.e., the contact information necessary to distribute information and perform various administrative tasks. This contact information may be collected and stored by FWS program offices through various means such as an online application or web form, email, voicemail, face-to-face or paper. Any FWS program or project that collects Sensitive PII, such as Social Security number, Date of Birth, or financial or payment information is not covered by this PIA. PIA coverage for projects that collect Sensitive PII will be provided under a system or program-specific PIA. For a list of projects covered by this PIA, please refer to the Appendix. The appendix will be updated as new and similar collections of contact information are identified.

What is the legal authority?

In general, the Service may collect contact information to facilitate communication the public under these authorities:

- 5 U.S.C. § 301 – Departmental regulations
- 16 U.S.C. § 9 – Fish and Wildlife Service
- 44 U.S.C. § 3101 – Records management by agency heads
- 44 U.S.C. § 3501 – Federal Information Policy

Contact information may also be collected as part of Service programs or projects that operate under other specific or derivative authorities. For a digest of all Federal laws under which the Service functions, please see https://www.fws.gov/laws/Lawsdigest.html.

C. 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*

D. Is this information system registered in CSAM?

☐ Yes
☒ No

E. 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

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

☒ Yes: FWS-27 Correspondence Control System, 64 FR 29055, May 28, 1999. This SORN currently is under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108.

Due to the variety of FWS programs that may collect contact information, records containing members of the public's contact information may be covered by other Government-wide or DOI Privacy Act system of records which may be viewed at https://www.doi.gov/privacy/sorn.

☐ No

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

☒ Yes: Due to the variety of FWS programs that collect contact information, records containing members of the public's contact information may be fall under various OMB Control Numbers for DOI or FWS information collections. Program managers must contact the FWS Information Collection Clearance Officer in the Division of Policy, Economics, Risk Management, and Analytics (PERMA) to coordinate the required Paperwork Reduction Act (PRA) review to ensure all collections of contact information are approved as necessary by OMB.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Group Affiliation
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address

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*

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?

Authorized uses of the PII include but are not limited to: to disseminate general information to individuals who have signed up to receive FWS communications; to provide wildlife or conservation data upon request; to arrange the individual's participation in a FWS initiative or study; to notify prior project participants of upcoming opportunities to submit information; and in order to verify information that the individual submitted as a participant in a FWS project.

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

☒ Within the Bureau/Office: Contact information may be shared with FWS personnel, including contractors, who have a need-to-know in the performance of their official

duties.

☒Other Bureaus/Offices: Contact information may be shared with DOI personnel who have a need-to-know in the performance of their official duties.

☒Other Federal Agencies: To enable the agency to respond to an inquiry by an individual to whom an agency record pertains.

☒ Tribal, State or Local Agencies: The appropriate Federal, State, tribal, local or foreign governmental agency that is responsible for investigating, prosecuting, enforcing or implementing a statute, rule, regulation, order or license, when we become aware of an indication of a violation or potential violation of the statute, rule regulation, order or license.

☒Contractor: Authorized contractors hired to work on FWS projects or systems who have a need-to-know may be involved in the collection or handling of contact information from members of the public.

☒ Other Third Party Sources: The appropriate agencies, entities, and persons when the Department determines that there has been a suspected or confirmed breach in order to assist the Department effort's to respond to the breach.

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

☒ Yes: The individual voluntarily provides his or her contact information. If he or she does not provide all the PII requested, FWS may not be able to provide a response or, the individual may not be able to participate in a FWS project.

☐ 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: Privacy Act Statements are included on paper and electronic forms that request PII from individuals and are maintained in a Privacy Act System of Record.

☒ Privacy Notice: FWS webpages contain a hyperlink to FWS's internet privacy policy.

☒ Other: This PIA and SORN-27 provide further notice to individuals.

☐ None

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

Information may be retrieved by the individual's name, project title, date or location.

I. Will reports be produced on individuals?

☐ Yes:

☒ No

Section 3. Attributes of System Data

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

Contact information is provided by the individual directly to the Service.

B. How will data be checked for completeness?

The contact information is collected directly from the individual and is assumed to be complete and accurate. Often web forms and surveys online utilize required fields which prevents the submission of incomplete forms. It is the responsibility of the individual to provide FWS with subsequent updates or any corrections needed.

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

It is the responsibility of the individual to ensure that the contact information they provide is up to date and current.

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

FWS retains the information no longer than is useful for carrying out the information dissemination or collaboration purposes for which it was originally collected. Contact information collected to facilitate communication with the public and related records are generally kept for no more than seven years in accordance with the Department Records Schedule (DRS) DAA-0048-2013-0002, Long-term Administrative Records. Mission-

related records may be categorized under a different, non-administrative schedule. Program managers are encouraged to work with the FWS Records Management Office to identify the official retention period for all records under their purview.

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

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA guidelines and 384 Departmental Manual 1.

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 minimal privacy risk to individuals who voluntarily provide their contact information to FWS for the purposes of facilitating communication. The collection directly involves the respondents. FWS collects the information directly from individuals so they are aware that FWS will maintain their information at least temporarily. FWS collects the minimal amount of information necessary. Individuals receive adequate notices regarding FWS' authority to collect, the authorized uses and permissible disclosures of their information at the time of collection via the hard-copy or electronic form or website. During the PII's use and retention, FWS utilizes appropriate physical, technical and administrative controls to limit access to authorized FWS personnel who have a need-to-know in the performance of their duties. Paper records are kept secure while not in use; electronic files are protected via the FWS' secure network.

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

☐ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

No new data about individuals can be derived from this system.

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.

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

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

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

Access to records in the system is limited to authorized personnel whose job responsibilities require such access, i.e. on a "need to know" basis. Electronic data is protected through user identification, passwords, database permissions and software

controls. Such security measures establish different access levels for different types of users through Role Based Access Controls.

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. Authorized contractors may handle or process PII or other sensitive information as part of their official duties. Contractors complete the same onboarding process as Federal employees and are required to complete annual Information Management and Technology (IMT), Privacy, Records Management, Section 508 Compliance, Controlled Unclassified Information, and the Rules of Behavior, Role Based Security Training and Role Based Privacy Training to maintain network access.

☐ 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

☒ No

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

☐ Yes

☒ 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?

FWS fully complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. Access to audit logs and audit tools are restricted to authorized personnel only via access control lists and authorized access to the project. FWS projects follow the least privilege security principle, such that only the least amount of access is given to a user to complete their job responsibilities.

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 Offsite
☒ 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 FWS Associate Privacy Officer, Information System Security Officer and projects' System Owners and/or Project Managers are responsible for protecting the privacy rights of the public and FWS personnel whose information we maintain. The FWS Associate Privacy Officer and the Privacy Act System Managers are responsible for responding to any complaints or requests for the amendment of records.

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

The Project Manager and/or Information System Owner, the Information System Security Officer and the FWS Associate Privacy Officer are responsible for assuring proper use of personal information. Loss, compromise, unauthorized disclosure or unauthorized access of PII is considered a security incident and is required to be reported to DOI-CIRC within one hour of discovery. The FWS Records Officer is also notified and is responsible for the reporting of record loss or the compromise of records to NARA.

Section 5. Review and Approval

PIAs for Bureau or Office level systems must be signed by the designated Information System Owner, Information System Security Officer, and Bureau Privacy Officer, and approved by the Bureau Assistant Director for Information Resources as the Reviewing Official. Department-wide PIAs must be signed by the designated Information System Owner, Information System Security Officer, and Departmental Privacy Officer, and approved by the DOI Chief Information Officer/Senior Agency Official for Privacy as the Reviewing Official.

Information System Owner

Email: shelley_hartmann@fws.gov
First Name: Shelley Last Name: Hartmann
Title: Deputy Associate Chief Information Officer
Bureau/Agency: FWS Phone: 703-358-2004

Signature: TONY HARTMANN Digitally signed by TONY HARTMANN Date: 2019.12.16 14:24:47 -05'00'

Information System Security Officer

Email: jay_mcmaster@fws.gov

First Name: Jay Last Name: McMaster
Title: Associate Chief Information Security Officer
Bureau/Agency: FWS Phone: 703-358-2133

Signature: JAY MCMASTER Digitally signed by JAY MCMASTER Date: 2020.01.09 11:03:43 -05'00'

Privacy Officer

Email: jennifer_schmidt@fws.gov
First Name: Jennifer Last Name: Schmidt
Title: Associate Privacy Officer
Bureau/Agency: FWS Phone: 703-358-2291

Signature: JENNIFER SCHMIDT Digitally signed by JENNIFER SCHMIDT Date: 2019.11.26 14:17:14 -05'00'

Reviewing Official

Email: paul_gibson@fws.gov
First Name: Paul Last Name: Gibson
Title: Associate Chief Information Officer
Bureau/Agency: FWS Phone: 703-358-2636

Signature: PAUL GIBSON Digitally signed by PAUL GIBSON Date: 2020.01.10 14:31:50 -05'00'

Appendix

Preliminary Aerial Waterfowl Observer Training System

FWS Migratory Bird program hosts a website at https://www.fws.gov/waterfowlsurveys/welcome.jsp for training and testing biologists and volunteers to perform aerial waterfowl surveys by improving inflight species classification and counting. The system is used to train biologists to identify waterfowl to species and count flocks of birds from an aircraft. The system collects FWS employees and members of the public's name, work email address and work phone number. The PII is used to track the training and accuracy of each observer that participates in FWS surveys in order to increase the quality of data used to support management decisions.

Federal Employee Viewpoint Survey (FEVS) for Non-permanent FWS employees

The personal email address that FWS short-term personnel (volunteers, interns, etc.) provides during the onboarding procedures is used to send them the FWS Non-Permanent Employee FEVS Survey when their summer employment is over and the individual is no longer working for FWS. Data from this survey will be used to generate summary statistics on non-permanent employees' workplace satisfaction at the regional (if number of responses reaches a minimum threshold to ensure anonymity) and national level.

Endangered and Threatened Wildlife, Experimental Populations

FWS collects information regarding experimental populations listed in 50 CFR 17.84 to help further recovery of the species and to assess the success of the reintroduced populations. Respondents are members of the public who notify FWS when an incident occurs and provide information related to the incident (species involved, location, and circumstance description, etc.) as well as his or her name, mailing address and phone number. The PII is used by FWS when necessary to verify or collect further information about the incident.

Lake Sturgeon Sightings

FWS collects information regarding sightings of Lake Sturgeon from members of the public. Individuals voluntarily provide their name, mailing address and email address; FWS uses this contact information to contact respondents when necessary to verify or confirm sighting details.

Ridgefield NWRC Use of Information Collection 1018-0140

This information collection allows members of the public to enter a lottery to participate in hunting and fishing programs that assist in the management of wildlife and their habitats at FWS' National Wildlife Refuges. Individuals voluntarily provide their name, mailing address, phone number and email address in order that the sponsoring Refuge may notify the applicant of

his or her selection as well as to follow up afterwards to learn of his or her hunting/fishing experience.

Oral History Project

The USFWS National Conservation Training Center (NCTC) partners with the FWS Retirees Association, through the FWS-chartered Heritage Committee, to coordinate the Service's oral history program. The Committee is comprised of FWS employees and retirees who volunteer to conduct oral histories with FWS retirees who consent to be interviewed and have their stories made available to the public at https://training.fws.gov/history/OralHistories.html.

Annual Teen Environmental Art Show

The San Francisco Bay National Wildlife Refuge sponsors an annual art exhibit for teens at the Refuge's Environmental Education Center. The Refuge collects the name, address, phone number and email address of young artists, as well as the parent's or guardian's consent, to the display of the artists' name and artworks and coordinate logistics for the show.

Sea Lamprey Control Program Database

The Service maintains a database of information critical to the management of invasive sea lamprey populations in the five Great Lakes. It maintains contact information of land owners in affected areas so that the Service can coordinate with them accessing the property and treating the water as necessary.