



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: Forest Resource Information System (FRIS) *(Formerly TSIS)

Bureau/Office: Bureau of Land Management / Oregon State Office

Date: 04/03/2018

Point of Contact:

Name: Suzanne S Wachter

Title: BLM Associate Privacy Officer

Email: swachter@blm.gov

Phone: (202) 912-7178

Address: 20 M Street SE, Washington DC 20003

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 Forest Resource Information System (FRIS) was formerly known as the Timber Sale Information System (TSIS). The name was changed to FRIS for organizational clarification due to a subsystem within FRIS was previously named Timber Sale Information System. FRIS is a collection of application modules that support the management and tracking of forest resources including: timber sale contract accounting, management, and activity tracking; stewardship contract management and activity; special forest product sales and activity; forestry inventory depletions resulting from trespass activity; and consolidated reporting. Each of these modules provide direct support to the Bureau of Land Management (BLM) Mission Goals 2.4.01 and 2.4.02 related to managing the use of forest and woodland products in the Public Domain (PD) and in the Oregon and California Lands (O&C). The modules are used to determine the percentages towards meeting those goals nationally. This PIA covers the following subsystems within FRIS: Timber Sale Information System (TSIS), Stewardship Contract Information Database (SCID), Special Forest Products (SFP), Trespass, FRIS Reports, TicketTracker (TT), Inventory, and Timber Appraisal System (TAS).

The Forest Resource Information System uses Active Directory (AD) authentication. AD authentication for user access is covered under the DOI Enterprise Hosted Infrastructure (EHI) Privacy Impact Assessment. For additional information on authentication please see the EHI PIA on the DOI Privacy website (www.doi.gov/privacy/pia). FRIS includes corporate information that is not covered by Privacy Act, etc.

C. What is the legal authority?

Clinger-Cohen Act of 1996
OMB Circular A-130, "Managing Information as a Strategic Resource"
Oregon and California Land Revested Act of 1937 (P.L. 75-405, known as the O&C Act)
Mineral Materials Act of 1947, 30 U.S.C. 601
Healthy Forests Restoration Act of 2003 (P.L. 108-148)
Agricultural Act of 2014 (P.L. 113-79, known as the 2014 Farm Bill)

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):* System Security Plan for Forest Resources Information System; 010-000000169

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 <i>If Yes, provide a description.</i>
Timber Sale Information System (TSIS)	To manage and track timber contracts.	Yes	Detailed information supporting the management and activities of a Timber Sale Contract. PII includes purchaser name, address and phone number.
Special Forest Products (SFP)	Special Forest Products Contract / Permit Management and Tracking System	Yes	Detailed information supporting the management and activities of a Special Forest Projects Contract. PII includes purchaser name, address, phone number, personal e-mail, citizenship and vehicle license plate number.
Trespass	Tracking of Unauthorized Timber Depletion System	Yes	Detailed information supporting the management and activities of an Unauthorized Timber Depletion. PII includes purchaser name, address and phone number.



Subsystem Name	Purpose	Contains PII (Yes/No)	Describe <i>If Yes, provide a description.</i>
FRIS Reports	Consolidated Data reporting and tracking of Forestry Contract Systems	Yes	Consolidated system reporting of activity, accomplishments (including Volume and Value) of TSIS, SCID, SFP and Trespass. PII includes purchaser name, address and phone number.
TicketTracker (TT)	Tracking and management of Scaling activities associated with Scaled Timber Contract	No	N/A
Timber Appraisal System (TAS)	Estimating, valuation and worth of timber to be sold by the Bureau	No	N/A
Inventory	Forest Inventory data collection	No	N/A

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):* BLM-16, Timber Sale Information System (TSIS), 75 FR 3919, January 25, 2010. This SORN may be viewed at https://www.doi.gov/privacy/blm_notices.

The BLM-16 TSIS SORN is currently being revised to provide updated content for the system and incorporate new Federal government-wide requirements in accordance with OMB Circular A-108.

No

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



Yes: *Describe:* OMB Control Number 0596-0085 is a US Forest Service control number this is a shared permit number between the U.S. Forest Service and Bureau of Land Management. The U.S. Forest Service is the designated lead in maintaining this OMB Control Number. The title of the control number is "Forest Products Removal Permits and Contracts." The expiration date is October 31, 2018.

No

Section 2. Summary of System Data

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

- Name
- Citizenship
- Personal Cell Telephone Number
- Personal Email Address
- Home Telephone Number
- Mailing/Home Address
- Driver's License
- Other: *Specify the PII collected.*

Vehicle description and license plate information is collected to validate authorized access to the forestry products. Citizenship is verified due to requirement found in 43 CFR § 5441.1 that bidders be U.S. citizens.

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?

The information is used to validate that a corporation or individual meets the qualifications to enter into a Forestry Products contract with the U.S. Government and to validate the permit and/or contract of those working on the land in accordance with Federal laws. All information within FRIS is used for the management and tracking of forest resources including: timber sale contract accounting, management, and activity tracking; stewardship contract management and activity; special forest product sales and activity; forestry inventory depletions resulting from trespass activity; and consolidated reporting.

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 is used internally by authorized users within BLM offices for compliance and validation purposes. All information within FRIS is used for the management and tracking of forest resources including: timber sale contract accounting, management, and activity tracking; stewardship contract management and activity; special forest product sales and activity; forestry inventory depletions resulting from trespass activity; and consolidated reporting.

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

Information may also be shared with other Bureaus/Offices as authorized and described in the routine uses contained in the BLM-16, Timber Sale Information System (TSIS) system of records notice.

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

Information may also be shared with other Federal agencies as authorized and described in the routine uses contained in the BLM-16, Timber Sale Information System (TSIS) system of records notice.

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

Information may also be shared with other Tribes, State or Local Agencies as authorized and described in the routine uses contained in the BLM-16, Timber Sale Information System (TSIS) system of records notice.

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

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.*

The permit/contracts process identifies the collection of PII information and the individual can decline to provide this information. Permits/contracts may not be issued to people who decline to provide complete information.

- 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.*

The Privacy Act Statement is provided on the application form/permit. And is available via a linked web page, as well as a PDF file that can be downloaded and printed.

- Privacy Notice: *Describe each applicable format.*

Notice is also provided through the publication of this privacy impact assessment and the BLM-16, Timber Sales Information System (TSIS) system of records notice, which may be viewed at <https://www.federalregister.gov/documents/2010/01/25/2010-1364/privacy-act-of-1974-as-amended-notice-to-amend-an-existing-system-of-records>.

- 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.).

Records can be retrieved by Permit Number, Name, Address, City, State, Zip Code, and Phone Number using keyword search functions. FRIS users can retrieve records by Permit Number and Name. System administrators can search for records by individual address records.

I. Will reports be produced on individuals?

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



Reports will be used for contract administration and/or BLM Law Enforcement purposes to validate authorized access and removal of forestry resources. Reports are available only to authenticated BLM users who are members of the SFP admin user group. FRIS reports may include first/last names, city, state, zip codes and vehicle information (year, make, model, color, license plate number, and state).

No

Section 3. Attributes of System Data

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

Information collected from individuals is verified against government-issued identification that is presented by purchaser/contractor at the time of purchase/contract to ensure the federally required qualifications for purchasing forestry products are met.

BLM Law Enforcement personnel in the field check for valid permit(s) to ensure compliance with contract requirements.

B. How will data be checked for completeness?

The individual has to provide complete information during the application process. Permits/contracts may not be issued to people who decline to provide complete information. Programmatically, FRIS has built-in requirements that certain information fields must be completed prior to the certification process (validation of data entry).

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

Information collected during the application process that is verified against government-issued identification is presumed to be current at the time it is collected. PII may be updated when a permittee purchases a new permit and verifies current information or provides new information.

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

The retention period for FRIS information submitted by the public is maintained under BLM Schedule 4, items 6g and 6g(1).

Item 6g - Forest Resource Information System (FRIS) FRIS is a collection of application modules that support the management and tracking of forest resources including; timber appraisal; timber sale contract accounting, management, and activity tracking; stewardship contract management and activity; special forest products sales and activity; forestry inventory depletions resulting from trespass activity; and consolidated reporting. The records retention is Permanent. The master file with documentation is



transferred to the National Archives and Records Administration (NARA) in accordance with 36 CFR 1235.44-50 every 5 years along with the current technical documentation (N1-049-09-003).

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

The procedures for the files contained in FRIS are documented in BLM Item 4/6(g1). The records retention is Permanent. The master file with documentation is transferred to the NARA in accordance with 36 CFR 1235.44-50 every 5 years along with the current technical documentation (N1-049-09-003).

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.

This system presents limited risk to the privacy of individuals. Only minimal information is collected by individuals and companies who voluntarily submit applications to obtain permits for forestry resources. Information is only available to authorized users via elevated account access. Audit logs are maintained to ensure accountability and compliance. FRIS data is available for internal use only, and as such is behind the BLM Firewall. The public can submit electronic permit applications information if they so choose, but they do not have access to the data in this process. Only BLM users with access to the system and its reports containing PII must belong to the approved user access groups.

FRIS is classified as moderate for FISMA and has all of the required system security documentation and a current Authority to Operate (ATO). In accordance with OMB Circulars A-123 and A-130, FRIS has controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions, software controls and data encryption. All employees including contractors must meet the requirements for protecting Privacy Act information.

Business rules and guidelines, as well as rules of behavior, have been established to prevent inadvertent disclosure to individuals not authorized to use the system or those who do not have a direct “need to know” certain information contained in the system. All end-users have an individual password and ID that is issued by the FRIS application. All new users will receive training on the use of the system. All DOI employees must complete mandatory privacy, security and records management training annually, and acknowledge the DOI Rules of Behavior.

The FRIS SSP describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data via User ID, IP Address, etc. Audit trails are also captured within the system to determine who has added, deleted or changed the data within the system. Any qualification over-rides require that the account manager document the reasoning and the login name with date and time is added by the system.



Accounts are reviewed annually to ensure that only authorized personnel have systems logins. Additionally, any account that is inactive for more than one year is automatically suspended. All personnel accessing the system must acknowledge the rules of behavior prior to each login.

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:*

Data is relevant and necessary to meet requirements for determining eligibility, and contract requirements for award of permit/contract are defined in CFRs and BLM Manuals. Each of these modules provide direct support to the Bureau of Land Management Mission Goals 2.4.01 and 2.4.02 related to managing the use of forest and woodland products in the Public Domain (PD) and in the Oregon and California Lands (O&C) and are used to determine the percentages towards meeting those goals nationally.

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?



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

F. Are the data or the processes being consolidated?

- Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*
- Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*
- No, data or processes are not being consolidated.

PII within the system is not consolidated. Consolidation is in the form of counting of totals, business objectives, permit types, volume and value. No PII information is processed in the form of consolidation. PII data of FRIS is managed through the administration of security controls and management of privileged access accounts.

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 granted access via BLM Business Owner Representative approval. Access to the system is only available through the BLM intranet, requiring employees who have access to the intranet to enter their PIV credentials, or username and password, which is validated through the DOI Active Directory to sign on to the DOI network and allow for oversight. Only authorized users have access to the system and access is limited by the permissions assigned to each employee. Employees who do not have authorization to use the system will not be able to view data.

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?*
- 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:*

FRIS is not intended to monitor individuals, except for audit features to ensure authorized access and use of information. Both system and network audit logs record username, time and date of logon, files accessed, critical user actions and system event.

No

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

Audit logs reports can include username, time and date of logon, files accessed, or other critical user actions or system event.

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

The system is a BLM Internet/Intranet application and the database is behind the BLM Firewall. Users with access to the system monitoring tools and its reports are limited to users with authorized and elevated system privileges. FRIS System and user logs are included in the tool set for monitoring and auditing unauthorized system use.

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 BLM Assistant Director Renewable Resource and Planning (AD-200) is responsible for receiving and responding to any oversight and management of the FRIS System security controls and the protection of the bureau information processed and stored in the FRIS application. The FRIS Information System Owner and the FRIS Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used and stored in the FRIS application. These officials, BLM and office emergency response officials, and authorized FRIS personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act, in consultation with the BLM Privacy Officer. The Privacy Act System



Manager and BLM Privacy Officer are responsible for providing adequate notice, making decisions on Privacy Act requests for notification, access and amendments, as well as processing complaints.

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 Forester, National Operations Center; O&C Forester, Division of Resources, Lands, Minerals, and Fire; and PD Forester, Division of Resources, Lands, Minerals, and Fire, are responsible for the oversight and privacy controls, and for ensuring to the greatest extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established procedures.