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: Online Permits
Bureau/Office: U.S. Fish and Wildlife Service (FWS)
Date: May 21, 2020
Point of Contact:
Name: Jennifer L. Schmidt
Title: Associate Privacy Officer
Email: FWS_Privacy @fws.gov
Phone: (703) 358-2291
Address: 5275 Leesburg Pike, MS: IRTM Falls Church, VA 22041-3803

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?

Online Permits, available at https://epermits.fws.gov, allows individuals and businesses to submit, pay and process FWS permit applications either through the online interface with Pay.gov. Pay.gov is operated by the U.S. Department of Treasury and you may find Pay.gov' s PIA on their website at https://fiscal.treasury.gov /files/pia/pay.gov-pclia .pdf. Applicants may opt to download the appropriate application from the FWS public forms website at https://www.fws.gov/forms/ and submit it through standard mail. FWS uses Online Permits to

issue and track permits and to query species and permit applicant/holder data for both domestic and international permits. The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) is the only treaty to ensure that international trade in plants and animals does not threaten their survival in the wild. A State or country that has agreed to implement the Convention is called a Party to CITES. Currently there are 183 Parties. They include 182 member countries and the European Union. More information about CITES is available at https://www.fws.gov/international/cites/.

FWS' original permitting system, the Service Permit Issuance and Tracking System (SPITS), maintains historical permit and permit applicant/holder data and is used by FWS personnel in conjunction with Online Permits. However, SPITS will be decommissioned and Online Permits replaced with one comprehensive permitting workflow system starting in September 2020. This PIA covers the current iteration of FWS' permitting system (Online Permits and SPITS) while the new system is developed. A new PIA will be conducted on " FWS ePermits" before its phased roll-out is expected to be complete in July 2021.

FWS is charged with issuing permits under various wildlife laws and treaties. Permits enable the public to engage in legitimate wild-life related activities that would otherwise be prohibited by law. FWS permit programs ensure that such activities are carried out in a manner that safeguards wildlife. Some permits promote conservation efforts by authorizing scientific research, generating data, or allowing wildlife management and rehabilitation activities.

C. What is the legal authority?

- Bald and Golden Eagle Protection Act (16 U.S.C. 668), Title 50, Part 22, of the Code of Federal Regulations (50 CFR Part 22)
- Endangered Species Act of 1973 (16 U.S.C. 1531-1544), (50 CFRPart 17)
- Migratory Bird Treaty Act (16 U.S.C. 703-712), (50 CFR Part 21)
- Marine Mammal Protection Act of 1972 (16 U.S.C. 1361 et seq.), (50 CFR Part18)
- Wild Bird Conservation Act (16 U.S.C. 4901-4916), (50 CFR Part 15)
- Lacey Act (18 U.S.C. 42); Injurious Wildlife, (50 CFR Part 16)
- Convention on International Trade in Endangered Species of Wild Flora and Fauna (CITES) (TIAS 8249); (50 CFR Part 23)
- General Provisions, (50 CFR Part 10)
- General Permit Procedures, (50 CFR Part 13)
- Importation,Exportation and Transportation of Wildlife, (50 CFR Part 14)
- Seizure and Forfeiture Procedures, (50 CFR Part 12)
- Migratory Bird Hunting, (50 CFR Part 20)

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*

010-000000465; Service Permit Issuance and Tracking System SSP

☐ 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.			

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/FWS-21, Permits System (June 4, 2008) 73 FR 31877. This system is exempt from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552aG)(2). *See* 40 FR 37217. This SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with 0MB Circular A-108.

INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) (March 12, 2007) 72 FR 11040.

☐ No

H. Does this information system or electronic collection require an 0MB Control Number?

☒ Yes: *Describe*

OMB Control No. 1018-0022 (expires 4/30/2021) Federal Fish and Wildlife Permit Application and Reports--Migratory Birds, 50 CFR 10, 13, 20, 21

OMB Control No. 1018-0167 (currently pending reinstatement at OMB) Eagle Take Permits an Fees, 50 CFR 22

OMB Control No. 1018-0093 (expires 8/31/2020) Federal Fish and Wildlife Permit Application and Reports--Management Authority, 50 CFR 12, 13, 14, 15, 16, 17, 18, 21, 23

OMB Control No. 1018-0094 (expires 3/31/2021) Federal Fish and Wildlife Permit Application and Reports - Native Endangered and Threatened Species, 50 CFR 10, 13, and 17

OMB Control No. 1018-0146 (expires 1/31/2021) Depredation Orders, 50 CFR 21.43 and 50 CFR 21.46

OMB Control No. 1018-0103, (currently pending merge with 1018-0146 at 0MB) Conservation Order for Light Geese, 50 CFR 21.60

OMB Control No. 1018-0133, (currently pending merge with 1018-0146 at 0MB) Control and Management of Canada Geese, 50 CFR 20.21, 21.49, 21.50, 21.51, 21.52 and 21.61

☐ No

Section 2. Summary of System Data

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

☒ Name	☒ Social Security Number (SSN)	☒ Personal Cell Number
☒ Birth Date	☒ Personal Email Address	☒ Group Affiliation
☒ Home Telephone Number	☒ Law Enforcement	☒ Employment Information
☒Mailing/Home Address	☒ Other: *Specify the PII collected.*	

All permit applicants provide their full name, or if applying as a business, corporation, public agency, Tribe or institution, the name of the principal officer; customs agent, if applicable; and the primary point of contact. Also, primary and alternate phone numbers; fax number of business applicants; physical/mailing address; email address; Tax Identification Number for business applicants which can be an SSN for sole proprietorships; and date of birth (DOB) from individual applicants only.

This system also contains records on corporations and business entities that are not subject to the Privacy Act, including company name, address and telephone number, TIN, DUNS number, and bank account and routing number. However, personal information related to individuals may be subject to the Privacy Act.

Users of the online application system must create an account by providing a Logon ID, password and email address. Applicants are not required to use Online Permits. Applicants may obtain hard-copy forms from their nearest FWS Regional Office or may download digital versions from the FWS Forms website at https://www.fws.gov/forms.

Each permit application collects information specific to the activity the applicant wishes to conduct and information about the applicant's education and experience conducting the activity. For example, individuals applying for a Migratory Bird taxidermy permit must describe their experience mounting migratory game birds and any training or schools attended. Applicants are asked to provide the names of any sub-permittees or persons assisting with permitted activities.

All permit applications also request disqualifying factors from applicants. These include any convictions for violating any statue or regulation relating to the activity for which the application is filled. Positive respondents are asked to provide the individual's name, date of conviction, civil penalty assessment or revocation; charge/s or reason/s for revocation, location of the incident, court, and legal action taken for each violation.

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
☒ Website
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems *Describe*

Applicant name and address are shared with Pay.gov to facilitate payments. Online Permits does not collect or maintain any credit card or financial information; it receives a notification from Pay.gov that payment has been received or not.

☐ Other: *Describe*

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

- Establish and verify an applicant's eligibility for a permit to conduct activities with protected wildlife and plants authorized under various conservation laws and treaties;
- Provide permittees with permit related information;
- Monitor and track permits affecting wildlife and plants;
- Analyze data and produce reports to monitor the use and trade in protected wildlife and plants.

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*

PII may be shared with Service personnel who have a need-to-know in the performance of their official duties. Data from Online Permits and SPITS is routinely shared with authorized FWS Office of Law Enforcement (OLE) personnel and users of the Service' s Environmental Conservation Online System (ECOS) also known as ECOSPHERE for the purposes of carrying out their official duties. PIAs for both OLE' s case management system and ECOS are available at on the DOI Privacy website at https://www.doi.gov/privacy/pia.

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

PII may be shared with DOI personnel who have a need-to-know in the performance of their official duties. For example, PII may be shared with subject matter experts employed by the Department for the purpose of obtaining scientific, management and legal advice relevant to making a decision on a permit application.

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

Limited PII is shared between Online Permits and the Department of the Treasury via pay.gov to facilitate payments. PII may be shared with the Department of Justice or other appropriate Federal agency that is responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, order or license; when there is a need to monitor activities conducted under a permit or evaluate regulated wildlife and plant trade and use; to a congressional office in response to an inquiry on behalf of a constituent; to GAO as required for the evaluation of permit programs; or to exchange information with other Federal wildlife and plant agencies, such as the

Department of Agriculture or the National Oceanic and Atmospheric Administration, on permits granted or denied to ensure compliance with all applicable permitting requirements.

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

PII may be shared with the appropriate Tribal, State, or local agency that is responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation , order or license; when there is a need to monitor activities conducted under a permit or evaluate regulated wildlife and plant trade and use; or to exchange information with other Tribal, State, or Local wildlife and plant agencies on permits granted or denied to ensure compliance with all applicable permitting requirements.

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

PII may be shared with FWS contractors when they have a need-to-know in the performance of their official duties toward accomplishing a FWS function related to permits. PII may also be shared with DOI contractors who are subject matter experts employed by the Department for the purpose of obtaining scientific, management and legal advice relevant to making a decision on an application or a permit.

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

PII may be shared to other authorities such as CITES and the World Conservation Monitoring Center, federally permitted rehabilitators, licensed veterinarians and individuals who seek assistance with sick, orphaned and injured birds under the Migratory Bird Treaty Act and the Bald and Golden Eagle Protection Act for purposes commensurate with original the purpose of collection. For example, FWS may release contact information for a bird rehabilitator with his or her consent when a member of the public requests assistance with locating a facility. FWS also routinely shares information about permit holders that are public institutions such as state university or federal agency or museum. PII may also be shared with appropriate agencies, entities or persons when DOI has determined there has been a breach of the system or when information from this system would aid another Federal agency or entity experiencing a breach of their system.

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.*

Individual permit applicants may choose not to apply for a permit or not to complete all of the permit application fields; however, failure to provide all requested information may prevent FWS from being able to approve the application. Applicants are not required to use the online

system and therefore may decline to provide PII needed for FWS to create a user account. Each application form and the Online Permits website include the required Privacy Act statement referencing SORN INTERIOR/FWS-21, Permits, where applicants may read the permissible uses and sharing of their personal information.

While FWS system administrators and users may not decline to provide their PII to gain system access in order to perform their official duties, they do receive notice of all permissible uses and sharing of their PII during the hiring and onboarding process.

☐ 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 paper-copy applications and is available via hyperlink on the Online Permits login page.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and the related SORNs published in the *Federal Register.* The online application site also contains hyperlinks to FWS' privacy and security policies. All users receive a notice of monitoring for appropriate usage. Pay.gov also provides notice to users through a hyperlinked privacy policy on their website and the Department of Treasury's corresponding PIA.

☒ Other: *Describe each applicable format.*

All permit application forms are approved at least every three years by 0MB, requiring notice in the *Federal Register* which provides the public the opportunity to comment on the forms. More information about the Department's privacy program including how to submit a request for records protected by the Privacy Act is available at DOI's Privacy website at https://www.doi.gov/privacy.

Further information about FWS' permitting programs can be found at https://www.fws.gov/permits/.

☒ None

Individuals, such as customs agents or business principal officers, may not be aware or receive specific notice that their PII is being provided to the Service as part of a permit application. For example, the names of persons assisting the applicant with permitted activities may be requested on the application. It is expected that these individuals have general knowledge FWS' permitting requirements. The Service encourages applicants to notify third parties and/or affected individuals of specific application submissions with their information and to confirm the accuracy of the information before providing to FWS.

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

Data is retrieved primarily by permit number and/or applicant name or contact information. Electronic records can be searched or retrieved by any data field in the application.

I. Will reports be produced on individuals?

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

System users can produce reports using various parameters based on information that has been provided by the applicant and/or permit holder. The reports enable the user to determine certain information regarding the application, including the type of application, status of the application, numbers of requests, fees paid, reports submitted, etc. This information is only accessible to authorized users and managers of the permit programs.

☐ No

Section 3. Attributes of System Data

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

Permit applicants must acknowledge that they have read and are familiar with Federal fish and wildlife regulations; that they are submitting complete and accurate information; and that any false statement in their application/s may lead to criminal penalties pursuant to 18 U.S.C. 1001.

FWS permit issuers thoroughly review each application for accuracy. Applications that are inaccurate or incomplete are rejected and returned to the applicant for completion or retraction. Permit issuers also ensure that payment where necessary has been made.

Use of pay.gov also helps to ensure accuracy as the applicant identifying information in Online Permits must match that provided to Pay.gov. Pay.gov is unable to process any payment if the application and payment identifiers do not match.

B. How will data be checked for completeness?

Online Permits uses required fields that must be completed prior to advancing within the automated application process. If required information is omitted, the applicant will receive an error message informing them that a required field must be completed prior to continuing with the application.

FWS permit issuers thoroughly review each application for completeness. Applications with missing or partial information are rejected and returned to the applicant for completion or retraction.

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

Permit holders are required to maintain up-to-date profile information for the life of the permit. Applicants are also required to verify and update their profile when applying for new or additional permits. Online Permit public users must change their password every 90 days. This provides opportunities for them to update their profile information as needed.

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

Data in the system is considered temporary and may be destroyed ten years after the permit expiration in accordance with FWS Records Schedule PERM-201, Permit Tracking Database (Nl-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?

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 a moderate risk to individual privacy due to the PII collected and maintained in Online Permits. The primary privacy risks are posed by unauthorized access, unauthorized disclosure and/or misuse of data in the system. There are also privacy risks inherent from data becoming law enforcement sensitive and/or shared with law enforcement; lack of specific notice to third parties identified in permit applications; and in collecting more information than is relevant and/or

storing information longer than necessary. These risks are addressed and mitigated through a variety of administrative, technical and physical security controls.

First, Online Permits collects the minimum information necessary to establish and verify an individual's eligibility for a permit. Each permit type collects the same standard identifying information (name, address, phone numbers, email address) for all applicants pursuant to 50 CFR 13.12, *General information requirements on applications for permits.* The rest of the application is tailored according to the activity the applicant wishes to conduct. Standardization of the PII collected helps the Service to process the applications timely and accurately. Incomplete applications are identified quickly and returned to the applicant for correction or retraction.

FWS provides adequate notice to permit applicants and users of the system. While individuals involved in and assisting with permit-required activities have general awareness of permit requirements, there is a risk that some individuals may not be aware that their PII is being provided to FWS as part of a specific permit application, especially where information for custom agents, brokers, business officers or representatives is required. Individual applicants may be asked to provide the names of persons assisting the applicant with permitted activities. In such cases, the Service encourages applicants to notify all third parties and/or affected individuals when supplying their information to FWS. Notice also helps to ensure the PII is correct. Otherwise, notice is available through the applicable SORNs, PIA and 0MB approval process, as well as FWS' Permitting programs website at https://www.fws.gov/permits/.

Privacy risks from sharing data with law enforcement include loss of data integrity; loss of data and data confidentiality for data shared and controlled by other organizations. Mitigations for these risks include FWS law enforcement investigation procedures and processes and system controls in FWS' Law Enforcement Management Information System (LEMIS). These mitigations are described in the LEMIS PIA available at https://www.doi.gov/privacy/pia. All authorized disclosures of PII outside of the Department are documented in the case file by the investigating case officer in accordance with the Privacy Act of 1974 (5 U.S.C. 552a(c)(l)) and to help maintain the integrity of the data.

Online Permits and SPITS access is granted to authorized individuals only. Authorized users of Online Permits are granted access only to the data sets needed to submit or renew permit applications, or to perform their official duties as FWS employees/contractors. SPITS is only accessible once authenticated to the FWS network and further restricted to those having a SPITS account. SPITS user accounts are approved by the permitting program's coordinator and tightly controlled by the SPITS system administrator. All FWS users are required to complete annual Role Based Security, Privacy and Records Management Training. Security and Privacy controls are implemented and tailored to prevent unauthorized disclosure and restrict access to only authorized users with a need to know. Audit logs are used to review for login information, successful logins, failed logins, and account lockouts for signs of unauthorized access or potential misuse. Audit trails of activity are maintained to reconstruct relevant security events. Audit logs are reviewed regularly and any suspected attempts of unauthorized access or scanning of the system are reported to the project manager and to IT Security. In addition, Online Permits

participates in the FWS Continuous Monitoring Program where its servers are routinely scanned; Continuous Monitoring Reports are filed quarterly and annual Internal Control Reviews (ICRs) are conducted where the controls are assessed, any remediation actions are completed, and the controls are validated.

Online Permits has undergone a formal Assessment and Accreditation and has been granted an authority to operate in accordance with Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. Online Permits is rated as Moderate based on the type of data and it requires the Moderate baseline of security and privacy controls to protect the confidentiality, integrity and availability of the PII contained in the system. Online Permits has developed a System Security and Privacy Plan (SSPP) based on NIST guidance and is a part of the FWS Continuous Monitoring program that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with DOI policy and standards.

Finally, the use of Online Permits is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each account accessing the system; time and date of access; and activities that could modify, bypass or negate the system's security controls. Audit logs are encrypted and are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning are reported to DOI Computer Incident Readiness Center (CIRC). FWS follows the principal of least privilege so that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete annual security and privacy awareness training, and those employees authorized to manage, use, or operate a system are required to take additional Role Based Security and Privacy Training. All employees are required to sign annually the DOI Rules of Behavioracknowledging their security and 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?

☒ Yes: *Explanation*

All data and PII requested from permit applicants is the minimum required to properly issue, track, and maintain FWS' permit programs. FWS uses this information to establish and verify an applicant's eligibility for a permit as required by statute.

☐ 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

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

☐ Yes: *Explanation*

☒ No, no new data is derived from data aggregation.

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

☐ Yes: *Explanation*

☒ No, not applicable.

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

The system does not derive new data or create previously unavailable data about an individual through data aggregation.

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: *Describe*

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

Applicants must create an Online Permits account in order to access the system. Access to data in the system is restricted to their own applications. Permit issuers in the FWS permitting programs are granted read/write access to their respective applications in Online Permits and SPITS to enable them to enter, review and update as necessary any applicant and permit data.

SPITS is only accessible once authenticated to the FWS network and further restricted to those having a SPITS account. FWS Office of Law Enforcement (OLE) personnel may obtain read-only access to Online Permits and SPITS in order to query and view applicant and permit data. Other users of SPITS data include permit legal examiners and biologists, permit program managers, system managers, attorneys, and FWS employees who have a need to know the information contained in the system to carry out their duties. Requests for SPITS user accounts are approved by the permitting program coordinator and controlled by the System Administrator.

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, the required Privacy Act contract clauses are included in the 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)?

☐ Yes. *Explanation*

☒ No

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

☒ Yes. *Explanation*

Online Permits maintains an internal audit log to monitor use, but is not intended to monitor or track individuals.

☐ No

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

The audit log records login time, end time, IP address, program module, and account name.

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

Principle of least privilege, log monitoring, administrative account control, effective account access controls (including account provisioning, account review, and account removal).

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 Online Permits Information System Owner is the official responsible for the oversight and management of the Online Permits security controls. The Information System Security Owner and the Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy. These officials and all authorized Online Permits users are responsible for protecting information processed and stored by Online Permits and for meeting the requirements of the Privacy Act and other Federal laws and policies for the data managed, used, and stored by Online Permits. Online Permits oversight and safeguards help to protect the privacy of the individuals about which information may be reside in Online Permits.

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 Online Permits Information System Owner is responsible for oversight and management of the Online Permits security and privacy controls, and for ensuring to the greatest possible extent that DOI and customer agency data in Online Permits is properly managed and that access to data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of customer agency and agency PII is reported to DOI-CIRC within one hour of discovery, as well as the Federal customer agency, in accordance with Federal policy and established procedures. In accordance with the Federal Records Act, the FWS Records Officer is responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.