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:

Forest Service Recreation One Stop (FS R1s)

Natural Resources and Environment

Forest Service

Date PIA submitted for review:

5/13/2025

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Benjamin Moreau	Benjamin.moreau@usda.gov	Unlisted
Information System Security Manager	Tasha Middleton	tasha.middleton@usda.gov	816-708-8310
System/Program Managers	Ashley Schoemer	Ashley.Schoemer@usda.gov	720-501-8725

Abstract

The Forest Service Recreation One Stop (FS R1s) system stands as a pioneering advancement in the realm of recreation reservation services, serving as a cornerstone utilized by 14 federal agencies. Its core function encompasses a comprehensive suite of reservation and business management tools, streamlining the administration of thousands of individual federal recreation locations and activities.

This Privacy Impact Assessment (PIA) is necessary due to the system's collection of Personally Identifiable Information (PII) from the public during reservation transactions. The Recreation.gov platform, a publicly accessible Software as a Service (SaaS) solution for reservations, trip planning, and information exchange, facilitates transactions for participating agencies that make reservations available through the service. The platform is overseen by the interagency Recreation One Stop Program Management Office (R1s PMO) under a Memorandum of Understanding. The platform's contracting and financial management responsibilities, including the Authorization to Operate (ATO) processes and associated IT security requirements, are centralized and spearheaded by the USDA/Natural Resource and Environment (NRE) /Forest Service.

The platform's development and support are governed by a performance-based support services contract with the Service Provider ensuring compliance with contractual obligations. Ownership of federal facility and reservation data within the platform rests with the Forest Service and participating agencies.

Overview

The Forest Service Recreation One Stop system is the data maintained in Recreation.gov, a one-stop shop for trip planning, information sharing and reservations as a SaaS solution. There are a total of 14 federal Participating Partners providing this service to the public. Nine of these partner agencies offer reservations, including the Army Corps of Engineers, Forest Service, National Park Service, Bureau of Land Management, Bureau of Reclamation, Fish and Wildlife Service, National Archives Records Administration, Presidio Trust, and the Naval District Washington.

Recreation.gov is used for:

- Making reservations for recreational activities on federal lands and waters and at federal facilities, online, by-phone, or in the field.
- Discovering recreation opportunities managed by federal agencies at parks, forests, lakes, museums, and other areas near designated locations.

The Recreation.gov SaaS provides for comprehensive web services, database management, and customer support. Recreation.gov hosts a range of sites that allow visitors to make reservations, such as reserving a campsite, securing a whitewater rafting permit, scheduling a ranger-led cave tour, and many others. Customers can use trip-planning tools to discover federal recreation sites and opportunities. If they need help, contact center agents offer assistance over the telephone, through live chat, or by e-mail. The solution also includes integrated physical hardware to allow users to make reservations and payments in person at federal facilities.

From a system perspective, FS R1s contains:

- Information about facilities, recreational activities, booking rules, and communications provided by federal agencies that participate in R1s.
- Information provided by the general public in the process of utilizing the services provided, such as user accounts, reservation details, and contact information.

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?

The collection of information within FS R1s is defined by specific legal authorities, arrangements, and agreements. These include but are not limited to:

- Interagency Agreements are held with the National Park Service and the Army Corps of Engineers
- Memoranda of Understanding are established with Army Corps of Engineers, National Park Service, Bureau of Land Management, Bureau of Reclamation, Fish and Wildlife Service, National Archives Records Administration, Presidio Trust, and the Naval District Washington.

  The nine federal agencies that participate in the Recreation One Stop program through a MOU have equal access, interests, and rights in the R1s data and the Recreation.gov system. However, access is controlled so that each participating agency may only access reservations and associated information for lands and activities managed by that participating agency.

- The Federal Lands Recreation Enhancement Act, 16 U.S.C. 6801–6814
- The Organic Act of 1897, (16 U.S.C. 473–478, 479–482, 551)
- Term Permit Act of 1915. (38 Stat. 1101, as amended, 16 U.S.C. 497);
- Multiple Use Sustained Yield Act of June 12, 1960 (74 Stat. 215, as amended; 16 U.S.C. 528–531);
- 1964 Wilderness Act (16 U.S.C. 1131– 1136);
- The National Historic Preservation Act of 1966. (Pub. L. 89– 665; 80 Stat. 915, 16 U.S.C. 470 et seq.);
- Land and Water Conservation Fund (L&WCF) Act of 1965, as amended (Pub. L. 93–303, June 7, 1974; 78 Stat. 897, as amended; 16 U.S.C. 460l (4) to 460l (11m);

- 23 U.S.C. 120 (note), Omnibus Budget Reconciliation Act of August 10, 1993 (Pub. L. 103–66, 107 Stat. 312)

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

Yes, ATO Date 4/26/24

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

USDA/FS-55 National Recreation Reservation System

https://www.fs.usda.gov/about-agency/foia/privacyact

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

Yes, OMB Control # 0503-0024

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)	□	Gender	☒	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	□	Sexual Orientation	□	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 information in the system/program?

Users of the system, including members of the public, are the primary source of information in the system. However, it's important to note that some personnel play a role in helping create accounts. These may include USDA employees, contractors, or others working on behalf of USDA, as well as Non-USDA Federal Government employees and USDA partners. The system gathers information directly from users and there are no data sourcing or data brokers involved with the collection of information.

2.2.1. How is the information collected?

1. **Direct Input by the Public Online:** Members of the general public can input their information directly into the system through the website when making reservations or using online services.
2. **Federal Personnel:** Federal personnel may enter data into the system when managing reservations or performing other tasks related to the operation of reservable facilities.
3. **Non-Federal Personnel** (Contractors, Partners, etc.): Non-federal personnel, such as contractors, concessionaires, or partners who have authorization to participate in the management of federal recreation facilities, may also input data into the system. This can include managing reservations, maintaining facility records, or providing customer support through call center agents.
4. **Call Center Agents:** Information may also be collected over the phone through call center agents, who could be federal employees or contracted staff, depending on the operational setup.

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

FS R1S uses commercial or publicly available data to enhance user experience, optimize operations, and improve decision-making processes. This includes integrating weather patterns, local events, and tourist attractions for comprehensive information. Commercial or publicly available data is not combined with Recreation.gov data for individual user analysis.

.

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

The system uses a combination of procedural checks and technical solutions to ensure accuracy. The system performs automated checks to validate certain data elements, such as confirming that email addresses adhere to standard formats and that phone numbers are in the recognized US 10-digit format. This serves as an initial validation step to ensure basic data integrity. Call center agents are trained to check and confirm verbal information provided over the phone. Federal staff managing recreational activities also confirm user information in the normal course of their operational duties.

Data Cleansing and Standardization:

The system performs automated checks to validate certain data elements, such as confirming that email addresses adhere to standard formats and that phone numbers are in the recognized US 10-digit format.

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

Yes

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

The agency employs third-party websites and/or applications to centralize federal recreation information and reservation services into one consolidated platform. By leveraging external platforms, it aims to streamline access to recreational resources, information, and reservation services, providing users with a unified and convenient experience. This approach ensures that users can effortlessly discover, plan, and book recreational activities across various federal lands and facilities through a single, user-friendly interface.

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

1. User Account Information: This may include names, email addresses, usernames, passwords, and other account credentials used for registration and authentication purposes.
2. Contact Information: Users may provide or access contact details such as mailing addresses, phone numbers, and email addresses for communication purposes or reservation confirmations.
3. Payment Information: users may input or access payment details such as credit card numbers, billing addresses, and payment transaction history. No credit card information is stored in the system.
4. Booking Details: Information related to reservations or bookings made through the platform, including dates, times, locations, and preferences for recreational activities or accommodations.
5. Usage Data: The platform may collect data on users' interactions, behaviors, preferences, and activities within the application or website, which may include IP addresses, device identifiers, browsing history, and usage patterns.

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

Follow the format below:

Privacy Risk: Unauthorized collection and storage of PII.
Mitigation:

To safeguard against unauthorized collection and storage of PII, the FS R1s system incorporates robust protective measures. These include a multi-layered defense strategy, beginning with a Content Delivery Network (CDN) fortified with distributed Web Application Firewall (WAF) to shield against external threats. Moreover, internal defenses consist of local firewalls equipped with Intrusion Prevention Systems (IPS) and an additional WAF module, coupled with instance-level firewalls and stringent application coding standards aimed at thwarting malicious attacks.

Prior to deployment, rigorous testing procedures are enforced to scrutinize system integrity, ensuring that vulnerabilities are promptly identified and rectified before production release. Also, PII data is strictly prohibited from test environments, lessening the risk of accidental exposure.
Internal access to the system is controlled, and multi factor authentication will deter unauthorized entry. While a select few administrators possess access privileges in development and test environments, none are granted access to the production database without explicit managerial approval. Access requests trigger an authorization process, involving firewall rule updates and credential verification.

Further, data is encrypted, making the database impervious to unauthorized restoration attempts from backups or snapshots.

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?

The PII information in the system is strictly utilized for reservation management, reservation or trip-planning related communication and notification, analytics and reporting, compliance, and legal requirements, maintaining and honoring reservations, troubleshooting reservation issues, sending refund checks, and enforcing location-specific business rules.

Disassociated elements of reservation information such as zip codes without names, street addresses, emails, and/or phone numbers may be used by participating agencies to undertake research activities that are OMB-approved under the Paperwork Reduction Act and that are studying or asking for specific feedback related to managing recreational activities on federal lands.

De-identified information on reservations is made available to the public through annual text-based data files available on the Recreation.gov website and through Application Programming Interfaces (APIs). The information shared publicly is aggregated and de-identified so that no PII is available or delivered.

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 creates reports but does not appear to conduct predictive analyses and anomalies.

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

Follow the format below:

Privacy Risk: Unauthorized access and use of PII.
Mitigation:

- All access and actions within the FS R1s production database are logged. This ensures accountability and traceability in case of unauthorized access or suspicious activities.

- Encryption of data when it is in transit (using https and other secure encryption transmission protocols) reduces the risk of the data being compromised during a customer's interactions with the system.

- Encryption of the database prevents unauthorized backup and restoration, adding an extra layer of security to protect the data even if the physical storage medium is compromised.

- Strict access controls are implemented, requiring all users to acknowledge the rules of behavior form before gaining access. This ensures that only authorized personnel can access the system and its data.

- User attestation is a crucial method to prevent unauthorized access to the FS R1s system, complementing existing access controls. It verifies the identity and permissions of individuals accessing the system, using methods like regular password updates (every 90 days), and quarterly reviews of user access privileges. This proactive approach not only enhances privacy protections but also helps detect and address anomalies or suspicious activities, strengthening the security posture of the FS R1s system.

- Distribution of the FS R1s Information Security Policies and Procedures document reinforces the importance of access control and acceptable usage policies among all personnel. This document serves as a guide outlining the protocols and best practices for handling sensitive information and helping to reduce the likelihood of unauthorized access incidents.

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 prior to the collection of information within Recreation.gov. According to the System of Records Notice (SORN) provided, individuals covered by the system include members of the public who register online to receive information about the program or make advanced reservations for recreation opportunities on Federal lands and waters. By registering online for information or making advanced reservations, individuals are presented with information regarding the collection of their data and given the opportunity to consent to its use in accordance with applicable privacy laws and regulations. The banner states "By logging in, I accept Recreation.gov's Terms of Use and Privacy Policy."

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

Individuals have the opportunity and/or right to decline to provide information when using R1s. As per the System of Records Notice (SORN) provided, individuals voluntarily register online to receive information or make advanced reservations for recreation opportunities on Federal lands. This indicates that participation in the system is generally optional, and individuals can choose whether to provide their personally identifiable information (PII) during the registration process.
By presenting information about the program and its associated data collection practices prior to registration, individuals are likely given the opportunity to make an informed decision regarding the provision of their information. If individuals decide not to provide their information, they may still be able to access certain features or information within the system, depending on its functionality and the nature of their interaction with the platform.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

Privacy Risk: Improper notice of collection, use, dissemination, and maintenance of PII. Usage of PII not limited to declaration provided to the user.

Mitigation:

1. Privacy Policy: FS R1s has a dedicated privacy policy accessible from the main page of the website. The policy outlines the commitment to protecting users' personal information and applies solely to transactions made and data gathered on the Recreation.gov website. Users are encouraged to review the privacy policy periodically as it may be updated from time to time. By visiting the site or providing information, users are deemed to accept the practices described in the privacy policy at that time.

2. Non-Sharing Policy: FS R1s does not release personal information, credit card, or financial information for use by other agencies or third party. Transactional information communicated between customers and the website is transmitted in an encrypted format for privacy and security purposes. Credit card information passes through a highly secure computing environment.

3. Account Deletion Policy: Users of FS R1s have the right to delete their accounts at any time, except when there are current or future reservations tied to their account. Upon account deletion, certain personal information, including first and last name, address (excluding zip code), email, password,

and phone numbers, is removed from account records. However, zip code information is maintained for location usage purposes. Personal information associated with individual reservations is preserved according to applicable Forest Service policies. Refunds for reservations previously associated with a deleted account will still be processed normally. Users can sign up again with the same or a different email, but reservations from a deleted account cannot be re-associated with a new account.

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?

In accordance with standard privacy policies, the retention period for information on our reservation site varies based on activity and specific circumstances. Active customer profiles are maintained for as long as they remain active within the system. An active profile is defined as one that has been accessed or used within a recent timeframe. Accounts are not deleted unless the account owner deletes their profile.

It's important to note that active profiles are retained indefinitely in the system, especially considering the nature of our service where many individuals may utilize the reservation system over extended periods of time. Alternatively, customers can remove their information from the system.

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.

Yes. Records 2300- Recreation, Wilderness and Related Resource Management and 2450- Timber Sale Permits. The FSH 6209.11- Records Management Handbook link is copied below:

https://www.fs.usda.gov/cgi-bin/Directives/get_dirs/fsh?6209.11

A routine evaluation procedure, typically conducted every 5 years, is in place to reevaluate the duration for retaining records in accordance with NARA guidelines and any changes in regulatory mandates or organizational demands. Additionally, it's important to note that NARA retention periods will be subject to review whenever a new reservation type is introduced into the system, ensuring ongoing compliance with regulatory standards.

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

Follow the format below:

Privacy Risk: Improper disposition and retention of PII accordance to regulatory guidance.
Mitigation: The risks associated with the length of time data is retained include:

1. Increased Exposure to Data Breaches: The longer data is retained, the greater the exposure to potential data breaches, unauthorized access, or malicious activities.
2. Privacy Concerns: Extended retention periods may pose privacy concerns, especially if personally identifiable information (PII) is stored for prolonged durations, increasing the risk of unauthorized disclosure or misuse.
3. Compliance Risks: Retention periods that exceed regulatory requirements or industry standards may result in non-compliance with data protection laws and regulations, leading to legal consequences and penalties.
4. Operational Burden: Managing and securing data over extended retention periods can be operationally burdensome, requiring additional resources and efforts to maintain data integrity and security.

To mitigate these risks, the FS R1s implements several measures:

1. Layered Data Protection: The database employs multiple layers of protection, including authentication mechanisms, strong passwords, and restricted access controls for internal users.
2. Restricted Access: Access to the production database is restricted to a small number of privileged users who must receive approval from management before accessing it.
3. Encryption: The database is encrypted, preventing unauthorized access or inadvertent restoration from backups or snapshots.
4. Limited Retention Scope for Christmas Tree Permits: While the retention period for Christmas Tree permits is longer (30 years), the reservation site mitigates this risk by implementing robust security measures to protect the stored data. Additionally, the actual data available for Christmas Tree permits is limited to records dating back to November 2020, reducing the exposure of PII information.

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?

Information is not routinely shared with any organizations outside of the Forest Service, but still within the Department of Agriculture. However, information is shared with FOIA Officers and the USDA Office of General Counsel when appropriate and required in responding to specific FOIA requests, lawsuits, or legal concerns.

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

Follow the format below:

Privacy Risk: Unauthorized disclosure and unsecured transmission of PII.

Mitigation: Information sharing is minimized to the extent possible. Ad hoc sharing of information with the service provider requires approval from leadership on both sides for awareness and oversight. Site operators do not have database permissions and it’s against policy to casually review, copy, or manipulate customer data. All operations are logged for future review. Routine sharing of data is codified into the application to meet customer requirements.

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?

All information shared with FS employees with appropriate access is also shared with employees with appropriate access at the other eight federal agencies that are party to the Recreation One Stop MOU. This includes, among other information, PII, reservations, trip planning details, facility availability, and visitor usage statistics. These agencies include:

- Army Corps of Engineers
- National Park Service
- Bureau of Land Management
- Bureau of Reclamation
- Fish and Wildlife Service
- Presidio Trust
- Naval District of Washington
- National Archives and Records Administration

Purpose of Information Sharing: The nine federal agencies that participate in the Recreation One Stop program through an interagency MOU have equal access, interests, and rights in the R1s data and the Recreation.gov system. However, access is controlled so that each agency may only access reservations and associated information for lands and activities managed by that agency. The sharing of data facilitates collaboration among these agencies responsible for managing public lands and recreational resources. It supports the improvement of reservation processes, enhances visitor experiences, and enables better resource management across federal sites.

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

Follow the format below:

Privacy Risk: Unauthorized access, data breaches, and potential misuse of personal data by external entities.

Mitigation: These risks have been identified and effectively mitigated through several measures:

1. Limited Access and Role-Based Permissions: Access to shared information is strictly controlled, with role-based permissions enforced to ensure that only authorized individuals within participating agencies have access. This minimizes the risk of unauthorized access and ensures that only those with a legitimate need can view the information.

2. Encryption of Shared Data: All shared data, particularly personally identifiable information (PII), is fully encrypted during transmission and at rest. Encryption adds an additional layer of

security, making it extremely difficult for unauthorized parties to intercept or decipher the transmitted data.

3. Secure Transmission Protocols: Information is transmitted using secure protocols and channels to safeguard its integrity and confidentiality during transit. This includes the use of encrypted communication channels and adherence to industry-standard security protocols.

4. Auditing and Monitoring: All instances of data transmission outside the Department are logged and regularly audited to detect any unauthorized access or suspicious activities. Continuous monitoring helps in identifying and addressing potential security breaches in a timely manner.

5. Compliance with Privacy Regulations: The sharing of information complies with the requirements of the Privacy Act of 1974 and other relevant privacy regulations. This ensures that data sharing activities are conducted in a manner that respects individuals' privacy rights and protects their personal information from unauthorized use or disclosure.

The identified privacy risks associated with external sharing of information are effectively mitigated, providing assurance that individuals' data is handled securely and in accordance with applicable privacy laws and policies.

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?

Users can update their information by securely logging into their FS R1s user accounts using the established username and password process, where they can access features like profile editing, data download options and transparent data access policies.

1. Logging into User Accounts: Users are required to log into their FS R1s user accounts.
2. Secure Authentication: The established username and password process ensures secure authentication.
3. Profile Editing: Users can update their information through profile editing features.
4. Data Download Options: Users have the option to download their data.
5. Transparent Data Access Policies: Clear policies are in place regarding how users can access their data.

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

The procedures for correcting inaccurate or erroneous information in the FS R1s system involve users taking responsibility for maintaining their Personally Identifiable Information (PII), as it is user-provided and user-maintained, with neither the Government nor the service provider (BAH) checking it for errors outside of the financial transaction processing workflow. However, within the transaction processing workflow, validation protocols are integrated to guarantee the precision of data throughout transactions.

1. Data Format Validation: Checking that data entered conforms to the specified format (e.g., date format, numerical values).
2. Range Validation: Verifying that values fall within acceptable ranges (e.g., ensuring a transaction amount is within a valid monetary range).
3. Duplicate Checking: Identifying and preventing duplicate entries to maintain data integrity.

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

Individuals are informed of the procedures for correcting their information through clear guidelines provided within the FS R1s system. Users are responsible for maintaining their own data and instructions on how to update or correct information are readily available within the platform's documentation and user interface. Also, there are Help Center articles that clarify how users can manage or correct their PII information, and users are able to use the Contact Center for assistance if they have difficulties with the self-service options.

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

Individuals have the alternative option of updating their Personally Identifiable Information (PII) at their own discretion, as users retain the autonomy to modify their PII whenever necessary.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk: Unauthorized Access, unintentional or intentional data integrity issues, identity theft

Mitigation: To mitigate the risks associated with updating Personally Identifiable Information (PII), FS RIs implemented the following measures:

1. Enhanced Authentication: Implementing strong authentication methods to ensure only authorized users can access and update their PII.

2. Encryption: Employing encryption techniques to protect PII both in transit and at rest, reducing the risk of unauthorized access in case of a breach.

3. Access Controls: Enforcing strict access controls to limit access to PII, ensuring only authorized personnel can view or modify sensitive information.

4. User Education: Providing end users with help center information and guidelines on best practices for updating PII, emphasizing the importance of accuracy and security in maintaining personal data. Providing Call Center Agents training for handling end users PII.

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?

Access to the system requires users to authenticate and be authorized to access the respective system. 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?

Access control within the system is facilitated through role-based permissions, ensuring that users only have access to the information necessary for their specific roles. External users, such as those making reservations, can create and manage their accounts but are restricted from accessing any Personally Identifiable Information (PII) beyond their own.

Internal users, including Government employees, Service Provider Contractors, and Concessionaires, are granted access to PII relevant to their daily responsibilities. Role-based permissions are structured hierarchically and are managed, assigned, and revoked at levels above individual users. Additionally, privilege and non-privilege attestation procedures play a role in maintaining the security and integrity of user access permissions.

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

There are no plans to share PII beyond that required to execute the business operations of the participating agencies, such as, honoring campground reservations, providing will call tickets or field validation of backcountry hiking permits.

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

For Forest Service (FS) employees, privacy training is conducted in alignment with federal regulations and organizational policies. This training encompasses educating users on the proper handling and safeguarding of Personally Identifiable Information (PII).

For Service Provider employees, privileged users undergo PII handling training as part of their onboarding process and annual security training. This training includes specific modules on privacy tailored to their roles and responsibilities within the program or system.

For other contractors, cooperators, and concessionaire personnel, concessionaires are private businesses or individuals authorized by managing authorities, like federal agencies or park services, to operate facilities or provide services within recreational areas. In the statement above, concessionaires refer to these authorized entities who manage amenities such as campgrounds, lodges, and restaurants within national parks, forests, or public lands. Before accessing the system, concessionaire personnel must acknowledge the FS R1s Rules of Behavior, which includes guidelines on PII handling and privacy. However, their specific PII training requirements are managed and enforced through concessionaire contracts/agreements with the relevant agency, rather than being directly overseen by the FS R1s program.

Approval Signatures:

ASHLEY SCHOEMER Digitally signed by ASHLEY SCHOEMER Date: 2025.06.18 10:21:17 -06'00'

Ashley Schoemer
System Owner (SO)
Recreation, Heritage & Volunteer Resources, Forest Service
United States Department of Agriculture

BENJAMIN MOREAU Digitally signed by BENJAMIN MOREAU Date: 2025.06.23 11:31:18 -04'00'

Benjamin Moreau
Acting Privacy Officer (PO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

BENJAMIN MOREAU Digitally signed by BENJAMIN MOREAU Date: 2025.06.23 11:31:37 -04'00'

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

TRACY HENDRIX Digitally signed by TRACY HENDRIX Date: 2025.06.17 19:42:46 -04'00'

Office of the Chief Privacy Officer
United States Department of Agriculture