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: Integrated Reporting of Wildland-Fire Information (IRWIN)
Bureau/Office: Office of the Secretary, Office of Wildland Fire
Date: October 11, 2017
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: Teri_Barnett@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

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 Integrated Reporting of Wildland-Fire Information (IRWIN) is an investment affiliated with the Wildland Fire Information and Technology (WFIT) program developed to provide an "end-to-end" fire reporting capability to facilitate the exchange or query of data. IRWIN implements the National Wildfire Coordinating Group (NWCG) data standards, and streamlines incident business processes and improves the quality of data for collecting and reporting wildland fire incidents and events. IRWIN supports fire reporting capability and coordination with multiple Federal and state agencies, and non-

Federal cooperating organizations. IRWIN is a cloud-based system. The IRWIN Core team is tasked with providing integrated data exchange capabilities between the existing applications used to manage incidents related to wildland fires. IRWIN is focused on the goals of reducing redundant data entry, identifying authoritative data sources, and improving the consistency, accuracy, and availability of operation data. Use of the IRWIN application creates seamless coordination, collaboration and information sharing of wildland fire incidents, reduces costs, and facilitates fire management planning, prevention, preparedness, protection and suppression.

IRWIN provides the capability to query data and facilitate reporting and analysis with multiple systems within the wildfire community. By interconnecting systems, new and updated information will automatically be available to the interagency systems connecting to IRWIN and to a dashboard to provide queries and reports. Such a capability will support a number of needs and provide benefits throughout the wildland fire community, allowing consistent reporting of data, reducing duplicative data entry, facilitating information sharing of data in geographically diverse systems, and increasing the accuracy and availability of wildland fire incident data.

IRWIN also consists of a "Portal" application which is also referred to as "Observer". Observer provides the capability for a user to see if data has been exchanged successfully between their internal system and IRWIN, to ensure their system had successfully exchanged data with IRWIN about transactions. Observer was developed to give users a "read only" capability to see if the data exchange between systems and IRWIN occurred successfully. No personally identifiable information (PII) is exchanged between IRWIN and other systems. The only PII contained within IRWIN or the Observer application is information used to create and manage user accounts for Observer and administrative accounts for IRWIN. The bare minimum amount of PII is collected from users to allow DOI to manage accounts in accordance with Federal Government IT security requirements identified within National Institute of Standards and Technology (NIST) SP 800-53.

C. What is the legal authority?

Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act, 44 U.S.C. 3501; the Clinger-Cohen Act, 40 U.S.C. 1401; OMB Circular A-130; and 112 Departmental Manual 7, Office of Wildland Fire.

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: 010-000000363, SSP Name: Integrated Reporting of Wildland-Fire Information

☐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.*
IRWIN Portal	Provides capability for persons to actually see IRWIN data transactions or see help and FAQ files.	Yes	The IRWIN Portal collects name, username, password, official email address, and security questions to create user accounts and for users to access and review IRWIN transactions.

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

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

☐Yes: *Describe*
☒No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.
☒Name
☒Personal Email Address
☒Other: *Specify the PII collected.*

Business email, phone number, username, password and security questions are collected from authorized users to create administrative accounts and to view the transaction dashboard.

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*

IRWIN supports fire reporting capability and coordination for multiple Federal agencies, state agencies, and non-Federal organizations.

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?

IRWIN is a fire reporting capability that facilitates the exchange of data and seamless coordination, collaboration and information sharing of wildland fire incidents, and fire management planning, prevention, preparedness, protection and suppression. PII is used to create administrative accounts for authorized users within IRWIN to allow administration of the application, hardware and software. PII is also collected to create user accounts within Observer to allow users to see (read/view only) transaction data flowing within IRWIN or transaction data that has caused an error, and to streamline incident business processes for collecting and reporting wildland fire incidents and events.

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 can be shared with the IRWIN Project Manager or the IRWIN Business Manager to improve IRWIN performance or to identify errors within IRWIN transactions. PII may also be used to ensure access control policy for IRWIN and Observer are implemented and accounts are properly managed.

☐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.*

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

The contractor will use PII to manage administrator and developer accounts.

☐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 voluntarily provide their names and other information at the time of collection to create a user account, and may decline to provide the information requested. Individuals will be denied access to IRWIN (administrator account) or Observer (user account) if they do not provide the requested information, which is required to establish an account and to manage user accounts and access to IRWIN.

☐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.*

Notice is provided to individuals through the publication of this privacy impact assessment.

☒Other: *Describe each applicable format.*

A warning banner is provided to individuals access IRWIN and IRWIN Portal at the login page.

☐None

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

IRWIN collects and reports wildland fire incidents and events, and data is retrieved by event information. IRWIN is not intended to maintain personal records on individuals. IRWIN does collect authorized user information for audit trail purposes to ensure authorized access, use, and security of the system. This type of information is retrieved by audit reports.

I. Will reports be produced on individuals?

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

Account management reports. Account manager use these to ensure account information is accurate and to delete accounts that are dormant.

☐No

Section 3. Attributes of System Data

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

Individuals validate the accuracy of the information they provide during the account creation process to request access to IRWIN. No other PII is collected from any source.

B. How will data be checked for completeness?

Information is verified by the account manager at the data collection point. If all fields are not completed by the user requesting access then an account is not created. Authorized user data is also reviewed quarterly and annually by the account manager for accuracy.

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

The DOI account manager reviews user accounts quarterly to ensure the account information is current and that the account is still needed. If accounts are dormant for more that 45 days the account is disabled and the individual is offered the opportunity to "refresh" the account by logging in. If they do not do so or they indicate the account is no longer needed it is deleted.

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

IRWIN records are covered under Department Records Schedule (DRS) 1.4.0013 System Maintenance and Use Records, which was approved by the National Archives and Records Administration (NARA)

(DAA-0048-2013-0001-0013). These records have a temporary deposition and fall under short-term Information Technology records. Records will be cut off when superseded or obsolete and destroyed no later than three years after cutoff. As long as the user's account is active, the system will retain the user's data. Upon termination of the user or license, the information will be removed from the system.

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

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1. Paper records, if produced, will be shredded. Data contained in electronic backups will be overwritten as new backups are produced. If electronic media are replaced due to aging or defect the media is sanitized in accordance with Federal government approved and verified processes. All equipment used for this purpose is in conformity with NIST SP 800-88, "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.

Privacy risks are minimal primarily because only the absolute minimum amount of information is collected to create and manage user accounts, including name, username, password, email address and phone number. The information is protected throughout all phases of its lifecycle within an authorized NIST Moderate system with adequate safeguards to protect the data within the system. No sharing of the information takes place outside of the authorized DOI personnel who are account managers and a limited number of DOI contractors with system administration privileges. PII is not used for any purpose other than user account management. All personnel have been trained in the proper collection, handling, dissemination, and destruction of PII and the requirement for the protection of PII is clearly identified within the IRWIN contracts. System audit logs are regularly reviewed by administrators in accordance with the DOI IRWIN Audit Policy, dated March 2017.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒Yes: *Explanation*

Information is required to support wildland fire incident response and events, and for effective management of user accounts in accordance with Federal IT security standards (NIST SP 800-53 rev 4).

☐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. New data is not being created.

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*

DOI IRWIN Portal Account Managers (3 DOI personnel)

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

Users only have access to their own PII for account management purposes. System administrators will have access to the limited amount of PII identified above to manage user accounts when user's information changes the IRWIN portal manager is informed to make changes.

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*

User logon is logged in audit logs. DOI is required to delete accounts that are inactive or dormant after 45 days so must know the last date of activity by any user.

☐No

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

Date and time of user logon, failed logon attempts, file access, and the last date of activity by any user are logged in IRWIN audit logs. Audit logs are reviewed by system administrators to determine if any malicious activity is occurring or has occurred.

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

Only administrators and account managers have access to information or the audit logs, and they are used to ensure that accounts are valid, accurate and being used at least once within any 45-day period. Accounts that are not used at least once within a 45-day period are deleted by DOI security policy. System security controls are implemented and enforced to protect the system and information within the system.

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*

The IRWIN system physical security controls that are implemented are those required by NIST, the Federal government and DOI for a moderate system.

(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 Director, Office of Wildland Fire, Office of the Secretary/Office of Wildland Fire serves as the IRWIN Information System Owner and the official responsible for oversight and management of security controls and the protection of agency information processed and stored in IRWIN. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in IRWIN, in consultation with the Departmental Privacy Officer.

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 IRWIN 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 IRWIN 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, and appropriate DOI officials in accordance with Federal policy and DOI policy and procedures outlined in the DOI Privacy Breach Response Plan.