**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:** National Fire Plan Operations and Reporting System (NFPORS)
**Date:** January 24, 2017
**Point of Contact:**
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: Teri_Barnett@ios.doi.gov
Phone: 202-208-1943
Address: 1849 C Street NW, Mail Stop 5545 MIB, 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 National Fire Plan Operations and Reporting System (NFPORS) is an interagency automated data management and reporting system funded jointly by the U.S. Department of the Interior (DOI) and the U.S. Department of Agriculture (USDA), for planning, managing, reporting, and tracking hazardous fuels reduction, post wildfire recovery including emergency stabilization and burned area rehabilitation, and community assistance activities. NFPORS enables uniform reporting of wildland fire information at field, regional, and national levels, and allows managers to respond to both strategic performance measures and day-to-day questions and management issues. NFPORS facilitates coordination and accountability across the DOI bureaus/offices with wildland fire management responsibilities and the USDA Forest Service, and helps meet the congressionally mandated requirements for accountability as set forth in the National Fire Plan and the Healthy Forests Initiative (or HFI), officially the Healthy Forests Restoration Act of 2003 (P.L. 108-148). NFPORS contains wildland fire records on fuel treatment, restoration rehabilitation, community assistance, and non-national fire plans, and does not contain personal records on individuals.

**C. What is the legal authority?**

The Healthy Forests Restoration Act of 2003 (P.L. 108-148); Federal Land Assistance and Enhancement Act of 2009 (FLAME Act) (43 USC 1701); National Cohesive Wildland Fire Management Strategy; Budget and Accounting Procedures Act of 1950, as amended (31 U.S.C. § Chapter 11); Chief Financial Officers Act (31 U.S.C. § 3512 *et seq.*); The Office of Management and Budget Circular A-127, Policies and Standards for Financial Management Systems.

**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*

010-000000368; NFPORS_SSP_FINAL_28JUL16

☐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 | 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)*

☒ No

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

*The Paperwork Reduction Act requires an OMB Control Number for certain collections of information from ten or more members of the public. If information is collected from members of the public, contact your Bureau Information Collection Clearance Officer for assistance to determine whether you need to obtain OMB approval. Please include all OMB Control Numbers and Expiration Dates that are applicable.*

☐Yes: *Describe*

☒ No

## Section 2. Summary of System Data

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

☒ Name
☐Citizenship
☐Gender
☐Birth Date
☐Group Affiliation
☐Marital Status
☐Biometrics
☐Other Names Used
☐Truncated SSN
☐Legal Status
☐Place of Birth

☐Religious Preference
☐Security Clearance
☐Spouse Information
☐Financial Information
☐Medical Information
☐Disability Information
☐Credit Card Number
☐Law Enforcement
☐Education Information
☐Emergency Contact
☐Driver's License

☐Social Security Number (SSN)
☐Personal Cell Telephone Number
☐Tribal or Other ID Number
☐Personal Email Address
☐Mother's Maiden Name
☐Home Telephone Number
☐Child or Dependent Information
☐Employment Information
☐Military Status/Service
☐Mailing/Home Address
☐Race/Ethnicity

☒ Other: *Specify the PII collected.*

Users' names, office phone numbers, and users' government email address are collected. The user name is used for user account and provisioning management. The users' office phone number and government e-mail address would be used for government communication to discuss and review data entries, and at times to work through role-based functions, project prioritization, and occasional application issues. Username and password is also collected to authenticate users that access the system.

**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*
NFPORS provides a secure interface for Federal employee users to enter their information directly into a secure cloud database as part of the application when requesting access to the system. Access to the NFPORS is protected through user authentication (username and password) and encryption.

**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*

- The users enter data into NFPORS through a website https://www.nfpors.gov/index.cfm?event=page.index
- NFPORS also extracts program performance data from two interconnected applications owned by the USDA Forest Service.

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

Employee user information collected is used to verify eligibility for access and use of NFPORS, and to stratify user roles into local, regional, and national groups. NFPORS does not perform any analytical functions on user information.

**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.*

The PII collected would be shared within the bureau to administer the access to the application for wildland fire fuels planning and reporting, and to manage the local, regional, and national roles of the user group.

NFPORS does not make any personal information available to other systems. There are no reports or extracts available to general NFPORS users that contain personal information. Only administrators have access to user information and that is limited to the organization for which they have administrator rights.

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

Access and use of information across bureaus/offices is not available based on the role based structure of NFPORS, however, a small number of individuals with user role of national level has access to all the collected PII across bureaus/offices.

The following bureaus have access to their own data:

- Bureau of Indian Affairs (BIA)
- Bureau of Land Management (BLM)
- Fish and Wildlife Service (FWS)
- National Park Service (NPS)
- US Geological Survey (USGS)
- Bureau of Reclamation (BOR)

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

The USDA Forest Service has access to some program data. Their system user information is shared with DOI for account management purposes. Details for the two systems that provide or consume NFPORS data with the USDA Forest Service:

**FACTS (Forest ACtivity Tracking System):**

The treatment and activity data only flows from the USDA Forest Service **Forest ACtivity Tracking System** to NFPORS and contains no user information.

**gPAS (geospatial Performance Accountability System):**

Data provided to gPAS is aggregated by fiscal year and state and includes only USDA Forest Service community assistance data, there is no user information included in the data transfer.

☐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.*

User data is occasionally shared with contractors maintaining the system for debugging purposes, which is done through the use of encrypted hard drives and secure file transfer where data is encrypted in transit and at rest. Data is destroyed securely when no longer required. No personal information is transmitted to external organizations.

☐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.*

To obtain a NFPORS user account, the user will access the NFPORS.gov website where they are presented with a User Warning banner, alerting them that the site being accessed is owned by the Government and that they agree to the Rules of Behavior applied to the use of this site. If the user does not agree to the User Warning or Rules of Behavior, they have the option of not requesting an account.

☐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.*

☒ Other: *Describe each applicable format.*

Users are provided a link to the NFPORS Rules of Behavior for using Government information technology resources and approved uses for the information provided by these resources. Users are also provided notice through the publication of this privacy impact assessment.

☐None

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

NFPORS contains wildland fire records on fuel treatments, restoration rehabilitation, community assistance, and non-national fire plan activities. These records are retrieved by a NFPORS assigned identifier, or by state or location, congressional district or location. Audit trails and user activities may be tracked for internal system administration purposes by name, user name or unit.

**I. Will reports be produced on individuals?**

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

☒ No

## Section 3. Attributes of System Data

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

An approving administrator (Bureau or National leads) verifies user account information.

**B. How will data be checked for completeness?**

An approving administrator (Bureau or National leads) verifies user account information and user privileges (roles and responsibilities) entered into the system before an account is granted.

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

Administrators review and edit, as necessary, existing users' account privileges every 90 days in accordance with the Administrators Account Management Manual. When the user moves from one Unit to another within the same organization or the user's job responsibilities have changed, the access privileges of the user will be changed. User account will be deleted when the user leaves the organization.

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

Records are maintained under the 7651 NFPORS records schedule, N1-048-08-19, Item 7651, which has been approved by the National Archives and Records Administration (NARA). The records disposition is temporary. Records are cut-off at the end of fiscal year, and destroyed 4 years after cut-off.

The NFPORS records schedule is being revised to address a business need to maintain NFPORS program and wildland fire information. This PIA will be updated to reflect any changes upon completion.

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

The records are disposed of by shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

The service contract between DOI and the service provider/contractor requires that at the conclusion of the project or transition to another vendor, all project data will be securely removed from the devices of the service provider/contractor. All the project records belong to DOI and can only be disposed of as directed by DOI.

**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.**

The privacy risk is low since only employee user credential and work contact information are collected and used for user account and project management purpose. The user account information will only be accessible for the system administrators. The program data is stored in a SQL Server database in a protected, FedRamp compliant cloud environment. NFPORS data is always encrypted in transit and at rest. The program records of the system will be retained and disposed of according to NFPORS record schedule, N1-048-08-19, Item 7651, NARA Guidelines and 384 Departmental Manual. Series of administrative, physical and technical controls are in place to ensure the confidentiality, integrity and availability of the information maintained in the NFPORS system, which further mitigates any risks.

## 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 data collected and maintained in NFPORS is used for planning, managing, reporting, and tracking hazardous fuels reduction, post wildfire recovery (emergency stabilization and burned area rehabilitation), and community assistance activities. The user information is collected and used for user account management.

☐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?**

N/A - the system does not create new data about individuals.

**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*

NFPORS is designed in a way that any authorized valid user may view data for any other organization anywhere. The administrators are responsible for making sure that accounts are granted only to valid users in accordance with NFPORS guides and manuals. Access procedures are documented in the various NFPORS user guides and the NFPORS Administrators Account Management Manual.

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

A NFPORS User is authorized to access the data on need to know and least privilege principle. Although the information contained in NFPORS is not sensitive, it is only viewable by authorized users of the application. NFPORS specific regional or state lead users are granted "edit privileges" in their Unit(s) or Region so that they may add or alter data in the production database. This is an important responsibility because the information in NFPORS is viewed and used by such a large audience. NFPORS Administrators ensure that users with edit privileges are those who have authorized wildland fire management program responsibility for their activities with fuels, restoration, and rehabilitation.

Users are identified in the NFPORS system using a unique user ID. Users must provide this ID and a password in order to gain access to the system. The system records the user ID of a user when they create a record as well as the date/time when the record was created. In addition, the system records the user ID and the date/time for the user that made the most recent modification to the record. The system also keeps track of records that have been deleted, when the record was deleted, and which user deleted the record.

**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 involved in the design, development, and maintenance of the system. The Privacy Act contract clauses are included in their contracts.

☐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 system monitors individuals to track the need for password reset to ensure the data is only viewable by authorized users who have current accounts in the system.

☐No

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

Users are identified in the NFPORS system using a unique user ID. Users must provide this ID and a password in order to gain access to the system. The system records the user ID of a user when they create a record as well as the date/time when the record was created. In addition, the system records the user ID and the date/time for the user that made the most recent modification to the record. The system also keeps track of records that have been deleted, when the record was deleted, and which user deleted the record.

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

The system only monitors individuals to track the need for password resets.

**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*

- Visitor Logs/Access Records
- Uninterruptable Power Supply

(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*

- Anti-virus and anti-malware software
- Regular scans to detect anomalous network traffic and/or unusual network activity

(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 of the DOI Office of Wildland and Fire serves as the NFPORS Information System Owner and the official responsible for oversight and management of the NFPORS security controls and the protection of customer agency information processed and stored by the NFPORS system. The

Information System Owner is 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 NFPORS.

**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 NFPORS Information System Owner is responsible for oversight and management of the NFPORS security and privacy controls, and for ensuring to the greatest possible extent that the other agency data is properly managed and that all access to customer agency and agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure is reported to DOI CIRC, US-CERT and privacy officials within 1-hour of discovery in accordance with Federal policy and established DOI procedures.