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:

FS Skynet (FS SN)

Natural Resources and Environment

Forest Service

Date PIA submitted for review:

06/08/2024

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

Abstract

The Forest Service SkyNet (FS SN) is a general support system (GSS) owned by the US Forest Service (FS) Chief Information Office (CIO) and operated by the Cloud Services Delivery (CSD) Branch of the FS CIO Foundational Digital Services (FSD) that is hosted on the Amazon GovCloud primarily and Amazon Commercial Cloud where necessary.

Overview

FS SN is a GSS owned by the US FS CIO and operated by the CSD Branch of the FSD .

FS SN utilizes the following types of resources: web servers and services, database services, software development tools, and authentication and authorization capabilities. These resources are used to provision logically separated production and work area environments for FS business units. The production environment consists of the resources used to host applications needed for daily operations. Logical separation is provided for each Business Service with access to the environment based on a zero trust model with security built into every layer of the applications. Additionally, the non-production environments are also logically separated for each Business Service and are accessed by FS employees and contractors. They contain resources needed to develop or improve IT assets that support the FS mission. This includes activities such as application development, testing, support, quality assurance, pilot projects, and any other relevant work that is not in production. The combination of the isolated Production and Non-production FS SN environments are used by FS business units to design, build, and deploy their mission-specific applications and systems.

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?

16 U.S.C. 472 and 551; 36 CFR 251.50 through 251.64

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

Yes, 10/09/2024.

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

USDA FS-24

1.4. Is the collection of information covered by the Paperwork Reduction Act?

Yes, OMB Control # 0596-0085, ICR Reference #202111-0596-004

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

Tribal ID

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

Skynet allows individuals to enter their own information at their discretion.

2.2.1. How is the information collected?

Users enters their own information into the web interface/application website.

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

No

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

The user is responsible for ensuring they enter their information into the system accurately.

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?

No

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: By Implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

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?

ePermits: Permittee information collected is used to track special forest product sales and to enforce the rules that come with the privilege of removing forest products from the forests. Law enforcement is responsible for monitoring and enforcing the rules associated with issuance of these permits. The permit forms are considered a short-form contract so come with legal obligations to monitor and be accountable for the products via the permits and the rules expressed on them.

CIAO: This information is used in escalating procedure should the personnel become missing, injured or otherwise fail to "check in".

Huckleberry: This information is used to allow members of the public the ability to obtain free-use permits to harvest Huckleberries and Mushrooms in the Gifford Pinchot National Forest.

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

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

Follow the format below:

Privacy Risk: Unauthorized access and use of PII.

Mitigation: PII access is controlled by role-based security which requires two factor authentication. All PII is encrypted in transit and at rest. PII is never shared or disclosed without proper security review and authorization.

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?

FS SN Privacy Impact Analysis (PIA) on the USDA PIA website.

The Federal register for SORN's and legal authorities

FS specific SORNs are also published on FS websites

Forms are approved through OMB for the Paperwork Reduction Act (also cited in the Federal Register) and they cite the privacy information act.

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

ePermits - Individuals may opt out of purchasing a permit at any time before payment. Once payment is made, the permit becomes a record that is required by NARA to be saved for 30 years.

CIAO: Users enter the information voluntarily.

Huckleberry: Individuals may opt out, however if they do decline, they will not receive the permit requested.

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.

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.

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?

All information gathered and printed on the 2400-1 form is retained by FS electronically for 30 years, as required by NARA retention schedule.

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.

2400-1 Permits are retained according to Timber Permits retention schedule #N1-95-88-2
(2450-4)

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.

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.

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?

Personal information will not be shared with other internal organizations or systems.

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

Follow the format below:

Privacy Risk: Privacy risks associated with internal sharing and disclosure include:
Unauthorized Access: Employees may access PII without proper clearance, leading to potential misuse.

Data Breaches: Internal systems can be vulnerable to breaches, compromising PII.

Insider Threats: Employees with malicious intent may exploit their access to PII for personal gain.

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.

Access Controls: Implement role-based access controls to limit who can access PII based on their job responsibilities.

Encryption: Use encryption for data in transit and at rest to protect PII from unauthorized access.

Regular Training: Provide ongoing training for employees on data privacy policies, the importance of protecting PII, and how to handle it securely.

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?

None

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

Follow the format below:

Privacy Risk: There are NO external sharing organizations. Privacy Risk is N/A.

Mitigation: There are NO external sharing organizations. Mitigation is N/A.

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 seeking access to records contained in this system of records, or seeking to contest content, may submit a request in writing to the Forest Service FOIA/Privacy Act Officer (contact information at https:// www.dm.usda.gov/foia/poc.htm). The request should include a daytime phone number and email. Provide as much information as possible about the subject matter of the records you are requesting.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the Forest Service FOIA/Privacy Act Officer (contact information at https:// www.dm.usda.gov/foia/poc.htm). Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate. Records are not stored except for within the permit itself. Individuals with permits can contact local offices for assistance to change inaccurate information.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the Forest Service FOIA/Privacy Act Officer (contact information at https:// www.dm.usda.gov/foia/poc.htm). Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate. Records are not stored except for within the permit itself. Individuals with permits can contact local offices for assistance to change inaccurate information.

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

Users are guided to their local FS offices with any issues or questions in a number of places throughout the permit-purchasing experience

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.

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?

The system protects PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. System data is secured in database using column level encryption.

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

The system uses role-based security based on separation of duties and least privileged access model. Roles are determined and granted by an authoritative person based on operational, and business needs of the user. Knowledge Management documentation outlines procedures that determine which users access the program.

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

There are no significant risks associated with the internal sharing of PII data. All personnel accessing FS SN PII data are cleared and trained annually on the proper handling and protection of PII data. The system itself is protected by role-based access layers and positive identification techniques such as multi-factor authentication to ensure only people authorized to view and act upon information about others can do so

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

System users are required to take the Annual Information Security Awareness Training Course and Rules of Behavior. Privileged system users are required to take the Role-based security training annually. The training includes PII security section.

Information Security Awareness (ISA) and Role-Based Security Training (RBST) are required at the levels appropriate.

Approval Signatures:

____

Zahid Chaudhry
System Owner
United States Department of Agriculture

____

Benjamin Moreau
Assistant Chief Information Security Officer (ACISO)/Privacy Officer
Natural Resources and Environment, Forest Service
United States Department of Agriculture

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.06.08 17:42:11 -04'00'

____

Office Of the Chief Privacy Officer
United States Department of Agriculture