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 Interagency Fire Center External Network General Support System (NIFCENET GSS)
Bureau/Office: Bureau of Land Management, National Interagency Fire Center
Date: October 28, 2022
Point of Contact:
Name: Catherine Brean
Title: Bureau Associate Privacy Officer
Email: blm_wo_privacy@blm.gov
Phone: (830) 225-3459
Address: BLM, IRM, DOI National Operations Center, Bldg. 50, Denver, Colorado 80224

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 NIFCENET GSS is a wide area network (WAN) that provides an interconnecting backbone to support several business-related and mission-related applications used by the NIFC. The NIFCENET GSS is a network operated by the Bureau of Land Management (BLM) Fire and Aviation Directorate at National Interagency Fire Center (NIFC). This network is completely isolated from the BLM GSS. The nation’s federal wildland fire community is a large and complex organization across the Department of the Interior’s (DOI’s) Bureau of Land Management (BLM), the National Park Service (NPS), U.S. Fish and Wildlife Service (FWS), and the Bureau of Indian Affairs (BIA), and the U.S. Department of Agriculture's Forest Service (USFS). These agencies manage wildland fire on nearly 700 million acres of federal public land, or one-fifth of the total land area in the United States. To support this complex organization an independent NIFCENET GSS was developed which includes servers, workstations, networking devices (routers, firewalls, switches, and intrusion detection systems), storage devices, backup devices, and print devices. NIFCENET GSS provides several services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the WAN.

The NIFCENET GSS system supports several minor applications. These minor applications include Joint Fire Science Program (JFSP) which funds scientific research on wildland fires & distributes results to help policymakers, fire managers and practitioners make sound decisions. The program provides credible research tailored to the needs of fire and fuel managers, engage/listen to clients to develop focused strategic lines of new research responsive to those needs. Proposals are solicited from scientists who compete for funding through a rigorous peer-review process designed to ensure the best projects are funded. The focus is on science delivery when the research is completed with a suite of communication tools to ensure managers are aware of, understand and can use the information to make sound decisions and implement projects. The JFSP application does collect and maintain personal identifiable information on individuals for the purpose of submitting fire research proposals and is addressed within the scope of this PIA. The Wildland Fire Management Information (WFMI) module provides access to the weather data that is transmitted from the more than 2,500 Remote Automatic Weather Stations (RAWS) located throughout the US. The Fire Incident Cost Code System (FireCode) provides a unique four-digit financial code to incidents and the Fire Equipment Ordering System (FEOS) is used to order Fire Engines and associated equipment. The Safety Reporting System (SafeNet) is used by the Interagency community for reporting safety issues while working out in the field and the Learning Content Management System (LCMS) provides operational training to the field but does not collect any data from the students. Lastly, the NIFC Asset Management System (NAMS) is used for inventory purposes for the RAWS unit.

The primary purpose of JFSP is to support interagency wildland firefighting operations and preparedness programs for all hazard responders. Users of this system consist of representatives from multiple federal and state agencies and other cooperating organizations who have an interest in this data. The JFSP funds scientific research on wildland fires and distributes results to help policymakers and fire managers. As part of the interagency effort, the https://www.firescience.gov website was developed for the opportunity to submit proposals for possible federal funding. The JFSP application for proposal process is managed by the BLM employees on the JFSP staff.

Much of the information in the NIFCENET GSS does not constitute a system of records because it is not retrieved by unique personal identifiers, or it is not considered Privacy Act information. However, where it does constitute a system of records, the information is addressed in one or more of DOI's System of Records Notices (SORNs) which are identified within this PIA and can be viewed at https://www.doi.gov/privacy/sorn.

C. What is the legal authority?

43 CFR, Public Lands: Interior
Title 15 U.S.C. Chapter 49 Section 2229, Fire Prevention and Control
Title 16 U.S.C. Chapter 41 Section 2106c, Enhanced Community Fire Protection

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)*

010-000000108/010-000000170; NIFCENET General Support System (GSS) System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
JFSP	Tracking projects proposals from scientists who compete for funding through a rigorous peer-review process designed to ensure the best projects are funded.	Yes	The PII contained in this application are personal name, address, home and cell phone number, and email address which is used to create a profile to obtain an account on Firescience.gov and for contact purposes. The data in the Joint Fire Science Program is the grant-tracking master datafile from 1998 to the present and includes the initial proposal explaining the research project (received via an on-line application

			hosted on the BLM JFSP website) with applicant contact information.
WFMI	This system is used to collect weather data, lightning data, fire occurrence data, and unit identifiers for providing information to the wildland fire community**.** **Weather:** The WFMI Weather module provides access to the weather data that is transmitted from the more than 2500 Remote Automatic Weather Stations (RAWS) located throughout the US. **Lightning:** The lightning module proves access to lightning strike data for the continental US and is fed to other applications for the purpose of viewing the data. **Fire Reporting:** The Fire Reporting module is the system of record for the fire occurrence data for the BIA, BLM, BOR, and NPS. **Unit Identifiers:** The Unit Identifiers module is the system of record for the NWCG unit identifiers, which	No	N/A

	are the codes that are used to uniquely identify the organizational units with the federal and state government that are involved in wildland fire management.		
FireCode	This system provides specific fire codes for new incidents**.** The FireCode system generates standard fire incident management financial codes for fire incidents for all fire agencies. FireCode allows the wildland fire agencies to more accurately track the costs of wildfire suppression across multiple jurisdictions. All federal wildland fire suppression agencies (BLM, BIA, FWS, NPS, USFS) utilize the FireCode application to generate the fire code project identifiers.	No	N/A
FEOS	This system is used internally to order fire trucks and associated equipment.	No	N/A
SafeNet	This system is used by the Interagency community for field	No	N/A

	reporting of safety incidents which gives BLM personnel a mechanism for reporting unsafe conditions in the field.		
LCMS	This system contains operational training to the field but does not collect any personal data from the students.	No	N/A
NAMS	NAMS is used for ordering remote automated weather system parts for the RAWS unit**.**	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes:

INTERIOR/DOI-86, Accounts Receivable: FBMS, 73 FR 43772 (July 28, 2008); Modification published 86 FR 50156 (September 7, 2021). Once a proposal is selected for funding, a purchase requisition is completed in the Financial and Business Management System (FBMS) which identifies the institution that is to receive the funds and the total amount authorized for the institution to complete the work. This allows the funding document to be put in place and is the ledger of record of this transaction within FBMS. No individuals receive funding directly from JFSP, only institutions who have received an approved Notice of Award.

INTERIOR/DOI-89, Grants and Cooperative Agreements: FBMS, 73 FR 43755 (July 28, 2008); Modification published 86 FR 50156 (September 7, 2021). This is an integrated finance and administrative system used by all bureaus and assists DOI to manage a variety of business functions, including the awarding of grants and establishing of cooperative agreements.

DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) - March 12, 2007, 72 FR 11040; Modification published 86 FR 50156 (September 7, 2021) used for Active Directory user accounts for authentication purposes.

Department-wide and BLM SORNs which are found at https://www.doi.gov/privacy/sorn

☐ No

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

☐ Yes:

☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address

All proposals must be submitted through the JFSP electronic submission process provided on the JFSP website (https://www.firescience.gov). This website contains the Funding Opportunity Announcements which includes all information and documents needed to submit a proposal. Paper copies are not considered. The PII collected on firescience.gov is used for completion of the online proposal and contact information of scientists regarding the status of a JFSP proposal.

Username and password are collected on the firescience.gov website from members of the public interested in obtaining funding. The following information is collected when a user creates an account: name, affiliation, phone number, and email.

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*

Land management and research customers, research proposal applicants, and project administrative staff are covered within the system. The information is collected through the JFSP firescience.gov website.

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 information is collected through the JFSP website where they provide their name, affiliation, phone number and email.

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

All references to any subsystem of NIFCENET containing any Personally Identifiable Information (PII) refers only to the JFSP website, firescience.gov. The JFSP funds scientific research on wildland fires & distributes results to help policymakers, fire managers & practitioners make sound decisions. BLM provides credible research tailored to the needs of fire & fuel managers, engage/listen to clients then develop focused strategic lines of new research responsive to those needs. BLM solicits proposals from scientists who compete for funding through a rigorous peer-review process designed to ensure the best projects are funded. BLM focuses on science delivery when the research is completed with a suite of communication tools to ensure managers are aware of, understand & can use the information to make sound decisions and implement projects.

The JFSP database collects proposals submitted through a form on the website and our Funding Opportunity Notices, conducts our peer review process through the database and final reports/publications from projects that were selected for funding.

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 by the BLM Fire and Aviation Directorate at NIFC for the peer review process in the JFSP database and for reports on projects selected for funding, and for creating profiles. Once the profile is created it is used to communicate the proposal status.

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

The peer reviewers from other bureaus/offices within DOI access proposals to complete review process. The only PII that is available are name and affiliation. Only the program office has access to the profile information. In addition, an appointed 12-person Governance Board representing the JFSP partnering agencies has been established and provides strategic direction and oversight to JFSP, identifies important research questions, and in coordination with the Program Office, selects proposals for funding. The 12-member panel includes members internal to DOI from the Bureau of Indian Affairs, U.S. Fish and Wildlife, National Park Service, U.S. Geological Survey and the DOI Office of Wildlife Fire. Proposals eligible for merit review are evaluated by a peer review panel assembled to review, rate, and recommend applications to the JFSP Governing Board for final selection using the predetermined evaluation criteria. Information is also shared with the DOI FBMS for the purpose of creating a purchase requisition and a ledger record of the transaction.

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

The JFSP, through its Governing Board, is chartered by the Fire Executive Council (FEC). The JFSP is jointly funded by the Department of the Interior and the U.S. Forest Service. Peer reviewers from the U.S. Forest Service, and as part of the governance board, access proposals to complete review process. The only PII available are name and affiliation. Only the program office has access to the profile information.

☒ Tribal, State or Local Agencies:

The JFSP's collaboration also extends to tribal, and state, for the purpose of becoming partners in JFSP sponsored research in fire science.

☒ Contractor:

The contractor is the developer of the application and accesses it when requested to make changes by the program lead.

☒ Other Third-Party Sources:

Each year, the JFSP offers Graduate Research Innovation (GRIN) awards to masters and doctoral students conducting research in fire science. This helps shape the next generation of resource managers and scientists. More than 150 colleges and universities have collaborated on and partnered with JFSP-sponsored research projects. The JFSP's collaboration also extends to private and nonprofit organizations.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: .

Individuals voluntarily request an account at Firescience.gov and are presented with a clearly posted Privacy Notice which states:

"The Bureau of Land Management (BLM) recognizes and respects the privacy rights of individuals about their personal data. This Privacy Notice ("Notice") explains what type of personal data we may collect about you and how we use it. Visitors are required to log in or provide personal information to view the publicly available content on FIRESCIENCE.gov page. BLM collects limited personally identifiable information, including your name, email address, telephone number, username, and password, in order to create a user account and authenticate your identity to manage secure access to the FIRESCIENCE.gov tools pursuant to 43 C.F.R., Public Lands: Interior, Title 15 U.S.C. Chapter 49 Section 2229, Title 16 U.S.C. Chapter 41 Section 2106c. Providing this information is voluntary. If you do not provide the requested account information you will not be able to access the FIRESCIENCE.gov. BLM will not share this information unless authorized or as required by Federal law for security or law enforcement purposes."

Applicants for research funding must create a profile to be considered for a proposal. Application forms are available online and are accessible once an individual completes the Profile Request Form and are contacted to confirm their information and provided a username and password. Individuals can decline to create an account on firescience.gov however, the individual may not have access to JFSP proposal application process. Individuals can only provide the information required online in order to be considered for a proposal. Alternatively, JFSP customers can download research products without submitting any contact information. Information is only used for the purpose for which it was intended.

☐ 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:

Notice is provided to individuals through the publication of this privacy impact assessment and the applicable DOI SORNs identified in Section 1.G above. All DOI SORNs may be viewed at https://www.doi.gov/privacy/sorn. The JFSP website https://www.firescience.gov contains a link to the DOI privacy policy notice and banner on the website. In addition, the DOI privacy policy link is also provided on the Firescience.gov Sign-in/New User Registration/New Role page used to sign in, submit proposals, apply for funding, manage projects, or review proposals.

☐ 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.).

Data is stored in the JFSP database and retrieved by project proposal number. The information is only retrieved by the JFSP staff.

I. Will reports be produced on individuals?

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

Reports can be generated on research proposals only by JFSP administrative staff. The reports will be used to manage the research proposal program. Account users can access their profile to submit proposals, check on status of proposals and upload additional information on funded projects.

☐ No

Section 3. Attributes of System Data

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

All information is obtained directly from the applicant so is presumed to be complete and accurate. Any inaccurate information provided by the applicant may be corrected during the user validation procedures, during the proposal process through email, or the user may update their own profile information.

B. How will data be checked for completeness?

There are mandatory fields that the customer must complete in order to receive a Profile/Role.

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

The individuals submitting the data are responsible for ensuring the information is correct. If the proposal is submitted correctly, they will receive a confirmation page. If this confirmation page is not received the proposal has not been submitted correctly. It is the responsibility of the individual to ensure the proposal has been submitted correctly by the closing date and time.

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

The permanent Joint Fire Science Grant Case Files are scheduled in accordance with Departmental Records Schedule (DRS)/General Rescords Schedule (GRS)/BLM Combined Records Schedule, Schedule 18 - Security and Protective Services Records, BLM 18/32L(1)(a). The cutoff for permanent records is the end of the fiscal year (EOFY) in which the project closes in where the hardcopy records will transfer to the Federal Records Center (FRC) one year after the cutoff, or when no longer needed locally, whichever is later. Electronic records are transferred (along with a public-use copy) to NARA immediately for records on hand, and at three-year intervals, under the instructions in 36 CFR 1235.44-50, or whichever transfer guidance is in place at the time of the transfer.

The temporary Joint Fire Science Grant Case Files are scheduled in accordance with DRS/GRS/BLM Combined Records Schedule, Schedule 18 - Security and Protective Services Records, BLM 18/32L(1)(b) through 18/32L(4). The cutoff varies based on the records series description and can be cutoff at the EOFY in which the project closes, when the request for announcement has closed, or when no longer needed. Retention periods range from 6 years, 3 years or when no longer needed for agency business.

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

Permanent records are never destroyed and are always identified for transfer to NARA at a specific time after cutoff. Permanent records are transferred to the FRC and then later transferred by the FRC to National Archives during NARA's annual move process. Permanent records may be transferred directly to the National Archives if they have met their disposition. All temporary records are scheduled for destruction, either at their cutoff date, or after a specific period of time after cutoff. Temporary records may be transferred to FRC where they will be destroyed when they reach their authorized disposal date. The volume of records and the retention period commonly dictate when files should be transferred to the FRC.

The procedures for disposition of JFSP records are documented within the DRS/GRS/BLM Combined Records Schedule.

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 moderate privacy risk due to the type and volume of personal information maintained in the system. JFSP database collects proposals submitted through our Funding Opportunity Announcements (FOA) notices, conducts the peer review process through the database and final reports/publications from projects that were selected for funding. Technical and operating controls based on the NIST 800-53 requirements are currently in place.

JFSP 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, database permissions and software controls. All end-users have an individual password and ID that is issued by the JFSP application manager.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting, maintain information longer than necessary, and sharing information with unauthorized recipients. This risk is mitigated by limiting access to the system to only those personnel who have an official need to perform their job duties and ensuring all users complete the mandatory privacy and information security training and if applicable, the role-based privacy and security training, annually as well as, acknowledge the DOI Rules of Behavior (ROB). Access to information is role-based and is only granted on a need-to-know basis. Accounts that are inactive for more than 90 days are automatically suspended. All personnel accessing the system must acknowledge the rules of behavior prior to each login. Only the minimal amount of data needed for identification purposes is maintained and used by the system. There is a risk that an application may be denied based on the submission of inaccurate information. All information is obtained directly from the applicant so is presumed to be complete and accurate. Any inaccurate information provided by the applicant may be corrected during user validation procedures or by the applicant themselves.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA and the DOI Privacy Policy located at the bottom of the webpage. In addition, there is a privacy notice presented when the user logs into the database and must agree before they can proceed.

There is a risk that records may be maintained longer than necessary. Records are maintained throughout the life of the project and procedures for retention and disposition are followed as described in the approved DRS/GRS/BLM Combined Records Control Schedule.

There is a risk mistakes can be made when a program must rely on a person to correctly transfer data manually from one electronic system to another. The JFSP proposals must be submitted electronically via the JFSP website which does not have a direct interface with DOI FBMS, and therefore requires manual input of the data into FBMS by a BLM NIFC employee. This risk is mitigated by FBMS data being checked for completeness as it is entered into the system, use of DOI-defined business rules, and database integrity to determine if the data is complete. Validation checks are also built into the application software that both prompt the user that an incorrect entry has been entered and must be corrected, and that a user has successfully inputted the data.

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: Contact information is both relevant and necessary as all proposals must be submitted electronically via the JFSP website (https://www.firescience.gov) and individuals are required to establish a profile and create a password. BLM also requires this contact information, so it is known who submitted a proposal. In addition, contact information is used advise proposal submitters whether they have been selected for funding or not, establish agreements for approved research proposals and to facilitate putting the funding award in place.

☐ 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 as no new data is derived.

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*

The research proposal information is restricted to JFSP administrative staff and the contractor that helps with the development of the application via Oracle Roles. The users only have access to their own profile.

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

Access is determined by job function. Access request procedures will follow the current Fire and Aviation process. The customers will only have access to research products. All other access is restricted by user roles.

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?*

Contract employees were involved in the design and development of the system and all Privacy Act contract clauses were included. Contractors will not be involved in the maintenance of the system.

☐ 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.

NIFCENET GSS does not provide any capability for monitoring individual members of the public. However, audit logging is used for security purposes for individuals submitting research proposals, agency employees, contractors and those with elevated privileges which may include username, date, and time of access, tracking successful and unsuccessful attempts to access the system, and any unauthorized changes to security configurations as well as other potential security violations. 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. Additionally, the system may capture a variety of user actions and information such as usernames, logon date, number of successful and unsuccessful logins, and modifications made to data by different users along with date and time stamps. Firewalls and network security configurations are also built into the architecture of the system and NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring.

☐ No

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

The audit logs contain the user ID, date/time of access, invalid logon attempts, user activity, and as identified in the previous response, IP address for the employee who entered or modified the database record but does not link it to any other PII information.

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

NIFCENT GSS can audit the 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. In accordance with applicable DOI guidance, unauthorized activity will be included in the audit logs and alerts are being continuously updated to improve security. The audit trail includes system user username, logon date and time, number of failed login attempts, and user actions or changes. The principle of least privilege is applied to ensure the system operates at privilege levels no higher than necessary to accomplish organizational missions or business functions. In addition, all internal users must complete annual Information Management Training, which includes, privacy, security, records management, and CUI, as well as role-based privacy and security training, prior to being granted access to the DOI network or any DOI system, and annually thereafter. All internal users are required to acknowledge and sign DOI ROBs which provides the guidance needed for users to fully understand the rules and their responsibilities.

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*

NIFC employees access the application either direct console on the BLM GSS or via the DOI Pulse Secure VPN. Also, an account must be approved and created before employees are able to have access.

(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 Privacy Officer and JFSP Information System Owner is responsible for protecting the privacy rights of the public and employees affected by the interface. The Joint Fire Science Program office lead is the JFSP Information System Owner and the official responsible for oversight and management of the JFSP security and privacy controls and the protection of agency information processed and stored in the JFSP application. The Information System Owner and JFSP Program Manager, in collaboration with the BLM Senior Management Team, 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 JFSP application. These officials and authorized JFSP 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, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with BLM Associate 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 Joint Fire Science Program office is responsible for ensuring the proper use of the data. Responsibility rests with the users of the system and the System Owner, the Joint Fire Science Program Office lead. All users receive system training, and all BLM employees and contractors are required to complete periodic Privacy Act training. All federal employees comply with the requirements in OMB Circulars A-123 and A-130 as well as the Departmental Manual, 383 DM 3, Privacy Act – Bureau Responsibilities. The JFSP Information System Owner and the BLM Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the BLM Associate Privacy Officer.