U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

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

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

Name of Project: Data Tracking System (DTS)
Bureau/Office: Fish and Wildlife Service (FWS)
Date: March 5, 2020
Point of Contact:
Name: Jennifer L. Schmidt
Title: FWS Privacy Officer
Email: FWS_Privacy@fws.gov
Phone: (703) 358-2291
Address: Division of Information Resources and Technology Management, 5275 Leesburg Pike, MS: IRTM, Falls Church, VA 22041

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 Data Tracking System (DTS) is the Department of the Interior's (DOI) enterprise-wide correspondence management system. DTS provides consistent document management and correspondence tracking. It was developed in-house at the Fish and Wildlife Service (FWS) and

is used by all DOI bureaus and main offices pursuant to Memoranda of Agreement (MOA) with FWS.

DTS users are authorized DOI employees and contractors who upload correspondence documents received from members of the public, Federal and non-Federal government agencies, congressional representatives, the media and others. Correspondence routed in DTS may be internally-generated as well such as Federal Register notices and all-employee email messages. DTS users route the correspondence for action and response to the appropriate office/s; assign tasks to other users; track documents using DTS' built-in version control and monitor correspondence packages until closure.

Each Department bureau and office is responsible for managing its own data and records within DTS. This is accomplished in part by utilizing separate logical databases within the system. FWS is responsible for providing system maintenance and technical assistance. FWS is not responsible for other bureaus or offices' data within DTS. Bureaus and offices develop and follow their own management controls, records schedules and other applicable guidance, in keeping with the Department's overarching policies, for the processing of DTS data, including Personally Identifiable Information (PII) and information protected by the Privacy Act of 1974.

C. What is the legal authority?

- 5 U.S.C. 301, Departmental regulations
- 44 U.S.C. 3101, Records management by agency heads

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*

UII: 010-000001559
SSP Name: Data Tracking System (DTS)

☐ 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)*

Due to the nature of DTS as DOI's enterprise correspondence management system, records may be covered by a Government-wide, Department-wide, or Bureau/Service Privacy Act system of records which may be viewed at https://www.doi.gov/privacy/sorn. INTERIOR/DOI-47: HSPD-12 Logical Security Files (Enterprise Access Control Service/EACS) 72 FR 11040 (March 12, 2007) provides coverage for retrieving all user accounts by personal identifiers.

For retrieving other DTS records by a personal identifier, such as the name of the respondent, FWS primarily relies on INTERIOR/FWS-27: Correspondence Control System, 73 FR 31877 (June 4, 2008). This SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108.

☐ No

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

☐ Yes: *Describe*
☒No

Section 2. Summary of System Data

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

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

☒ Other: *Specify the PII collected.*

User (login) names and government email addresses are recorded for Federal employees who are authorized DTS users.

As DOI's enterprise correspondence management system, DTS maintains various correspondence packages and records of individuals and organizations communicating with a Department bureau or office. Due to the purpose of the system and its broad range of communications received, a significant amount of personal information is collected and maintained in DTS. Federal, Tribal, state, or local agencies, private third-party entities and members of the public, including DOI employees and contractors, correspond with DOI bureaus, offices, programs or officials, and typically include in the correspondence their name and contact information. Individuals and/or their authorized representatives regularly write to the Department about sensitive matters and voluntarily provide further details in their correspondence, including SSN, DOB, medical/health or financial information, disability data, security clearance or background investigation materials. Any PII that an individual chooses to include in his or her correspondence, including Sensitive PII, may be uploaded into DTS.

The Department bureau or office that owns the record is responsible for handling and processing the data in accordance with all applicable laws and DOI policies, including the Privacy Act of 1974. FWS is not responsible for the management of other bureaus' and offices' records or data within DTS. Bureaus and offices are responsible for their own management controls and procedures, in keeping with the Department's overarching guidance, for the processing of DTS data.

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*

The primary source of the PII collected in DTS, with the exception of DTS users, is the individual. Any individual, including employees and contractors of DOI, or representative of an external organization may send an inquiry to DOI. DOI receives correspondence from members of the public, DOI personnel, representatives of Federal and non-Federal governments, non-profit organizations, private institutions and the media. Responses to inquiries contained in a DTS record may include other records and information from the Department as well as information or records garnered from other agencies. The source of DTS user PII is DOI records.

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 (DTS users only)
☐ Other: *Describe*

Individuals submit data in paper form or by email which is then recorded in DTS by an authorized user. Members of the public do not have access to DTS. The web application is only accessible by authorized DOI users and is only accessible on the DOI network.

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

The Department bureau or office will use the PII to provide a response to the inquiry. DTS collects the minimal information necessary to provide a response. Individuals voluntarily supply their contact information and any other information they deem necessary for DOI to take appropriate action and provide an adequate response. This information may include sensitive data such as personal, medical, and/or financial information. Any and all information that an individual voluntarily submits to DOI as part of official correspondence may be maintained in DTS. The Department bureau or office will use the relevant information to provide an adequate response to the inquiry.

The Active Directory username (work email address) of authorized DTS users is an authentication identification factor. The employee's email address also is used to send notifications of task assignments in DTS.

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.*
Information in DTS may be shared with DOI personnel (employees and contractors) who have a need-to-know in the performance of their official duties in which case information is securely routed to the appropriate offices and individuals required to provide input or review for a response to an inquiry from the public, a member of Congress, or another agency.

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

Information in DTS may be shared with DOI personnel (employees and contractors) who have a need-to-know in the performance of their official duties. When input or review is required from more than one bureau or departmental office, DTS securely routes information to the appropriate bureaus, offices or individuals for each document.

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

PII in DTS may be shared in accordance with the Privacy Act of 1974 and the routine uses listed in the applicable SORNS; for example:

To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation.

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

To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

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

To an expert, consultant, grantee, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

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

To Federal, state, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

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.*

Individuals voluntarily provide PII when seeking action from DOI. They may decline to provide

their contact information; however, incomplete submissions may result in DOI's inability to respond. Individuals also voluntarily provide any and all further information they consider necessary for DOI to take appropriate action and provide an adequate response. This may include sensitive personal information beyond PII. Individuals may contact DOI at any time to stop action on or correct their correspondence; however, the record will still be maintained in DTS according to the applicable records retention period. Federal employees and contractors may decline to provide their PII but will not be able to onboard as a Federal employee or perform their official duties.

☐ 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.*

Privacy Act Statements are provided to Federal employees during the onboarding process on the Declaration for Federal Employment, Employment Eligibility Verification and Fair Credit Reporting Release forms that are maintained in the DOI's Federal Personnel and Payroll System (FPPS).

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and related SORNS published in the *Federal Register*. Federal personnel receive privacy notices prior to logging onto government computers and DTS. More information about the Department's privacy program including compliance documents and how to submit a request for agency records pertaining to you is available at DOI's Privacy website at https://www.doi.gov/privacy.

☐ 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.).

DTS records are retrieved by a DTS identifier, a tracking number given to all correspondence packages. Records in DTS may also be retrieved by name, organization name, or state. DTS users may also look up other users by email address to route correspondence. This feature helps ensure that correspondence is shared with users authorized to access the information.

DTS user accounts are retrieved by the employee or contractor's username and government email address as part of the Active Directory (AD) authentication process, either directly as the

username identifier for all AD-enabled applications and services, or indirectly as part of the Personal Identity Verification (PIV) card authentication process.

I. Will reports be produced on individuals?

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

Authorized system users can generate reports based on search criteria such as names, organizations, and addresses located in the database. These reports are used to aggregate the number of correspondence entries in correlation to a particular individual's name or organization located within the system. For example, a user can produce a report detailing how many correspondences associated with a particular member of Congress, by entering a Congressional representative's name in the search form. Access to these reports is based on an Access Control List that is maintained by the system administrator.

DTS can produce employee user and activity reports. The reports provide a detailed description of application usage and frequency of use by an individual. Only individual(s) designated by the System Owner or system administrator will have access to these reports.

☐ No

Section 3. Attributes of System Data

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

Information such as mailing address and phone numbers are provided voluntarily by the individual corresponding with the agency and are therefore presumed to be accurate. It is the responsibility of the individual to contact DOI/Bureau as needed to correct any information or amend his or her inquiry.

B. How will data be checked for completeness?

The information is provided directly by the individual and therefore presumed to be complete. The individual may contact DOI/Bureau to provide further information.

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

The currency of contact information is guaranteed by attempting to respond to the incoming request and by forwarding information to the appropriate parties. Contact information provided by members of the public is presumed to be current; otherwise, mail is returned. In both cases, the bureau or office responsible for the record will update DTS accordingly.

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

Retention periods for DTS vary as records in DTS are maintained by subject matter in accordance with applicable DOI bureau of office records schedule, Department Records Schedule or General Records Schedule, approved by the National Archives and Records Administration (NARA) for each specific type of record maintained by the Department.

Each Department bureau and office is responsible for enforcing their records schedules. Each bureau's data is logically separated, so bureaus may follow their own records schedules (in accordance with the Department and as approved by NARA) and are prevented from accessing other bureaus' records. Records retention periods may also be suspended by litigation holds, court orders, preservation notices, and similar issued by the DOI Office of the Solicitor or other authorized official.

Unless otherwise specified by the office or program that owns the data FWS records in DTS are maintained in accordance with the DOI Records Schedule, DAA-0048-2013-0002, Long-term Administrative Records. Records under this schedule are considered temporary and may be destroyed seven years after cut-off or seven years after the fiscal year in which the files were closed.

The retention period for user account records vary, depending upon user activity. "Active" accounts are retained indefinitely, provided that the user completes required annual training per the established deadline. Accounts that are inactive for 60 days are automatically moved to the "Inactive Users" group in Active Directory. Accounts are deleted from the Inactive Users group after 90 days.

There may be unscheduled records in DTS. Unscheduled records are considered permanent. These records may not be destroyed and must be maintained until NARA has approved the retention schedule.

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. Paper reports (based on electronic output from DTS) will be shredded or pulped within the organization. Records may also be pulped, macerated, or shredded by a wastepaper contractor; however, a Federal employee must witness the destruction. If authorized by the organization that created the records, a contract employee may witness the destruction. Any contract or agreement that is put into place will prohibit the resale of the materials and must include the required Federal Acquisition Regulation (FAR) Privacy Act clauses and civil and criminal provisions of the Privacy Act for proper safeguarding of the records until their destruction.

Electronic data will be overwritten (wiped). All removable storage media (disks, tapes, CD-ROMs, etc.) will be removed before any equipment is transferred, disposed of, or donated. Procedures are documented in the System Security Plan.

There may be unscheduled records in DTS. Unscheduled records are considered permanent. These records may not be destroyed and must be maintained until NARA has approved the retention schedule.

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.

DTS primary privacy risks include unauthorized access, unauthorized disclosure and misuse of the data in the system. There is a privacy risk related to records unscheduled for disposition. Data may become inaccurate as a result of maintaining the records longer than necessary. There is another privacy risk that individuals may not be aware of all the permissible ways their information may be shared once submitted to DOI. These risks are addressed and mitigated through a variety of administrative, technical and physical controls.

User access is granted to authorized DOI employees and contractors by system administrators. Each DOI bureau and office that uses DTS may have one or more designated Agency Administrators who can authorize users and assign them to one of the agency's data groups in accordance with the DTS Agency Administrators Guide. Users are granted access to the data group/s needed in order to perform their official job duties. Each DOI Bureau and main office have staff dedicated to correspondence management and are the primary DTS users. This helps to ensure that DTS is used properly and consistently within each Bureau, and that only completed packages are routed to the correct recipients to the Department. Database access is also governed and limited by each user's email domain. Authorized users are provided access to DTS using single sign-on and validated through the DOI Active Directory.

Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized monitoring. In addition, firewalls and network security arrangements are built into the architecture of the system, and NIST guidelines and Departmental policies are implemented to ensure system and data security. System administrators will review the activities of the users to ensure that the system is not improperly used, including unauthorized monitoring. Access is restricted to only those individuals authorized by System Administrators on a need to know basis in order to perform their job duties consistent with the purposes of the system. This includes physical controls such as maintaining the system server in a secure location; and technical controls of limiting access to selected repositories of documents and data within the system, such as the authorized individual's bureau or office. Limitations on access are maintained through user login and authentication.

There is a unique privacy risk for DOI employees or contractors who write to DOI or are written about as subjects of DOI correspondence packages, as other DOI employees may become aware of personal, sensitive information. For example, if a DOI employee contacts his or her Congressional representative for assistance with a personnel complaint or administrative investigation, the representative's correspondence to DOI, including details related to the employee, may be maintained in DTS and accessed by authorized DTS users with a need-to-know.

There is minimal privacy risk to authorized DTS users, all of whom are Federal employees or contractors. DTS maintains limited information about personnel in order to grant authorized system access and utilizes mitigating controls to protect this data. The PII maintained is the individual's government username and email address and is not considered sensitive.

These privacy risks are mitigated. The DTS has undergone a formal Assessment and Accreditation and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. DTS 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. DTS 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.

Several notices of routine uses, authorized disclosures and all the permissible ways that DOI may collect, use, distribute or maintain information about individuals in DTS are provided by this PIA, the applicable SORNs, other DOI privacy program information and DOI's website privacy policy at https://doi.gov/privacy.

Finally, the use of DTS 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 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 Behavior acknowledging 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*

Information collected from the public is the minimum needed to provide an agency response to their inquiries. Individuals provide further details and information they consider relevant for the Department to know in order to take appropriate action and provide an adequate response. This information may include PII and other information protected by the Privacy Act of 1974. The system is designed to prevent unauthorized access by utilizing separate logical databases within the system and limiting access to those databases to a few authorized DTS users from each Department bureau or office. Access to sensitive data or to data in other agencies' databases is only available if the user's office has been included in the workflow for the record, or when actively routed by an authorized DTS user to other authorized users. This prevents users from accessing sensitive information without a need-to-know. Furthermore, the data collected is not used for any other purpose or shared beyond DOI except in accordance with the Privacy Act of 1974 and the routine uses listed in the applicable SORNs.

☐ 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: The bureaus do not use DTS or the PII therein to monitor individuals. DTS users can utilize reporting features to monitor public interest or to provide information to other entities. Reports are used to provide a more comprehensive response to Congressional requesters or to the public, related to subject areas of their interest and to track the quality of agency responses.

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

No new data about members of the public is 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: *Describe*

Users must have a DOI Active Directory account assigned by their bureau or office and have need-to-know in order to perform their official duties. User accounts are first authorized by their respective Agency Administrator (AA). An AA authorized in the Memorandum of Agreement (MOA) assigns each user to an office code within DTS. Data access is restricted to authorized users within each bureau and office. Records routed to an office in another agency will only be visible to the offices of that agency to which they were routed. Records may only be edited by offices that are in the routing for each record. Records marked as sensitive may only be viewed by offices they were routed to even within the agency that owns the data. The system may only be accessed from within the DOI network or using the DOI Virtual Private Network (VPN). All users must authenticate using a PIV card issued by DOI.

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

All access requires PIV card authentication wherein data is shared with a DOI Active Directory database of information on employees and contractors. Account users are reviewed and validated annually. Usernames and government email addresses are validated annually by network administrators, based on annual completion of Information Management Training (IMT), and role-based security training and role-based privacy training, as applicable.

Standard user accounts are reviewed and validated annually. Elevated user accounts are reviewed and validated quarterly. Users have access to certain fields within their Active Directory profile via the Enterprise Account Management System. Users can modify such fields as Title, Department, Supervisor, Org Code and Location. Access requires Active Directory username and password.

Developers have access to data as required to support the users of the system. The system implements separation of duties. System administrators who maintain operating systems and networks do not have access to the data system itself. Auditors must obtain permission from the bureau that owns the data to view any information in the system.

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

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

Contractors may be involved with the maintenance of the system. Contractors also may be involved in developing upgrades to the system. When a contract provides for the operation of a system of records on behalf of the Department, the Privacy Act requirements and Departmental regulations on the Privacy Act must be applied to such a system. The Federal Acquisition Regulations (FAR) also require that certain information be included in contract language and certain processes must be in place. The required FAR Privacy Act clauses are included as part of the statement of work and the contractor was provided with copies of the Department's Privacy Act regulations and applicable policies.

☐ 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*

Audit logs are maintained for seven years. The logs record the username, IP address, timestamp, files accessed, and user action performed.

☐ No

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

The system implements all applicable security controls as defined by the NIST SP 800-53. Audit records are maintained for each web request submitted by a user. System Administrator actions are logged. Invalid login attempts are logged for each server. Reports of activity are reviewed weekly.

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

DTS utilizes NIST's Control AU-09(4) Protection of Audit Information - Access by Subset of Privileged Users to help prevent unauthorized monitoring. This control requires that the number of users authorized to perform audit-related activity is limited to a small subset of privileged-users.

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 DTS Information System Owner is the official responsible for the oversight and management of the DTS 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 DTS users, Agency Administrators are responsible for protecting information processed and stored by DTS and for meeting the requirements of the Privacy Act and other Federal laws and policies for the data managed, used, and stored by DTS. DTS oversight and safeguards help to protect the privacy of the individuals about which information may be reside in DTS.

The Department bureaus and offices are responsible for handling and processing the data in accordance with all applicable laws and DOI policy, including the Privacy Act of 1974. FWS is not responsible for the management of other bureau and offices' records or data within DTS. Bureaus and offices are responsible for their own internal controls and policy guidance, in keeping with the Department's overarching guidance, for the processing, handling and maintenance of DTS data.

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 DTS Information System Owner is responsible for oversight and management of the DTS security and privacy controls, and for ensuring to the greatest possible extent that DOI and customer agency data in DTS 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. Bureau and office data in DTS is under the control of each bureau/office data owner. Each customer agency is responsible for the management of their own data and the reporting of any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities, processing or management of the data. In accordance with the Federal Records Act, the Departmental Records Officer and bureau Records Officers are responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.

The Department bureaus and offices are responsible for handling and processing the data in accordance with all applicable laws and DOI policy, including the Privacy Act of 1974. FWS is not responsible for the management of other bureau and offices' records or data within DTS. Bureaus and offices are responsible for their own internal controls and policy guidance, in keeping with the Department's overarching guidance, for the processing, handling and maintenance of DTS data.