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: Tracking Accountability Performance System (TAPS)
Bureau/Office: Bureau of Indian Affairs (BIA), Office of Trust Services (OTS)
Date: 03/11/2020
Point of Contact:
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Road N.W., 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 Bureau of Indian Affairs Office of Trust Services carries out Indian Affairs trust responsibilities to Indian tribes, individuals and oversees all activities associated with the management and protection of trust and restricted lands, natural resources, and real estate services. The office provides land-related functions to Indian trust owners including acquisition, disposal, rights-of-way, leasing and sales, and assists them in the management, development, and

protection of trust land and natural resource assets. Programs administered by the Office of Trust Services include real estate services; land title and records; probate; natural resources; forestry and wildland fire management; irrigation, power and safety of dams.

The Tracking Accountability Performance System (TAPS) is an in-house developed, major application managed by the Office of Trust Services (OTS). TAPS is a tool used to enhance workforce management practices, maximize productivity and efficiency at both a staff and program level. It provides a means to track responses to inquiries, manage case-related information and day-to-day workload of the Trust Services branch. TAPS groups information together and makes it readily accessible to all who need access to information about a case. It manages the collection of customer communications, forms, process documents, reports and supporting documentation needed for compliance and audit. TAPS supports a user's need to respond quickly to assigned deadlines. TAPS tracks operational performance and productivity, generates analytical metrics to assist Regional Directors and the Central Office in carrying out Indian Affairs trust responsibilities. It provides critical performance data on the Land Titles and Records mission to address and meet Governmental Performance Results Act targets. TAPS also provides staff with quick access to case data for responding to inquiries from Congress, Indian Tribes and beneficiaries, and BIA senior management.

C. What is the legal authority?

25 CFR Part 150, Land records and title documents; 25 CFR Part 151, Land Acquisitions; 25 CFR Part 152, Issuance of patents in fee, certificates of competency, removal of restrictions, and sale of certain Indian lands; The Act of March 3, 1901 (Pub. L. 56–382; 25 U.S.C. 311); The Act of March 3, 1921 (Pub. L. 66–359; 25 U.S.C. 393); Indian Land Consolidation Act (Pub. L. 97–459); HEARTH Act of 2012 (Pub. L. 112-151); The Alaska Native Claims Settlement Act (Pub. L. 92-203); The Act of February 14, 1920 (25 U.S.C. 413); Indian Mineral Development Act of 1982 (Pub. L. 97-382); The Act of June 25, 1910, (Pub. L. 88-301, as amended)

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 Code: 010-000001920, Tracking Accountability Performance System, System Security Plan (SSP), June 25, 2019

☐ 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	None	No	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)*

This system is not a Privacy Act system of records and does not maintain records on individuals, however, employee names, usernames, and contact information are covered under the DOI-47: HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, system of records notice, which may be viewed at https://www.doi.gov/privacy/doi-notices. Case tracking support documents uploaded into TAPS are maintained under DOI system of records notice BIA-04, Trust Asset and Accounting Management System (TAAMS), 79 FR 68292, November 14, 2014, which may be viewed at https://www.doi.gov/privacy/bia_notices.

☐ 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
☒ Social Security Number (SSN)
☒ Truncated SSN
☒ Birth Date
☒ Personal Email Address

☒ Home Telephone Number
☒ Mailing/Home Address
☒ Child or Dependent Information
☒ Group Affiliation
☒ Tribal or Other ID Number
☒ Other: *Specify the PII collected.* Federal tax identification number, current land ownership, date of death, and information about parents of landowners, which is used to maintain chain-of-title history, classify legal land held in trust or restricted status may be contained within TAPS through scanned or uploaded documents that may be provided as supporting documentation. The scanned documents uploaded to TAPS are provided in either a non-optical character recognized portable document format or a Tagged Image File Format (TIFF) digital image that cannot be searched.

TAPS contains personally identifiable information from individuals, non-Indians and Indians, Indian Tribal entities, and the owners of land held in trust or restricted status by the Federal Government. This system may also contain full names of Department of the Interior (DOI) and Bureau of Indian Affairs (BIA) employees and officials who are acting in their official capacity to administer program activities, or TAPS management functions.

The collection of the Social Security Number (SSN) is incidental and is not needed for which TAPS was designed. SSNs are not requested or actively collected, but may be included in correspondence received by applicants inquiring about the status of a case or included in scanned or uploaded documents and are used to ensure accurate identification because people may have the same name and date of birth. The scanned documents uploaded to TAPS that may contain SSNs are provided in either a non-optical character recognized portable document format or a Tagged Image File Format (TIFF) digital image that cannot be searched.

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

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☐ Third party source
☒ State agency
☐ Other: *Describe*

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

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

☒ Fax
☒ Telephone Interview
☐ Information Shared Between Systems
☐ Other: *Describe*

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

TAPS is used as a case management tool to track land queries and manage employee work assignments and performance of tasks within the Office of Trust Services (OTS). The collection of PII comes from documents provided to each division within OTS to be included as part of an active case file. These documents and the information in the documents is used to oversee the administration, processing, and maintenance of legal land transactions, leasing activities, title documents, document certification, title research and examination, and the determination of legal title of Federal Indian trust or restricted lands. PII may be used for management, control, and monitoring of operational activities and documents related to client interaction with OTS. Work-related contact information collected from OTS employees is used to assign and track work assignments related to a case.

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 data is only shared with OTS staff that perform actions associated with completing a TAPS task for their assigned Regional Office or Indian beneficiaries. TAPS does not allow sharing of information across Regional Offices.

☐ 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.*

PII may be shared with a congressional office in response to a written inquiry from an individual covered by the TAAMS system of record as authorized and for the purposes stated in the TAAMS system of record notice. Data may be shared as required by law or authorized under the Privacy Act and published routine uses in BIA-04, Trust Asset and Accounting Management System (TAAMS), 79 FR 68292, November 14, 2014, system of records notice. The SORN may be viewed at https://www.doi.gov/privacy/bia_notices.

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

PII may be shared with Indian Tribes that exercise jurisdiction over the land where the parcel is located as authorized and for the purposes stated in the TAAMS system of records notice.

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

Information may be shared with contractors providing Information Technology support services for routine maintenance, future system enhancements and 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.*

Individuals requesting information maintained in TAPS can decline to provide information or consent to the use of PII by not providing documentation needed to determine the status of their case. Providing information is voluntary. The impact to the individual for not providing information may result in being unable to provide status of a request or OST services.

☐ 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 Notice: *Describe each applicable format.*

Privacy notice is provided through the publication of this privacy impact assessment and the published SORNS: BIA-04, Trust Asset and Accounting Management System (TAAMS), 79 FR 68292, November 14, 2014, system of records notice; the SORN may be viewed at https://www.doi.gov/privacy/bia_notices and DOI-47: HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, system of records notice, which may be viewed at https://www.doi.gov/privacy/doi-notices.

☒ Other: *Describe each applicable format.*

A DOI security policy banner appears when a user attempts to log into TAPS.

☐ None

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

Specific retrieval identifiers used are case number, case reference name, program assigned, and staff member assigned to complete a TAPS task. PII values, including Names and Tribal Enrollment Numbers may be contained within optional TAPS Summary fields. Values, if entered in the Summary field may be retrieved using full or partially entered search values, but retrieval of these values is not done in the course of normal business processes.

I. Will reports be produced on individuals?

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

Reports are not produced on or about individuals but on the actions of authorized system users. Reports can be generated to include any of the following events: successful and unsuccessful account logon events, account management events, object access, and authorized privilege functions. Access to these reports is limited to authorized system administrators in the performance of their official functions.

Section 3. Attributes of System Data

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

The only data obtained from sources other than DOI records comes from an individual requesting status on their case. The individual is responsible for ensuring the information provided is accurate and is presumed to be accurate by OST staff. The receipt and results of inquiries are recorded into TAPS and case status is updated as appropriate. Post-quality assurance reviews are performed on all data collected by each Division within OTS.

B. How will data be checked for completeness?

The only data obtained from sources other than DOI records comes from an individual requesting status on their case. The individual is responsible for ensuring information provided is complete. OTS staff assigned to the case crosscheck information against incoming correspondence and inquiries received via mail, email, fax, telephone or in-person interviews. Supervisory personnel, departmental leads, independent reviewers and managers perform quality assurance activities to ensure accuracy and completeness. Outgoing TAPS response correspondence is reviewed for accuracy and completeness by OTS staff, which includes Supervisor, Branch Office Manager, Division Manager or Regional Director-level, before release of information to eligible recipients.

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

The only data obtained from sources other than DOI records comes from an individual requesting status on their case. The individual is responsible for ensuring information provided is current. OTS staff assigned to the case crosscheck information against incoming correspondence and inquiries received via mail, email, fax, telephone or in-person interviews. Supervisory personnel, departmental leads, independent reviewers and managers perform quality assurance activities to ensure accuracy and completeness. Outgoing TAPS response correspondence is reviewed for accuracy and completeness by OTS staff, which includes Supervisor, Branch Office Manager, Division Manager or Regional Director-level, before release of information to eligible recipients.

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

TAPS data is maintained under the following Department of the Interior Records Schedule 1 - Administrative records retention and disposition schedules, approved by the National Archives and Records Administration (NARA), under NARA Job Numbers DAA-0048-2013-0001-0001, 0013, and -0014, and can be seen at: https://www.doi.gov/sites/doi.gov/files/uploads/DRS-Admin-Schedule-Final-Approved-06-19-2014.pdf

- 1.1A - Short-term Administration Records, Routine Administration Files [0001]. Disposition is Temporary. Records are cut-off as instructed in the agency/bureau records manual, or at the end of the fiscal year in which the record is created if no unique cut-off is specified. Records are destroyed three years after cut-off.
- 1.4A - Short-term Information Technology Records, 1.4A1 - [0013] System Maintenance and Use Records. Disposition is Temporary. Records are cut-off when superseded or obsolete. See records manual for specific criteria that may determine when a records is obsolete or superseded. Records are destroyed no later than 3 years after cut-off.
- 1.4A - Short-term Information Technology Records, 1.4A2 - [0014] System Planning, Design, and Documentation. Disposition is Temporary. Records are cut-off when superseded by newer version or upon termination of the system. Records are destroyed 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?

Records are disposed of in accordance with the applicable records retention schedules for each bureau or office, Departmental policy and NARA guidelines. Copies of records approved for destruction are disposed of by shredding or pulping for paper records, records on electronic media are degaussed or erased in accordance with applicable NARA Guidelines, 384 Department Manual 1, Department and/or Indian Affairs Records Schedules, and the National Institute of Standards and Technology Special Publication 800-88 Revision 1, Guidelines for Media Sanitization.

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 privacy risk to the individuals due to the sensitive PII that is collected, which are non-searchable, copies of records used as supporting documents and maintained in TAPS. Supporting documents obtained from TAAMS may include legal land description, current ownership information, probate and history of Indian trust lands, including title and beneficial ownership, and resources management, classification for all land held in trust or restricted status by the federal government for the benefit of Indian tribes and individual Indians; any encumbrance against the title to land; documentation such as probates and Judge's Orders which contain a decedent's first and last name; administrative corrections and notices; mortgages and release of mortgages, deeds, death certificates, cadastral surveys, fee patents; realty documents such as rights-of-way and leases, title status reports and land tract maps; which may include personally identification information such as name, address, BIA identification number, phone number, information about parents of landowners for identification purposes, Social Security number, as well as other personally identifiable information described under the *Categories of Records in the System* heading of BIA-04, Trust Asset and Accounting Management System (TAAMS), 79 FR 68292, November 14, 2014, SORN which may be viewed at https://www.doi.gov/privacy/bia_notices. This risk is mitigated through administrative, physical, and technical controls that have been implemented to protect the confidentiality, integrity, and availability of information in the system. TAPS 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. TAPS 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. To mitigate this risk, access to files is strictly limited to authorized personnel who require access to perform their official duties. In addition to physical controls, operational and technical controls in place to limit these risks include firewalls, encryption, malware identification, and periodic verification of system users. System administrators utilize user identification, passwords, least privileges, and audit logs to ensure appropriate permissions and access levels are enforced. The audit trail will include 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.

There is also a risk information in TAPS may be used outside the scope of the purpose for which it was collected. This risk is mitigated by access controls implemented to ensure only authorized

personnel have access to the information needed to perform official duties and access to TAPS is limited to OST employees. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and need-to-know factors, 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. 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. In addition to physical controls, operational and technical controls in place to limit these risks include firewalls, encryption, malware identification and periodic verification of system users. Firewalls and intrusion detection systems monitor and block unauthorized connections. Current antivirus software is used to check for viruses in real time and logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest, when stored on Federal government owned and operated computer systems with restricted access. Access controls and system logs are reviewed regularly as part of the continuous monitoring process. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets. TAPS has met BIA's information system security requirements, including operational and risk management policies.

There is a risk that individuals may not have notice of the purposes for collecting their information, including how it will be used, or that their PII is sourced from other DOI internal system such as TAAMS. Individuals are notified of the privacy practices through this PIA and through the published DOI SORN: BIA-04, Trust Asset and Accounting Management System (TAAMS), 79 FR 68292, November 14, 2014; which may be viewed at https://www.doi.gov/privacy/bia_notices. The TAAMS SORN provides a detailed description of TAPS system source data elements and how an individual's PII is used.

There is a risk that TAPS may collect and share more information than necessary to complete program goals and objectives. To mitigate this risk, access to data is restricted and authorized personnel are instructed to not gather or store unnecessary information about individuals.

There may also be a risk associated with the accuracy and currency of supporting documentation collected from TAAMS. OST relies on the accuracy and currency of documentation submitted by individuals submitting requests for status and for collected from TAAMS, which is the responsibility of the TAAMS system owner.

There is a risk that information in the system will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. This risk is mitigated by ensuring all users are made aware of their information handling responsibilities, they are reminded through policy and training to follow applicable record retention schedules and requirements of the Federal Records Act. The data collected and stored in TAPS is limited to the minimal amount of data needed to meet the Office of Trust Services' mission. OST maintains the records for a maximum of three years. Information collected and stored within TAPS is maintained, protected, and disposed of in compliance with all applicable

Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. TAPS data is maintained under the following Department of the Interior Records Schedule 1 - Administrative records retention and disposition schedules, approved by the National Archives and Records Administration (NARA), under NARA Job Numbers DAA-0048-2013-0001-0001, -0013, and -0014 , and can be seen at: https://www.doi.gov/sites/doi.gov/files/uploads/DRS-Admin-Schedule-Final-Approved-06-19-2014.pdf

- 1.1A - Short-term Administration Records, Routine Administration Files [0001]. Disposition is Temporary. Records are cut-off as instructed in the agency/bureau records manual, or at the end of the fiscal year in which the record is created if no unique cut-off is specified. Records are destroyed three years after cut-off.
- 1.4A - Short-term Information Technology Records, 1.4A1 - [0013] System Maintenance and Use Records. Disposition is Temporary. Records are cut-off when superseded or obsolete. See records manual for specific criteria that may determine when a records is obsolete or superseded. Records are destroyed no later than 3 years after cut-off.
- 1.4A - Short-term Information Technology Records, 1.4A2 - [0014] System Planning, Design, and Documentation. Disposition is Temporary. Records are cut-off when superseded by newer version or upon termination of the system. Records are destroyed 3 years after cut-off.

An audit trail of activity is maintained sufficient to reconstruct security relevant events. 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 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. DOI employees must take privacy, Federal Information Systems Security Awareness (FISSA), and records management training prior to 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*

TAPS is a case management tool that supports the OTS mission by providing an array of general and operational process management capabilities such as caseload management, correspondence tracking, general administrative and operational task management, and workload monitoring. The information collected for TAPS is necessary and directly related to the purpose for which the system was designed.

☐ 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. TAPS 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*

TAPS users are given access to data on a 'least privilege' basis and a need-to-know to perform official functions. Data resides in multiple tables and limits users' access by organizational role and responsibility related to their TAPS assigned task.

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

TAPS users are only given access to data on a 'least privilege' principle and a need-to-know based on the individual's roles and responsibilities, which requires user's supervisor approval.

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. The appropriate Federal Acquisition Regulation Security and Privacy Act Clauses and other security and privacy provisions are in the Contract. 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.

☐ 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*

The TAPS system is not designed to identify or locate individuals. However, audit logs are maintained on user access to the system, as well as changes to data made by users of the system. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination for the purpose of compliance with Federal cybersecurity regulations to protect the information system and data within the system. Audit logs capture information such as username, time and date of access, and other relevant user actions and activities.

☐ No

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

Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. Additionally, audit logs capture account creation, modification, disabling, and termination. Audit Logs also collect information on system users such as username, logon date and time, number of failed login attempts, files accessed, user actions or changes to records.

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

TAPS has the ability to audit usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. TAPS System Administrators review the use of TAPS and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. TAPS 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 will be required to consent to TAPS Rules of Behavior. TAPS users must complete Federal Information System Security Awareness (FISSA) training, 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.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The TAPS audit trail will include system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system is reported immediately to IT Security.

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 Information System Owner, Information System Security Officer, 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 TAPS. The Information System Owner and the Privacy Act system managers for the related DOI systems are responsible for addressing any Privacy Act complaints and requests 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 TAPS Information System Owner is responsible for daily operational oversight and management of the system's 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 TAPS Information System Owner and Information System Security Officer 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 1-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.