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: Operations Inventory and Timber Sales Accounting and Reporting System (OPINV/TSARP)
Bureau/Office: Bureau of Indian Affairs/Midwest Regional Office
Date: December 2, 2020
Point of Contact
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

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 Division of Forestry and Wildland Fire Management (DFWFM) oversees the National Indian Forestry and Wildland Fire Management Program, which is a cooperative effort of the United States Department of the Interior (DOI), Bureau of Indian Affairs (BIA), Office of the Deputy Director - Trust Services, Division of Forestry and Wildland Fire Management, Intertribal Timber Council and individual Tribal governments on reservations. The Division is responsible for providing coordination, management, planning, oversight, and monitoring for all activities related to development and protection of trust forest resources, including the National Wildland Fire Program.

The Operations Inventory and Timber Sales Accounting and Reporting System (OPINV/TSARP) is a client-server, major application developed to automate and standardize the data collection and reporting for timber sales and forest stand data in the BIA, Midwest Region. OPINV/TSARP manages records of forest stands containing descriptive information, history, and project planning and records of timber sales and forest permits containing descriptive information, buyers, volumes, values, collections, and sale administration inspections.

OPINV/TSARP consists of two databases used only within the Midwest Region. Input into the tables consist of data describing the forest stand such as location, acres, ownership (Indian or Non-Indian), cover type, accessibility, operability, etc., or data describing sale or permit data, contracted logger, volume, values, and type of forest product. Other tables include data on insect and disease; tree species, product and volume; site index measurements; stand planning; fire information; and stand activity history. Users query and sort the data to locate stands in need of timber harvesting, thinning, planting, and surveys. This information is used to set up harvesting schedules, forest development work, forest inventory, and other forest management operations.

The OPINV/TSARP does not provide BIA with the capability to identify or monitor individuals. BIA manages OPINV/TSARP user accounts using the Identity Information System (IIS). This includes establishing, activating, modifying, reviewing, disabling and removing of OPINV/TSARP accounts. The application relies upon system level access enforcement. The access to the application is via Windows Active Directory (AD) file permissions. Local users who are members of the group can access the database file. Users first have to log into the network using their regular network accounts and then if they are a member of OPINV/TSARP user group can access the Access Database file through Windows file sharing. In addition, only authorized users have a shared password to access the files based on their locations.

The OPINV/TSARP uses AD authentication. AD authentication for user access is covered under the DOI Enterprise Hosted Infrastructure (EHI) Privacy Impact Assessment (PIA). For additional information on authentication, please see the EHI PIA on the DOI Privacy website: http://www.doi.gov/privacy/pia.

C. What is the legal authority?

25 U.S.C. 33 et seq., National Indian Forest Resource Management; 25 U.S.C. 163, Roll of membership of Indian tribes; 25 U.S.C. 196, Sale or Other Disposition of Dead Timber; 25 U.S.C. 406, Sale of timber on lands held under trust; 25 U.S.C. 407, Sale of timber on unallotted lands; 25 U.S.C. 413, Fees to Cover Cost of Work Performed by Indians; 25 U.S.C. 415, Leases of Restricted Lands; 25 U.S.C. 466, Indian forestry units, Rules and Regulations; 25 U.S.C. 5301, Self-determination contracts; 16 U.S.C. 594, Protection of timber owned by United States from fire, disease, or insect ravages; 16 U.S.C. 2101, Congressional statement of purpose; 18 U.S.C. 1853, Trees cut or injured; 18 U.S.C. 1855, Timber set afire; 18 U.S.C. 1856, Fires left unattended and unextinguished; Chapter 1 of Title 48, CFR Chapter 1 (Federal Acquisition Regulations).

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?

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*

UII Code: 010-000000071, Operations Inventory and Timber Sales Accounting and Reporting System (OPINV/TSARP), System Security and Privacy Plan

☐ 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	Not Applicable	Not Applicable	Not Applicable

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)*
☒ No

OPINV/TSARP is not a Privacy Act system of record. However, some records in OPINV/TSARP are maintained under DOI system of records notice(s):

- DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, for login records to access the OPINV/TSARP system
- DOI-87, Acquisition of Goods and Services: Financial and Business Management System (FBMS), 73 FR 43766, July 28, 2008, awarded timber sale contract information
- BIA-04, Trust Asset and Accounting Management System (TAAMS), 72 FR 8772, November 14, 2014, for timber sale contracts and documentation. This SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.

These SORNs may be viewed at https://www.doi.gov/privacy/sorn.

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.

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
☒ Other:

There are separate databases for each Agency and the Regional Office with their own Agency or Regional Office-specific password. There is no identifying information associated with a User. Users don't have their own individual Username or password. Users log in based on their geographic location.

OPINV/TSARP may also contain non-sensitive, business-related contact information of company representatives that are not subject to the Privacy Act, as well as data on a small proportion of sole proprietors, which are covered by the Privacy Act. Records pertaining to individuals acting on behalf of corporations and other business entities may reflect personal information. Information is only collected about entities that have been awarded a contract. PII collected from contractors includes contractor name, work address, work phone number, and work email address.

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

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: Information collected is obtained from awarded contracts, timber sale documentation, and BIA Forestry personnel.

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

☒ Paper Format
☐ Email
☐ Face-to-Face Contact
☐ Web site
☐ Fax

☐ Telephone Interview
☐ Information Shared Between Systems
☒ Other: Information is collected directly from awarded contracts and timber sale bids which are in paper format.

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

The intended use of the PII collected is for contact purposes, future forest management planning and forest history (contractor's work on a specific forest), and may be used when producing summaries by contractor for tree-cutting volume and billing purposes.

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 may be shared with BIA employees acting in their official capacity in the performance of official functions to implement forest management planning and timber sale administration.

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

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

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

Information may be shared with a Tribe to aid in timber sale preparation and project planning.

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

Information may be shared with the OPINV/TSARP Development Contractor and Office of Information Management Technology staff providing information technology support services for routine maintenance, future system enhancements, and day-to-day technical support.

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

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.*

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

The business contact information used in OPINV/TSARP is taken from awarded contracts not from the individual. Information is provided voluntarily as a condition to do business with the government.

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 Notice: *Describe each applicable format.*

OPINV/TSARP is not a Privacy Act system of record. Privacy notice is provided through publication of this privacy impact assessment and the published DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040; March 12, 2007, DOI-87, Acquisition of Goods and Services: FBMS, 73 FR 43766; July 28, 2008, and BIA-04, Trust Asset and Accounting Management System (TAAMS), 79 FR68292, November 14, 2014, for awarded contracts and timber sale documentation. These SORNS may be viewed at https://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.*

Users are presented with a DOI security warning banner that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

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

OPINV/TSARP records are retrieved by searching on Tribal reservation, compartment, and forested stands.

I. Will reports be produced on individuals?

☐ Yes: *What will be the use of these reports? Who will have access to them?*
☒ No

No reports are produced on individuals. Two standardized reports, the “Report of Timber Cut” and the “Forest History Project” are produced based on forested stand data. Contractor information may be included in the reports associated with the stands and contracts.

Section 3. Attributes of System Data

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

Data is not collected from other sources. Contractor information is obtained from awarded contracts that are managed by BIA.

B. How will data be checked for completeness?

Contractor information is manually entered into OPINV/TSARP and is checked for completeness by the Foresters.

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 data is validated at the time of entry. Once the data has been entered, it is not updated. For example, if a company changes its name after a sale is closed, the name initially entered into OPINV/TSARP would not be updated. The name of the company used when the contract was executed becomes part of the historical record.

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

Paper records are covered by Indian Affairs Records Schedule (IARS) Records Series 4400-Forestry and Fire, and have been scheduled as permanent records under the National Archives and Records Administration (NARA) Job No. N1-075-04-002, approved November 21, 2003. Records may include timber sales, monthly timber cut reports, cutting permits, log scale sheets, forestry scale and check scale report, financial statements for Indian-owned operations, forestry manuscript of annotated maps, timber trespass, and timber marketing records. Records are maintained in the office of records for a maximum of 5 years. Records are cut-off at the end of the fiscal year. The records are then retired for permanent safekeeping to the American Indian Records Repository which is a Federal Records Center. Subsequent legal transfer of records to the National Archives of the United States will be as jointly agreed to between the United States Department of the Interior and the National Archives and Records Administration.

OPINV/TSARP master data file has been scheduled as permanent records under the NARA Job Code Number N1-075-07-013, approved June 12, 2007, and maintained under IARS Records Series 2200-Operations Inventory (OPINV).

OPINV/TSARP system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001-0013), approved by the National Archives and Records Administration (NARA). These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off.

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

Data and information maintained within OPINV/TSARP is retained under the appropriate NARA approved Indian Affairs Records Schedules (IARS). Data disposition follow NARA guidelines and approved Records Schedule for transfer, pre-accession and accession activities to NARA. These activities comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins and the Bureau of Trust Funds Administration, Office of Trust Records, which provides records management support to include records management policies and procedures, and development of BIA's records retention schedule. System administrators dispose of DOI records by 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 limited risk to the privacy of individuals due to the minimal amount of non-sensitive PII contained in OPINV/TSARP. Information collected about entities that have been awarded a contract are only business-related contact information. Users enter an Agency or Regional Office-specific password and do not have their own individual Username or password. OPINV/TSARP has undergone a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. OPINV/TSARP is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. Access to files is strictly limited to authorized personnel who need access to perform official functions. System and information access is based on the "least privilege" principle combined with a "need-to-know" in order to complete assigned duties. Furthermore there are separate databases for each Agency and the Regional Office with their own Agency or Regional Office-specific password, which further limits sharing of information, and that users do not require their own username and password to access the database, access to a database is controlled by the MWRO Manager. BIA manages OPINV/TSARP user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of OPINV/TSARP user accounts. System administrators utilize user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system is reported to IT Security. Annually, employees complete privacy training which includes the topics of inappropriate use and unauthorized disclosure. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. Physical, operational, and technical controls are in place and other security mechanism have also been deployed to ensure data and system security such as firewalls, virtual private network, encryption, malware identification, intrusion detection, and periodic verification of system user activity. Audit logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use to control access, protect against inappropriate use or disclosure to unauthorized individuals.

There is a risk that OPINV/TSARP may collect and share more information than necessary to complete program goals and objectives, or information may be used outside the scope of the purpose for which it was collected. Only the minimal amount of information needed to perform official functions for which the system was designed is collected and maintained in order to provide a service or perform official functions. Authorized personnel with access to the system are instructed to only collect the minimum amount of information needed to perform official functions for which the system was designed and are to share information only with individuals authorized access to the information and that have a need-to-know in the performance of their official functions. Employees complete privacy training which includes topics on the collection and unauthorized disclosure of information. Users are advised not to share sensitive data with individuals not authorized access and to review applicable system of records notice before sharing information. Employees are aware information may only be disclosed to an external agency or third party if there is informed written consent from the individual who is the subject of the record; if the disclosure is in accordance with a routine use from the published SORN and is compatible with the purpose for which the system was created; or if the disclosure is pursuant to one of the Privacy Act exceptions outlined in 5 U.S.C. 552a(b). Before authorizing and granting system access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and "need-to-know" factors, and based on the "least privilege" principle. Access restrictions to data and various parts of the system's functionality is role-based and requires supervisory approval. Access to OPINV/TSARP is regularly cross-reference against records in IIS as part of the continuous monitoring program. OPINV/TSARP meets BIA's information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. The risk is minimized because once the contract/contractor data has been entered, it is not updated. For example, if a company changes its name after a sale is closed, the name initially entered into OPINV/TSARP would not be updated. The name of the company used when the contract was executed becomes part of the historical record. Contractor information is obtained from awarded contracts and is validated as it is input into OPINV/TSARP. The majority of the information used in OPINV/TSARP is obtained from logically organized panels used to input data, which can be selected from dropdown list values. The use of dropdown list values and pick lists significantly reduces the possibility of entering incorrect values.

There may be a risk associated with the collection of information from another DOI system. OPINV/TSARP extracts contractor information from paper-based, awarded which come from FBMS, an internal DOI system. The Branch of Forestry relies on the accuracy and currency of information obtained from FBMS, which is the responsibility of the system owner.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The Branch of Forestry, as the information owner, is responsible for managing and disposing of BIA records in OPINV/TSARP. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued business and Tribal value. Branch of Forestry ensures only records needed to support its program, Tribes, and Tribal members is maintained. Branch of Forestry maintains the records for a maximum of five years or when no longer needed for current business operations, at which time they are transferred to the American Indian Records Repository, a Federal Record Center for permanent safekeeping in accordance with retention schedules approved by NARA under Job Code N1-075-07-013, Series 2200 – OPINV. Information collected and stored within OPINV/TSARP is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not have notice of the purposes for collecting their information. Although information is not collected directly from the individual, the risk is mitigated as individuals are notified of privacy practices through this PIA and through the published DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040; March 12, 2007, DOI-87, Acquisition of Goods and Services: FBMS, 73 FR 43766; July 28, 2008, and BIA-04, Trust Asset and Accounting Management System (TAAMS), 72 FR 8772, February 27, 2007, for awarded contracts and timber sale documentation. SORNs may be viewed at https://www.doi.gov/privacy/sorn. The PIA and SORN provide a detailed description of system source data elements and how an individual's PII is used.

In addition to the risk mitigation actions described above, the BIA follows the "least privilege" security principle, such 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. Access to the DOI Network requires two-factor authentication. Users are granted authorized access to perform their official duties and such privileges comply with the principles of separation of duties. Controls over information privacy and security are compliant with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. DOI employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, and Controlled Unclassified Information before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

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*

The use of the system and data collected is relevant and necessary to the purpose for which OPINV/TSARP was designed and supports the Indian Affairs mission of providing coordination, management, planning, oversight, and monitoring for all activities related to development and protection of trust forest resources, including the National Wildland Fire Program. The OPINV/TSARP was specifically developed to support the Indian Affairs trust forest management responsibilities.

☐ 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

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?

Not Applicable. OPINV/TSARP is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

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?

Users are only given access to data on a 'least privilege' principle and 'need-to-know' to perform official functions. BIA manages OPINV/TSARP user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of OPINV/TSARP user accounts. The Midwest Regional Office (MWRO) manager decides who gets access and at what level and notifies the system administrator what user accounts to establish, close or suspend. The MWRO manager decides at what level each user has rights to resources.

OPINV/TSARP is a standalone application designed in Microsoft Access and does not have built-in access control mechanisms. The application relies upon system level access enforcement. Access to the application is via Windows Active Directory (AD) file permissions. Local users who are members of the group can access the database file. Users first have to log into the network using their regular network accounts and then if they are member of OPINV user group can access the Access Database file through Windows file sharing. Each Agency and Regional Office maintains a shared password for accessing only their available information. There are separate databases for each Agency and the Regional Office, each with their own password. There is no other identifying information associated with the users. Users do not have their own individual username or password.

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 are required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. The following Privacy Act contract clauses were included in the contract.

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.224-3, Privacy Act Training (Jan 2017)
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

☐ 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*
☒ No

The OPINV/TSARP system is not intended to monitor individuals. There is no way to monitor individuals activities as there are no individual passwords or usernames that can lead to the identity of an individual. OPINV/TSARP is a stand-alone application designed in Microsoft Access and does not have built-in access control, audit or monitoring capabilities.

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

The OPINV/TSARP system is not intended to monitor individuals. OPINV/TSARP is a stand-alone application designed in Microsoft Access and does not have built-in access control, audit or monitoring capabilities.

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

OPINV/TSARP is a stand-alone application designed in Microsoft Access and does not have built-in access control, audit or monitoring capabilities. OPINV/TSARP System Administrators review access to the system to ensure that the system is only used by authorized individuals. OPINV/TSARP assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users are required to consent to OPINV/TSARP Rules of Behavior. Users must complete annual Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially upon employment and annually thereafter, to ensure an understanding of their responsibility to protect privacy.

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. OPINV/TSARP is a stand-alone application designed in Microsoft Access and does not have built-in access control, audit or monitoring capabilities. The monitoring security practices is completed manually to validate only authorized users have access to OPINV/TSARP.

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 Associate Chief Information Officer (ACIO) is the Information System Owner (ISO). The ISO, Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in OPINV/TSARP. The ISO and the Privacy Act system managers are responsible for addressing any Privacy Act complaints and requests for notification, access, redress, or amendment of records in consultation with the DOI Privacy Officials.

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 OPINV/TSARP ISO and ISSO are responsible for oversight and management of the OPINV/TSARP security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The OPINV/TSARP ISO, ISSO, and bureau and office system administrators are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within one hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with DOI Privacy Officials. Program officials and users are also responsible for protecting PII and meeting requirements under the Privacy Act and Federal law and policy, and for reporting any potential compromise to DOI-CIRC and privacy officials. In accordance with the Federal Records Act, the Office of Trust Records is responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.