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.

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: Information Collection 1018-0094 (Under OMB's Paperwork Reduction Act)

Date: October 23, 2017

Bureau/Office: U.S. Fish and Wildlife Service (FWS), Ecological Services

Bureau/Office Contact Title: Biologist, National ESA Recovery Permits Coordinator, ES SPITS Liaison

Point of Contact
Email: Amy_Brisendine@fws.gov
First Name: Amy
M.I.: E
Last Name: Brisendine
Phone: 703-358-2005
Address Line 1: 5275 Leesburg Pike
Address Line 2:
City: Falls Church
State/Territory: VA
Zip: 22041

Section 1. General System Information

A. Is a full PIA required?

This is a threshold question. Indicate whether the system collects, maintains, uses or disseminates information about members of the general public, Federal employees, contractors, or volunteers. If the system does not contain any information that is identifiable to individual (e.g., statistical, geographic, financial), complete all questions in this section and obtain approval and required signatures in Section 5. The entire PIA must be completed for systems

that contain information identifiable to individuals, including employees, contractors and volunteers.

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

Note: There are two ways that information is maintained currently under this information collection. In some cases, the Regional Offices receive and maintain paper copies of applications, see https://www.fws.gov/forms/display.cfm?number1=200 (forms 3-200-54, 55, and 56 for copies of these applications). Reports associated with those application forms are also submitted; some of them may be submitted via email to the Regional permit staff member rather than be submitted via paper copies.

Some of this information is maintained in the FWS Permitting System "SPITS". For the information maintained in SPITS, refer to the SPITS System Security Plan or the SPITS PIA.

☐ 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?

Describe the purpose of the system and how it relates to the program office's and Department's mission. Include the context and background necessary to understand the purpose, the name of the program office and the technology, project or collection being assessed.

This information collection is associated with applications for permits issued under Section 10 of the Endangered Species Act (16 U.S.C. 1531 et seq.) (ESA) and the associated reporting as the result of an issued permit. We use the information we collect through permit applications and the associated reports to determine the eligibility of applicants for permits requested in accordance with the ESA and their compliance with these permits. FWS regulations implementing this Statute are in chapter I, subchapter B of title 50 of the Code of Federal Regulations (CFR). These regulations stipulate general and specific requirements that when met allow the Service to issue permits to authorize activities that are otherwise prohibited. This information collection includes the following permit application forms and reporting requirements associated with these application forms.

The applications are:
- FWS Form 3–200–54 (Enhancement of Survival Permits Associated with Safe Harbor Agreements and Candidate Conservation Agreements with Assurances).
- FWS Form 3–200–55 (Scientific Purposes, Enhancement of Propagation or Survival Permits (i.e., Recovery Permits) and Interstate Commerce Permits).
- FWS Form 3–200–56 (Incidental Take Permits Associated with a Habitat Conservation Plan).

C. What is the legal authority?

A Federal law, Executive Order of the President (EO), or DOI requirement must authorize the collection and maintenance of a system of records. For Privacy Act systems, the response should reflect the information provided in the authority section of the Privacy Act system of records notice.

- 16 U.S.C. 1531 et seq.
- 50 CFR 13, 50 CFR 17
- the Bald and Golden Eagle Protection Act (16 U.S.C. 668), 50 CFR 22
- the Endangered Species Act (16 U.S.C. 1531-1544), 50 CFR 17
- the Migratory Bird Treaty Act (16 U.S.C. 703-712), 50 CFR 21
- the Marine Mammal Protection Act (16 U.S.C. 1361, et seq.), 50 CFR 18
- the Wild Bird Conservation Act (16 U.S.C. 4901-4916), 50 CFR 15
- the Lacey Act: Injurious Wildlife (18 U.S.C. 42), 50 CFR 16
- Convention on International Trade in Endangered Species of Wild Fauna and Flora (TIAS 8249), 50 CFR 23
- General Provisions, 50 CFR 10; General Permit Procedures, 50 CFR 13
- Wildlife Provisions (Import/export/transport), 50 CFR 14

D. Why is this PIA being completed or modified?

Indicate why the PIA is being conducted. For example, the system is being significantly modified or two systems are being merged together.

☐ 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: Renewal of existing system and addition of information collection reporting forms associated with permits for activities with endangered and threatened species under Section 10 of the ESA.

E. Is this information system registered in CSAM?

The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name* UUI Code: 010-000000465, SSP Name: FWS System Security Plan (SSP) for Service Permit Issuance and Tracking System, dated July 12, 2017.

☐No

Appendix A – DI-4001 PIA Form

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

Enter "None" if no subsystems or applications are hosted. For General Support Systems (GSS) be sure to include all hosted major applications, minor applications, or other subsystems, and describe the purposes and types of PII if any. Privacy risks must be identified and adequately addressed for each hosted application or subsystem identified in the GSS PIA. A separate PIA should be conducted for each hosted application or subsystem that contains PII to ensure privacy implications are assessed. In any case, the GSS PIA must identify all hosted applications, describe the relationship, and reference or append the PIAs conducted for the hosted applications. The GSS PIA and associated PIAs must be reviewed and approved by all officials as appropriate; and all related PIAs, SORNs and supporting artifacts must be entered into CSAM.

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

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

A Privacy Act SORN is required if the information system or electronic collection contains information about individuals that is retrieved by name or other unique identifier. Provide the DOI or Government-wide Privacy Act SORN identifier and ensure it is entered in CSAM for this system. For new SORNS being developed, select "Yes" and provide a detailed explanation. Contact your Bureau Privacy Officer for assistance identifying the appropriate Privacy Act SORN(s).

☒ Yes: *List Privacy Act SORN Identifier(s)* Permits System, FWS-21
☐ No

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

The Paperwork Reduction Act requires an OMB Control Number for certain collections of information from ten or more members of the public. If information is collected from members of the public, contact your Bureau Information Collection Clearance Officer for assistance to determine whether you need to obtain OMB approval. Please include all OMB Control Numbers and Expiration Dates that are applicable.

☒ Yes: *Describe* OMB Collection Number 1018-0094
☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.
Identify all the categories of PII that will be collected, stored, used, maintained or disseminated. Describe any additional categories of PII not already indicated, as well as any new information that is created (for example, an analysis or report), and describe how this is done and the purpose of that information.

☒ Name
☐ Citizenship
☐ Gender
☒ Birth Date
☒ Group Affiliation
☐ Marital Status
☐ Biometrics
☐ Other Names Used
☐ Truncated SSN
☐ Legal Status
☐ Place of Birth
☐ Religious Preference
☐ Security Clearance
☐ Spouse Information
☐ Financial Information
☐ Medical Information
☐ Disability Information
☐ Other: *Specify the PII collected.*

☐ 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
☒ Personal Email Address
☐ Mother's Maiden Name
☒ Home Telephone Number
☐ Child or Dependent Information
☐ Employment Information
☐ Military Status/Service
☒ Mailing/Home Address

B. What is the source for the PII collected? Indicate all that apply.
Include all sources of PII collected. For example, information may be collected directly from an individual through a written form, website collection, or through interviews over the phone or in person. Information may also come from agency officials and employees, agency records, from a computer readable extract from another system, or may be created within the system itself. If information is being collected through an interface with other systems, commercial data aggregators, or other agencies, list the source(s) and explain why information from sources other than the individual is required.

☒ 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.

Indicate all the formats or methods for collecting PII that will be used. If the system receives information from another system, such as a transfer of financial information or response to a background check, describe the system from which the information originates, how the information is used, and how the systems interface.

☒ 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?

Describe the intended uses of the PII collected and maintained in the system and provide a detailed explanation on how the data will be used. The intended uses must be relevant to the purpose of the system; for Privacy Act systems, uses must be consistent with the published system of records notice.

The information collected is to establish and verify an applicant's eligibility for a permit to conduct activities with protected wildlife and plants under the ESA. It will also be used to provide the public and permittees with permit-related information; to monitor and track applications, permits and associated reports as required under the ESA and the associated regulations and to monitor the permitted activities.

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

Indicate all the parties, both internal and external to DOI, with whom PII will be shared. Identify other DOI offices with assigned roles and responsibilities within the system, or with whom information is shared, and describe how and why information is shared. Also, identify other federal, state and local government agencies, private sector entities, contractors or other external third parties with whom information is shared; and describe any routine information sharing conducted with these external agencies or parties, and how such external sharing is compatible with the original purpose of the collection of the information. If sharing is pursuant to a Computer Matching Agreement, provide an explanation. For Privacy Act systems, describe how an accounting for the disclosure is maintained.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*
Within FWS; users of SPITS will include biologists, permit program managers, system managers, attorneys, and other employees of the U.S. Fish and Wildlife Service who have a need to know the information contained in the system to carry out their duties, in accordance with Privacy Act requirements.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*
There may be a need to share information, in accordance with Privacy Act requirements, with other bureaus/offices for the purpose of obtaining scientific, management, and legal advice relevant to making a decision on an application for a permit.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*
There may be a need to share information, in accordance with Privacy Act requirements, with other federal agencies for the purpose of obtaining scientific, management, and legal advice relevant to making a decision on an application for a permit. As outlined in the Privacy Act System of Records, disclosures outside the DOI may be made under the routine uses without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected.

There may be a need to share information, in accordance with Privacy Act requirements, to provide addresses obtained from the Internal Revenue Service to debt collection agencies for purposes of locating a debtor to collect or compromise a Federal claim against the debtor, or to consumer reporting agencies to prepare a commercial credit report for use by the DOI.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*
There may be a need to share information, in accordance with Privacy Act requirements, with Tribal, State or Local Agencies for the purpose of obtaining scientific, management, and legal advice relevant to making a decision on an application for a permit. As outlined in the Privacy Act System of Records, disclosures outside the DOI may be made under the routine uses without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected.

☒ Contractor: *Describe the contractor and how the data will be used.*
There may be a need to share information, in accordance with Privacy Act requirements, with contractors, experts, or consultants employed by the FWS when necessary to accomplish a FWS function related to this system of records.

☒ Other Third Party Sources *Describe the third party source and how the data will be used.*
There may be a need to share information, in accordance with Privacy Act requirements, with congressional offices in response to an inquiry to the office by the individual to whom the record pertains; with the General Accounting Office or Congress when the information is required for the evaluation of the permit programs.

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

If "Yes," describe the method by which individuals can decline to provide information or how individuals consent to specific uses. If "No," state the reason why individuals cannot object or why individuals cannot give or withhold their consent.

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

Required application fields are identified.

A Privacy Act Statement is posted on each form. By signing the application, an applicant acknowledges that they have either read or are familiar with the associated information, to include the associated consent. This is the responsibility of the applicant.

The on-line application provides a hyperlink to the site's privacy policy. Continuing with the application process, an applicant acknowledges that they have either read or are familiar with the associated information, to include the associated consent. This is the responsibility of the applicant. Submission of requested information is required in order to process applications for permits authorized under the laws, treaties, and regulations identified on the form. Failure to provide all requested information may be sufficient cause for the U.S. Fish and Wildlife Service to deny the request. All information collections have valid Office of Management and Budget (OMB) control numbers displayed.

☐ 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.

Describe how notice is provided to the individual about the information collected, the right to consent to uses of the information, and the right to decline to provide information. For example, privacy notice to individuals may include Privacy Act Statements, posted Privacy Notices, privacy policy, and published SORNs and PIAs. Describe each format used and, if possible, provide a copy of the Privacy Act Statement, Privacy Notice, or a link to the applicable privacy policy, procedure, PIA or referenced SORN Federal Register citation (e.g., XX FR XXXX, Date) for review. Also describe any Privacy Act exemptions that may apply and reference the Final Rule published in the Code of Federal Regulations (43 CFR Part 2).

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

The following Privacy Act Statement is posted on both paper and electronic forms:

Privacy Act Statement

Authority: The information requested is authorized by the following: the Bald and Golden Eagle Protection Act (16 U.S.C. 668), 50 CFR 22; the Endangered Species Act (16 U.S.C. 1531-1544), 50 CFR 17; the Migratory Bird Treaty Act (16 U.S.C. 703-712), 50 CFR 21; the Marine Mammal Protection Act (16 U.S.C. 1361, et seq.), 50 CFR 18; the Wild Bird Conservation Act (16 U.S.C. 4901-4916), 50 CFR 15; the Lacey Act: Injurious Wildlife (18 U.S.C. 42), 50 CFR 16; Convention on International Trade in Endangered Species of Wild Fauna and Flora (TIAS 8249), 50 CFR 23; General Provisions, 50 CFR 10; General Permit Procedures, 50 CFR 13; and Wildlife Provisions (Import/export/transport), 50 CFR 14.

Purpose: The collection of contact information is to verify the individual has an eligible permit to conduct activities which affect protected species. This helps FWS monitor and report on protected species and assess the impact of permitted activities on the conservation and management of species and their habitats.

Routine Uses: The collected information may be used to verify an applicant's eligibility for a permit to conduct activities with protected wildlife; to provide the public and the permittees with permit related information; to monitor activities under a permit; to analyze data and produce reports to monitor the use of protected wildlife; to assess the impact of permitted activities on the conservation and management of protected species and their habitats; and to evaluate the effectiveness of the permit programs. More information about routine uses can be found in the System of Records Notice, Permits System, FWS-21.

Disclosure: The information requested in this form is voluntary. However, submission of requested information is required to process applications for permits authorized under the listed authorities. Failure to provide the requested information may be sufficient cause for the U.S. Fish & Wildlife Service to deny the request.

☐ Privacy Notice: *Describe each applicable format.*

☐ 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.).
Describe how data is retrieved from the system. For example, is data retrieved manually or via reports generated automatically? Are specific retrieval identifiers used or does the system use key word searches? Be sure to list the identifiers that will be used to retrieve data (e.g., name, case number, Tribal Identification Number, subject matter, date, etc.).

Data will be retrieved via the following identifiers:

(a) Permit number; and
(b) Applicant information
Electronic records may be searched on or retrieved by any data field. The method of retrieval is dependent upon the report or purpose of usage and whether a need to know exists. Records are retrieved for several purposes, such as processing a permit application, verifying an individual has a permit to conduct an activity with a protected species, and tracking whether permit reports have been submitted.

I. Will reports be produced on individuals?
Indicate whether reports will be produced on individuals. Provide an explanation on the purpose of the reports generated, how the reports will be used, what data will be included in the reports, who the reports will be shared with, and who will have access to the reports. Many systems have features that allow reports to be generated on data in the system or on user actions within the system.

☒ Yes: *What will be the use of these reports? Who will have access to them?*
Yes. SPITS collects the following information that is identifiable to the individual (if they apply as an individual rather than a business/government agency): Full name, current address, date of birth, telephone number, email address (optional, unless applying online), country, county, province (if applicable), and qualifications of the applicant (such as education or experience provided to support an applicant's ability to conduct a requested activity). Records include documents that reflect (1) the general administrative processing of the application and permit; (2) public review required by certain laws, including comments received; (3) our consultation with subject matter experts, including but not limited to experts within the FWS and in State, Federal, local, and foreign agencies, if applicable, for the purpose of obtaining scientific, management, and legal advice; (4) our evaluation of information to make a decision on an application for a permit, and to monitor activities that occur under the permit; (5) occupation; (6) location, types, purpose of proposed activity; and (7) reports of activities conducted under an issued permit.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?
Data accuracy and reliability are important requirements in implementing the Privacy Act which requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. The information has to have some form of verification for accuracy due to the Privacy Act provisions that require that only relevant and accurate records should be collected and maintained about individuals.

Data is collected from the individual; it is not collected from any other source.

B. How will data be checked for completeness?
Describe the procedures to ensure data is checked for completeness. To the extent practical, PII should be checked for completeness to ensure accuracy within the context of the use of the data.

Applicants (individuals and businesses) are required to maintain up-to-date information for the life of the permit. Applicants are also required to verify and update their profile when applying for new or additional permits. The information is received from individual permit applicants and is only as reliable and current as that provided by the applicant.

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

Describe the steps or procedures taken to ensure the data is current and not out-of-date. Where are they documented? For example, are they outlined in standard operating procedures or data models? Data that is not current also affects the relevancy and accuracy of the data. This is particularly true with data warehousing. A data warehouse is a repository of an organization's electronically stored data and is designed to facilitate reporting and analysis. A data warehouse may contain data that is not current which would cause a domino effect throughout the data stores.

Applicants (individuals and businesses) are required to maintain up-to-date information for the life of the permit. Applicants are also required to verify and update their profile when applying for new or additional permits. The information is received from individual permit applicants and is only as reliable and current as that provided by the applicant.

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

Identify all applicable records retention schedules or explain at what development stage the proposed records retention schedule is in. Information system owners must consult with Bureau/Office Records Officers early in the development process to ensure that appropriate retention and destruction schedules are identified, or to develop a records retention schedule for the records contained in the information system. Be sure to include applicable records retention schedules for different types of information or subsets of information and describe if subsets of information are deleted and how they are deleted.

The retention periods of data/records in the system are covered by FWS Records Schedule PERM 201, Permit Tracking Database (N1-022-05-01/108).

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

Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This may be obtained from records retention schedules, the Departmental Manual, bureau/office records management policies, or standard operating procedures.

Procedures for the disposition of data are in accordance with disposal procedures identified in Federal NARA statutes, including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33), NARA regulations (36 CFR Chapter XII Subchapter B), the Departmental Manual (385 DM8.8), FWS guidance: Records Management Part Electronic Records, 282 FW 4, Electronic Records and 283 FW 1, Records Management; Records Disposition, and IRM Bulletin No 1001-004.

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.
Describe and analyze the major potential privacy risks identified and discuss the overall impact on the privacy of employees or individuals. Include a description of how the program office has taken steps to protect individual privacy and mitigate the privacy risks. Provide an example of how information is handled at each stage of the information life cycle. Also discuss privacy risks associated with the sharing of information outside of the Department and how those risks were mitigated. Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department.

In accordance with OMB Circulars A-123, and A-130 Appendix III, the data in this collection will have controls in place to prevent the potential misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, database permissions and software controls. Each user is required to complete the annual Information Management and Technology (IMT) Awareness Training, in addition to the Role Based Privacy Training (RBPT) for those with additional privacy responsibilities.

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?
Describe how the use of the system or information collection relates to the purpose of the underlying mission of the organization. Is the information directly relevant and necessary to accomplish the specific purposes of the system? For Privacy Act systems, the Privacy Act at 5 U.S.C. 552a(e)(1) requires that each agency shall maintain in its records only such information about an individual that is relevant and necessary to accomplish an agency purpose required by statute or by executive order of the President.

☒ Yes: *Explanation* The information collected is to establish and verify an applicant's eligibility for a permit to conduct activities under Section 10 of the ESA.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?
Does the technology create new data or conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? Is data aggregated in a way that will permit system users to easily draw new conclusions or inferences about an individual? Electronic systems can sift through large amounts of information in response to user inquiry or programmed functions, or perform complex analytical tasks resulting in other types of data, matching, relational or pattern analysis, or reporting. Discuss the results generated by

these uses and include an explanation on how the results are generated, whether by the information system or manually by authorized personnel. Explain the purpose and what will be done with the newly derived data. Derived data is obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information to form additional information that is usually different from the original source information. Aggregation of data is the taking of various data elements and turning it into a composite of all the data to form another type of data, e.g., tables or data arrays.

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

☒ No

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

Will the results or new data be placed in individuals' records? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☒ No

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

Will the new data be used to make determinations about individuals or will it have any other effect on the subject individuals? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☒ No

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

Explain how accuracy of the new data is ensured. Describe the process used for checking accuracy. Also explain why the system does not check for accuracy. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.

No new data is derived from this system.

F. Are the data or the processes being consolidated?

If the data is being consolidated, that is, combined or united into one system, application, or process, then the existing controls should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not inappropriately accessed or used by unauthorized

individuals. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of identification and authentication that is a technical measure that prevents unauthorized people or processes from accessing data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.

☐ 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.
Describe the process by which an individual receives access to the information within the system. Explain what roles these individuals have and their level of access. If remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication). Do users have "read-only" access or are they authorized to make changes in the system? Also consider "other" users who may not be as obvious, such as the GAO or the Inspector General, database administrators, website administrators or system administrators. Also include those listed in the Privacy Act system of records notice under the "Routine Uses" section when a Privacy Act system of records notice is required.

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

Users of the system (paper and electronic records) will include biologists, permit program managers, system managers, attorneys, and other employees of the U.S. Fish and Wildlife Service who have a need to know the information contained in the system to carry out their duties. The System Administrator and Programmer will have access to the data in the system to carry out their responsibilities. Other parties where data may be shared with are outlined in the Permits System of Records Notice, FWS-21. Disclosures outside the DOI may be made under the routine uses without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected.

1) To subject matter experts, including but not limited to experts in State, Federal, local, and foreign agencies, for the purpose of obtaining scientific, management, and legal advice relevant to making a decision on an application for a permit.
2) To the public as a result of publishing **Federal Register** notices announcing the receipt of permit applications for public comment or notice of the decision on a permit application;

(however, redactions in accordance with the Privacy Act will be made prior to providing any information to the public).

3) To Federal, State, local or foreign wildlife and plant agencies for the exchange of information on permits granted or denied to assure compliance with all applicable permitting requirements.
4) To Captive-bred Wildlife registrants under the Endangered Species Act for the exchange of captive-born, non-native endangered and threatened species, and to share information on new developments and techniques of captive breeding of these protected species.
5) To Federal, State, and local authorities who need to know who is permitted to receive and rehabilitate sick, orphaned, and injured birds under the Migratory Bird Treaty Act and the Bald and Golden Eagle Protection Act; federally permitted rehabilitators; individuals seeking a permitted rehabilitator with whom to place a sick, injured, or orphaned bird in need of care; and licensed veterinarians who receive, treat, or diagnose sick, orphaned, and injured birds;
6) To the Department of Justice (DOJ), or a court, adjudicative, or other administrative body or to a party in litigation before a court or adjudicative or administrative body, when:
   a) One of the following is a party to the proceeding or has an interest in the proceeding:
      (i) The DOI or any component of the DOI;
      (ii) Any DOI employee acting in his or her official capacity;
      (iii) Any DOI employee acting in his or her individual capacity where the DOI or DOJ has agreed to represent the employee; or
      (iv) The United States, when DOI determines that DOI is likely to be affected by the proceeding; and
   b) The DOI deems the disclosure to be:
      (i) Relevant and necessary to the proceedings; and
      (ii) Compatible with the purpose for which we compiled the information.
7) To 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, or when we need to monitor activities conducted under a permit or evaluate regulated wildlife and plant trade and use.
8) To a congressional office in response to an inquiry to the office by the individual to whom the record pertains.
9) To the General Accounting Office or Congress when the information is required for the evaluation of the permit programs.
10) To a contractor, expert, or consultant employed by the FWS when necessary to accomplish a FWS function related to this system of records.
11) To provide addresses obtained from the Internal Revenue Service to debt collection agencies for purposes of locating a debtor to collect or compromise a Federal claim against the debtor or to consumer reporting agencies to prepare a commercial credit report for use by the DOI.

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

Users are normally only given access to certain data on a "need-to-know" basis for information that is needed to perform an official function. Care should be given to avoid "open systems" where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system or application. However, access should be restricted when users may not need to have access to all the data. For more guidance on this, refer to the Federal Information Processing Standards [FIPS] Publications in the authorities section. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of applying logical access controls, which are system-based means by which the ability is explicitly enabled or restricted. It is the responsibility of information system owners to ensure no unauthorized access is occurring.

Access to the data is determined by the official role the individual is filling as determined by that individual's supervisor, coupled with a demonstrated need-to-know in accordance with 375 DM 19. The system manager has read and understands the Department's guidance as identified. All staff using the permit database are required to log out of the password protected file server and computer at the end of the day. The system has a log on disclaimer on the use of records.

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 required Privacy Act clauses 52.224.1 and 52.224.2 were included in their contracts.

☐ No

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

Are there new technologies used to monitor activities of the individual in any way? Access logs may already be used to track the actions of users of a system. Describe any new software being used, such as keystroke monitoring.

☐ Yes. *Explanation*

☒ No

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

Most systems now provide the capability to identify and monitor individual's actions in a system (e.g., audit trail systems/ applications). For example, audit logs may record username, time and date of logon, files accessed, or other user actions. Check system security procedures for information to respond to this question.

☒ Yes. *Explanation*

SPITS is able to identify and monitor SPITS account users through its audit logs. The SPITS AU-02(3) control states the following, "SPITS maintains an internal audit log. The log records login time, end time, IP address, program module, and account name. Developer uses Microsoft SQL Server Log to monitor database activities daily. Developer also uses Windows Operating system Event logs to monitor access daily. SPITS logon process allows 5 failed attempts. After that Program Coordinator must reset the locked account. SPITS automatically de-activates accounts that have had no activity in the last 60 days. An email is generated and sent to the Program Coordinator."

☐ No

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

The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) detail how audit logs should be used for DOI systems. Provide what audit activities are maintained to record system and user activity including invalid logon attempts and access to data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication of users to the system. Examples of information collected may include username, logon date, number of failed logon attempts, files accessed, and other user actions on the system.

SPITS audit logs capture and collect Login time, end time, IP address, program module used, account name, and number of failed login attempts.

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

Certain laws and regulations require monitoring for authorized reasons by authorized employees. Describe the controls in place to ensure that only authorized personnel can monitor use of the system. For example, business rules, internal instructions, posting Privacy Act Warning Notices address access controls, in addition to audit logs and least privileges. It is the responsibility of information system owners and system managers to ensure no unauthorized monitoring is occurring.

The principle of least privilege, log monitoring, administrative account control, effective account access controls (including account provisioning, account review, and account removal) are all used to prevent unauthorized monitoring.

N. How will the PII be secured?

Discuss how each privacy risk identified was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. Describe auditing features, access controls, and other possible technical and policy safeguards such as information sharing protocols, or special access restrictions. Do the audit features include the ability to identify specific records each user can access? How is the system audited? For example, does the system perform self audits, or is the system subject to third party audits or reviews by the Office of Inspector General or Government Accountability Office (GAO). Does the IT system have automated tools to indicate when information is inappropriately accessed,

retrieved or misused? Describe what privacy and security training is provided to system users. Examples of controls include rules of behavior, encryption, secured facilities, firewalls, etc.

(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.

Although all employees who have access to information in a Privacy Act system have responsibility for protecting and safeguarding that information, often the information system owner and Privacy Act system manager share the responsibility for protecting the privacy rights of employees and the public. For Privacy Act responsibilities refer to 383 Department Manual Chapters 1-13 and DOI Privacy Act regulations at 43 CFR Part 2. Also, describe how Privacy Act complaints and requests for redress or amendment of records are addressed.

The FWS Privacy Officer, in conjunction with the 1018-0094 collection coordinators, are responsible for protecting the privacy rights of employees. The FWS Associate Privacy Officer receives complaints and request 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?

This may be the information system owner and Privacy Act system manager, or may be another individual with designated responsibility, or otherwise stipulated by contract or in language contained in an agreement (e.g., Head of the Bureau or Program Manager). There may be multiple responsible officials. Consider a system that contains several databases from different program offices; there may be one information system owner and several Privacy Act system managers. Also, describe who is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information.

The Information System Owner and Privacy Officer are responsible for assuring proper use of employee data. Loss, compromise, unauthorized disclosure or unauthorized access of PII is considered a “security incident” that must be reported to DOI-CIRC within one hour of discovery.

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: amy_brisendine@fws.gov
First Name: Amy Last Name: Brisendine Title: Biologist
Bureau/Agency: U.S. Fish & Wildlife Service Phone: 703-358-2005

Signature: Amy Brisendine

Information System Security Officer

Email: philip_olson@fws.gov
First Name: Philip Last Name: Olson Title: SPITS ISSO
Bureau/Agency: U.S. Fish & Wildlife Service Phone: 303-275-2366

Signature: PHILIP OLSON Digitally signed by PHILIP OLSON
Date: 2017.10.31 08:02:35 -06'00'

Privacy Officer

Email: katherine_gonyea@fws.gov
First Name: Katherine Last Name: Gonyea Title: Acting, Privacy Officer
Bureau/Agency: U.S. Fish & Wildlife Service Phone: 703-358-2244

Signature: KATHERINE GONYEA Digitally signed by KATHERINE GONYEA
Date: 2017.10.31 11:18:31 -04'00'

Reviewing Official

Email: kenneth_taylor@fws.gov
First Name: Kenneth Last Name: Taylor Title: Assistant Director of Information Resources
Bureau/Agency: U.S. Fish & Wildlife Service Phone: 703-358-1968

Signature: KENNETH TAYLOR Digitally signed by KENNETH TAYLOR
Date: 2017.11.16 10:19:11 -05'00'