U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

National Resources and Environment, Forest Service

Interagency Resource Ordering Capability (NRE FS IROC)

Date PIA submitted for review:

5/21/2024

Mission Area System/Program Contacts:

	Name	**E-mail**	**Phone Number**
Mission Area Privacy Officer	Benjamin Moreau	Benjamin.Moreau @usda.gov	386-301-4060
Information System Security Manager	Kristopher Harig	kristopher.harig@usda.gov	208-387-5170
System/Program Managers	Elise Hawes	elise.hawes@usda.gov	208-659-6274

Abstract

This Privacy Impact Assessment (PIA) is about the NRE FS Interagency Resource Ordering Capability system (NRE FS IROC). NRE FS IROC is a system supporting the US Forest Service (FS) Fire and Aviation Management (FAM) mission area.

Overview

IROC is a system that provides automated support to interagency dispatch and coordination offices within the wildland fire organization. The system: 1) provides current status of resources available to support mobilization activities; 2) enables dispatch offices to exchange and track resource order information electronically; and 3) enables dispatch offices to rapidly and reliably exchange mission-critical emergency electronic messages. Resources include qualified individuals, teams, aircraft, equipment and supplies to fight wildland fires and respond to all hazard incidents. IROC is identified as an HVA with DHS and carries an HVA ID: 210923000844.

Section 1.0 Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

National Forest Management Act of 1976 (Public Law 94-588).

- **Healthy Forests Restoration Act of 2003** (Public Law 108-148): This act promotes the health and restoration of forest ecosystems.

1.2 Has Authorization and Accreditation (A&A) been completed for the system?

Yes, 8/26/2024.

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

SORN - USDA/FS–52, Resource Ordering and Status System (ROSS), USDA/FS

1.4. Is the collection of information covered by the Paperwork Reduction Act? No

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

	Identifying Numbers		
☐	Social Security number	☐	Truncated or Partial Social Security number
☐	Driver's License Number	☐	License Plate Number
☐	Registration Number	☐	File/Case ID Number
☐	Student ID Number	☐	Federal Student Aid Number
☐	Passport number	☐	Alien Registration Number
☐	DOD ID Number	☐	DOD Benefits Number
☐	Employee Identification Number	☐	Professional License Number
☐	Taxpayer Identification Number	☐	Business Taxpayer Identification Number (sole proprietor)
☐	Credit/Debit Card Number	☐	Business Credit Card Number (sole proprietor)
☐	Vehicle Identification Number	☒	Business Vehicle Identification Number (sole proprietor)
☐	Personal Bank Account Number	☐	Business Bank Account Number (sole proprietor)
☐	Personal Device Identifiers or Serial Numbers	☐	Business device identifiers or serial numbers (sole proprietor)
☒	Personal Mobile Number	☒	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number		

			Biographical Information		
☒	Name (including nicknames)	☒	Sex	☒	Business Mailing Address (sole proprietor)
☐	Date of Birth (MM/DD/YY)	☐	Ethnicity	☒	Business Phone or Fax Number (sole proprietor)
☐	Country of Birth	☐	City or County of Birth	☐	Group/Organization Membership
☐	Citizenship	☐	Immigration Status	☐	Religion/Religious Preference
☐	Home Address	☐	Zip Code	☐	Home Phone or Fax Number
☐	Spouse Information	☐		☐	Children Information

□	Marital Status	□	Military Service Information	□	Mother's Maiden Name
□	Race	□	Nationality	□	Global Positioning System (GPS)/Location Data
□	Personal e-mail address	☒	Business e-mail address	□	Personal Financial Information (including loan information)
□	Employment Information	□	Alias (username/screenname)	□	Business Financial Information (including loan information)
□	Education Information	□	Resume or curriculum vitae	□	Professional/personal references
Biometrics/Distinguishing Features/Characteristics					
□	Fingerprints	□	Palm prints	□	Vascular scans
□	Retina/Iris Scans	□	Dental Profile	□	Scars, marks, tattoos
□	Hair Color	□	Eye Color	□	Height
□	Video recording	□	Photos	□	Voice/ Audio Recording
□	DNA Sample or Profile	□	Signatures	□	Weight
Medical/Emergency Information					
□	Medical/Health Information	□	Mental Health Information	□	Disability Information
□	Workers' Compensation Information	□	Patient ID Number	□	Emergency Contact Information
Device Information					
□	Device settings or preferences (e.g., security level, sharing options, ringtones)	□	Cell tower records (e.g., logs, user location, time, etc.)	□	Network communications data
Specific Information/File Types					
□	Personnel Files	□	Law Enforcement Information	□	Credit History Information
□	Health Information	□	Academic/Professional Background Information	□	Civil/Criminal History Information/Police Record
□	Case files	□	Security Clearance/Background Check	□	Taxpayer Information/Tax Return Information

2.2. What are the sources of the information in the system/program?

IROC data is entered by authorized users at various locations (e.g., offices, incident locations). In addition, IROC obtains information from other systems. This includes Organization Information System (OIS), Fire and Aviation Management Authorization (FAMAuth), Integrated Reporting of Wildland Fire Information (IRWIN), Virtual Incident Procurement (VIPR) , and Interagency Cache Business System (ICBS).

2.2.1. How is the information collected?

IROC data is entered by authorized users at various locations (e.g., offices, incident locations). This includes OIS, FAMAuth, IRWIN, VIPR, and ICBS. For user entered information (fire/all-hazard related need) come from resources that have been granted ordering authority per each incident. In addition, IROC obtains information from other systems. This information (also fire/all-hazard related) can also be ordered from connected applications.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

Yes, SAM.gov for public vendor account information.

2.4. How will the information be checked for accuracy? How often will it be checked?

IROC data received by incident resources are checked for accuracy and completeness by an authorized IROC user. To ensure that the IROC user enters the data correctly, audits are performed by co-workers or others in the ordering chain by verifying the information entered matches paper copy documentation. Data from other applications are imported using standard mechanisms that review the data automatically for completeness.

2.5. Does the system/program use third-party websites?

No

2.5.1. What is the purpose of the use of third-party websites?

N/A

2.5.1.1. What PII will be made available to the agency though the use of third-party websites?

N/A

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

Follow the format below:

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Section 3.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

All IROC data is collected, to order, track, mobilize, deploy, and report on a multitude of resources, including qualified individuals/overhead, teams, crews, aircraft, equipment and supplies to fight wildland fires and respond to all-hazard incidents. The resource order form that IROC produces is used for incident check in, payment, time, and is a permanent record.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No, the system does not use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly.

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Inadequate Consent: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Overuse of Information: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

Loss of Data Control: When PII is shared with third parties, there is a risk of losing control over how that data is used, potentially leading to unauthorized access or exploitation.

Mitigation: By Implementing some or all the following mitigation actions, mission areas may better safeguard PII and ensure responsible use in compliance with PA requirement:

Purpose Limitation: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

Transparency: Inform individuals about how their personal information will be used, including any potential secondary uses, through clear and accessible privacy notices.

Regular Training: Provide regular training for employees on privacy laws and the importance of adhering to the defined uses of personal information to ensure compliance.

Access Controls: Implement access controls to restrict who can use personal information and for what purposes, ensuring that only authorized personnel have access to sensitive data.

Section 4.0 Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

Notice is provided to individuals through the SORN.

Notice is also given on the website. The only use of IROC information is to support incident activities. If an individual does not wish to work on an incident, they do not have to be in IROC.

4.2. What options are available for individuals to consent, decline, or opt out of the project?

The only use of information provided in IROC is for work at an incident. If an individual does not wish to work at an incident, they need not be in IROC.

If you are a resource looking to obtain qualifications to work incidents your data must be in IROC.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

Privacy Risk: Privacy Act risks associated with notices include:

Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Non-compliance with Regulations: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

Insufficient Updates: Notices that are not regularly updated to reflect changes in data practices or legal requirements can mislead individuals and result in privacy violations.

Mitigation: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act requirements:

Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

User Consent: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Transparency: Clearly outline what personal data is being collected, the purpose of data collection, how it will be used, and who it will be shared with.

Data Minimization: Limit data collection to only what is necessary for the stated purpose. Avoid collecting excessive or irrelevant data.

User Rights: Inform users about their rights regarding their personal data, including access, correction, deletion, and the ability to object to processing.

Notice is also given on the website. The only use of IROC information is to support incident activities. If an individual does not wish to work on an incident, they do not have to be in IROC.

Section 5.0 Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

5.1. What information is retained and for how long?

Because NRE FS IROC data deals with wildland fire incidents, information is retained indefinitely per Forest Service requirements.

Fire incident records are retained in appropriate categories under '5180 – Fire Reports' (Permanent)

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

NARA has approved the retention period as recorded. Per NARA the retention will be as stated. Records are maintained subject to the Federal Records Disposal Act of 1943 (44 U.S.C. 366-380) and the Federal Records Act of 1950, and so designated in the Forest Service Records Management Handbook (FSH) 6209.11. The records are stored in an electronic data warehouse and electronic media for 7 years from the date of the last action. Disposal of data will be through secure methods that sanitize the information from all media; hard copies will be shredded or burned.

5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the retention of information include:

Excessive Data Retention: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

Data Breaches: The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Non-compliance with Regulations: Failing to adhere to legal requirements regarding data retention periods can lead to regulatory penalties and legal liabilities.

Inconsistent Retention Practices: Different mission areas/agencies may follow varying retention practices, resulting in confusion and potential violations of privacy policies.

Mitigation: Implementing the following mitigation actions, mission areas can ensure responsible retention of PII while complying with the PA.

Data Retention Policy: Use NARA data retention policies that outlines how long different types of PII will be retained and the rationale for those timeframes.

Regular Reviews: Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.

Secure Disposal Procedures: Establish secure methods for the disposal of personal information that is no longer needed, such as shredding paper documents or using data-wiping software for electronic files.

Access Controls: Implement strict access controls to limit who can view and manage retained personal information, reducing the risk of unauthorized access.

Data Minimization: Collect and retain only the PII that is necessary for the intended purpose, minimizing the risk associated with holding excessive data.

Documentation and Training: Ensure that employees are aware of and trained on the data retention policy, including the importance of compliance and the procedures for handling personal information.

Retention Schedule: Follow a retention schedule that specifies the duration for retaining different types of records and when they should be reviewed or disposed of.

FS has determined that the data retention periods and practices are adequate to safeguard PII while ensuring that mission critical data is available to support system restoration in the event of unplanned outages.

Section 6.0 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

OIS, FAMAuth, VIPR, and ICBS. Organization, user, incident, request, resource, and contract data is shared/received to support fire/all-hazard related needs. This information is transmitted via secure API's. IROC's connection uses TLS 1.2, a key exchange ECDHE_RSA with P-384, server signature RSA with SHA-512, and AES 128 GCM cipher.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

IRWIN connected applications. Organization, user, incident, request, resource, and contract data is shared/received to support fire/all-hazard related needs. This information is transmitted via secure API's. IROC's connection uses TLS 1.2, a key exchange ECDHE_RSA with P-384, server signature RSA with SHA-512, and AES 128 GCM cipher.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: Privacy act risks associated with external sharing and disclosure include:

Unauthorized Access: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Data Breaches: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.

Loss of Control: Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

Non-compliance with Regulations: Sharing PII without proper consent or outside the parameters set by privacy laws can result in legal penalties and reputational damage.

Inconsistent Data Management Practices: Different third parties may have varying practices for handling PII, leading to inconsistencies in data protection and increased risks.

Insufficient Due Diligence: Failing to conduct proper due diligence on third parties before sharing PII can expose mission areas to risks associated with partnering with unreliable or non-compliant entities.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Data Sharing Policy: Develop a clear policy outlining the conditions under which PII can be shared externally, including legal and compliance requirements (ex.: Computer Matching Agreements, SORNs, Business Agreements).

Due Diligence: Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.

Written Agreements: Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.

Need-to-Know Basis: Limit the sharing of PII to only what is necessary for the intended purpose, adhering to the principle of data minimization.

Transparency with Users: Clearly inform individuals about potential external sharing of their personal data in privacy notices, including the types of entities with whom data may be shared and the purposes for sharing.

Section 7.0 Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1. What are the procedures that allow individuals to gain access to their information?

Individuals wishing to request access to their records should contact the appropriate OPM or agency office, as specified in the Notification Procedure section of the SORN. Individuals must furnish the following information for their records to be located and identified: a. Full name(s). b. Date of birth. c. social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting access must also comply with the Office's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

7.2. What are the procedures for correcting inaccurate or erroneous information?

Current employees wishing to request amendment of their records should contact their current agency. Former employees should contact the system manager. Individuals must furnish the following information for their records to be located and identified. a. Full name(s). b. Date of birth. c. social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting amendment must also comply with the Office's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).

7.3. How are individuals notified of the procedures for correcting their information?

Individuals wishing to inquire whether this system of records contains information about them should contact the appropriate OPM or employing agency office, as follows: a. Current Federal employees should contact the Personnel Officer or other responsible official (as designated by the employing agency), of the local agency installation at which employed regarding records in this system. b. Former Federal employees who want access to their Official Personnel Folders (OPF) should contact the National Personnel Records Center (Civilian), 111 Winnebago Street, St. Louis, Missouri 63118, regarding the records in this system. For other records covered by the system notice, individuals should contact their former employing agency. Individuals must furnish the following information for their records to be located and identified: a. Full name. b. Date of birth. c. social security number. d. Last employing agency (including duty station) and approximate date(s) of the employment (for former Federal employees).

7.4. If no formal redress is provided, what alternatives are available to the individual?

Current employees wishing to request amendment of their records should contact their current agency. Former employees should contact the system manager. Individuals must furnish the following information for their records to be located and identified. a. Full name(s). b. Date of birth. c. social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting amendment must also comply with the Office's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk: Privacy Act risks associated with redress include:

Inadequate Processes: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Lack of Transparency: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Failure to Address Complaints: Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

Delayed Responses: Slow responses to redress requests can frustrate individuals and exacerbate feelings of mistrust and dissatisfaction, potentially leading to reputational harm.

Mitigation: Implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

User Awareness Campaigns: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.

Dedicated Privacy Officer/Privacy Point of Contact: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.

Section 8 Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.

8.1. How is the information in the system/project/program secured?

NRE FS IROC serves interagency federal, state, and local wildland fire and all-hazard response efforts. NRE FS IROC has utilized a federation approach called FAMAuth to authenticate users. USDA employees authenticate through e-Authentication using LincPass. Other Federal agency employees use assigned personal identity verification (PIV) access and non-Federal users will authenticate with Login.gov, which incorporates a non-PIV two-factor authentication process.

The Login.gov solution was selected as an accepted Office of Personnel Management (OPM)-provided solution to comply with multi-factor authentication (MFA) requirements for non-federal users. Using the Fire NESS-provided portal FAMAuth, NRE FS IROC implements the USDA e-Auth factored Login.gov Single Sign-On (SSO) service using username and password augmented with an additional security authentication factor using short message service (SMS). The account authorization allows access to a central selection frame from which the user may access the provisioned application for which the user is previously approved. In this case, the application is IROC.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

Federal users use the PIV access and personal identification number (PIN) verification provided by the original USDA e-Auth application. The user accesses the same central selection frame and may select from the same (or an enhanced) set of earlier provisioned and approved applications, (again, in this case, IROC).

It must be noted that only the specific applications for which the user has previous approval will appear in the portal. It is possible that the user may have no authorizations to any current application and may see an empty portal.

The system uses both individual (non-privileged) accounts and privileged administrator accounts; it does not use shared or group accounts; it does not permit any actions to be performed without identification and authentication; and it does not provide public access to the system.

Privileged accounts are required to only be federal PIV authorized users. Individual (non-privileged) accounts are either PIV or e-Auth-Login.gov username/password-SMS MFA.

Ordinary privileged account access is through the same portal as ordinary access. Backend access is accessed through a different uniform resource locator (URL) that is permanently maintained by the Service Now administration. This URL forces a login through FAMAuth. Both types of administrative access require authentication through

FAMAuth. No administration can be performed without logging into the system using FAMAuth. This includes Service Now Administrators.

All requests to create system accounts must be reviewed and approved according to "IROC Access Controls" procedure documentation. All individual (non-privileged) and privileged administrator accounts are reviewed at least quarterly.

8.3. How does the program review and approve information sharing requirements?

Information sharing requirements are documented, reviewed, and approved as part of the Interconnection Security Agreements (ISAs), Interconnection Security Plans (ISPs), and or other documented agreements between NRE FS IROC and each system that we share information with.

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

All Federal Agency employees and FS contractors are required to take annual security awareness and privacy training in accordance with Federal requirements.

Approval Signatures:

Sean Triplett
NRE FS IROC System Owner
United States Forest Service
United States Department of Agriculture

Benjamin Moreau
Mission Area Privacy Officer/ Assistant Chief Information Security Officer
United States Forest Service
United States Department of Agriculture

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.05.05 13:37:15 -04'00'

Office of the Chief Privacy Officer
United States Department of Agriculture