Privacy Impact Assessment

for

Forest Service Recreation One Stop (FS R1s)

Policy, E-Government and Fair Information Practices

Version: 1.4

Date: October 12, 2023

Prepared for: USDA FS CIO

USDA

United States Department of Agriculture

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.

Privacy Impact Assessment for the USDA IT System/Project:

Forest Service Recreation One Stop (FS R1s)

Policy, E-Government and Fair Information Practices

Date PIA submitted for review:

October 12, 2023

Mission Area System/Program Contacts:

Mission Area Privacy Officer:
Cynthia Ebersohn
Cynthia.ebersohn@usda.gov
386-301-4060

Information System Security Manager:
Ellen Shaw
Ellen.shaw@usda.gov
202-697-1728

System/Program Manager:
Benjamin Moreau
Benjamin.Moreau@usda.gov
202-380-6165

Abstract

The abstract provides the simplest explanation for the "what does the system do?" and will be published online to accompany the PIA link.

The Forest Service Recreation One Stop (FS R1S) system represents an evolutionary leap forward in the recreation reservation services utilized by more than 12 participating federal agencies. FS R1S provides a full suite of reservation and business management tools to manage more than 107,000 individual federal recreation locations and activities. This PIA is being conducted because the system will collect PII from the public in the process of making and paying for reservation transactions.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

The system name FS Recreation One Stop (R1s) and it is a cloud-based Software as a Service (SaaS) travel planning system managed by the USDA Forest Service by the Director of Recreation, Heritage and Volunteer Resources.

The purpose of FS R1s is to provide an interagency program with a full suite of recreation reservation and business management tools. FS R1s is employed by over 3,700 federal recreation facilities to manage more than 107,000 recreation locations and activities across more than 12 participating federal agencies.

It is essential to understand that the FS R1s information system is developed, owned, hosted, operated and maintained by Booz Allen Hamilton (BAH), the SaaS vendor of recreation.gov. The Forest Service is simply procuring the services provided by this SaaS solution. The data that is specific to the customer (Forest Service) instance of Recreation.gov, is a part of the R1s boundary, not the Recreation.gov boundary. No infrastructure, hardware, firmware or software component of this SaaS solution resides within federal IT infrastructure. The single aspect of this SaaS solution owned by the Federal Government is the data produced, processed, and contained within the system.

Booz Allen Hamilton was selected as the service provider by an interagency selection panel through a competitive source selection process conducted over a 4-year period.

All information contained within FS R1s is government-owned. FS R1s collects information from private citizens worldwide who conduct transactions on the system. The information collected is limited to only that information required to both conduct the transaction and enforce any unique business rules mandated by a recreation location's approved management plan. This information is classified as PII and protected accordingly. Such information includes items such as the customer's full name, billing address and phone number.

All PII information contained in the system is fully encrypted while at rest and only accessible by those select personnel with the required role-based permissions to do so. Such role-based permissions required to access PII within the system are only granted to those customer service personnel with the need to access, modify and cancel reservations, as well as those field personnel who will require access to the PII in order to verify customer reservations and verify information in order to enforce unique business rules.

Information collected to enforce unique business rules may vary depending on the nature of the rule being enforced, for example: vehicle license plate numbers (for OHV permits), drivers' license numbers (for OHV permits), alternate trip leader's name and address (for river rafting & backcountry camping permits), emergency contact information (wide variety of permits), etc. Collection of this type of information occurs under the FS R1s system.

A typical transaction on the system involves an external customer using the www.recreation.gov website to search for recreation opportunities and making a reservation, purchasing tickets, or entering a lottery. The checkout workflow requires the user to log into the system using their username and password, enter the required payment & contact information and enter any unique information required for enforcement of inventory-specific business rules. The payment processing module is compliant with all relevant U. S. Department of Treasury and Payment Card Industry (PCI) security requirements for the protection of financial and PII data. Payment data is not retained; only the payment approval status provided by the payment processing module.

Information sharing includes PII that can be accessed by the receiving facility managing incoming reservations (e.g., the campground manager will have access to report for his/her specific campground so they know who will be arriving for each site). The user enters their own payment information directly into the Third-Party Entity (TPE) system without traversing the Recreation.gov system using iframe technology. An "iframe" (short for "inline frame") is a technology used in web development to embed one web page within another. It's like a window or frame that allows you to display content from another website or web application within the context of the current page you're viewing. This can be useful for integrating content from different sources into a single webpage. At no time is PII, including payment information, exchanged between Recreation.gov and TPE. Once authorization for payment is complete, TPE sends a payment status of "successful" or "unsuccessful" to Recreation.gov. There is no access to the TPE database by anyone in FS, USDA, or contractors supporting Recreation.gov.

In addition to the public facing aspect of the services, there is an internal component accessible by federal recreation managers and authorized concessionaires offering a full suite of tools to manage recreation inventory at their facilities, track and report on usage and financial metrics, manage site personnel access to FS R1s internal functions, and provide a wide range of customer service functions while in the field.

Authority to operate a consolidated interagency reservation service is derived from The Federal Lands Recreation Enhancement Act (FLREA) of 2005; 16 U.S.C. § 87.

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?

Authority to operate a consolidated interagency reservation service is derived from The Federal Lands Recreation Enhancement Act (FLREA) of 2005; 16 U.S.C. § 87.

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

Yes

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

N/A

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

Yes

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 the information in the system/program?

The primary source of information is from the of general public. However USDA employees, contractors, other entities working on behalf of USDA, non-USDA Federal Government employees, and/or USDA partners may aide the general public in creating their accounts.

2.2.1. How is the information collected?

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.

Federal Personnel: Federal personnel may enter data into the system when managing reservations or performing other tasks related to the operation of reservable facilities.

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.

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?

The system does not utilize commercial or publicly available data sources to supplement the personally identifiable information (PII) collected from users. Instead, it primarily relies on the PII directly entered by individuals during their interactions with the system. This data is used exclusively for the purposes of conducting transactions, maintaining reservations, enforcing location-specific business rules, and generating anonymized metrics for informed decision-making. The system does not augment its PII dataset with external sources of information accessible to the general public, and all data collected is based on user-provided information.

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

Data Validation Rules: Implementing robust data validation rules within the system to check for accuracy and consistency. While the system already verifies email and phone number formats, consider expanding these rules to validate other data fields. For instance, you can use regular expressions or pattern matching to ensure that names, addresses, and other PII elements adhere to expected formats.

Real-Time Error Checking: Incorporating real-time error checking during data entry. As users input information, the system can provide immediate feedback if there are potential discrepancies or inaccuracies. This can include flagging potential misspellings, incorrect formatting, or inconsistent data.

Duplicate Detection: Implementing mechanisms to detect and prevent the creation of duplicate records. Duplication can lead to inaccurate data and potential privacy issues. Utilize algorithms and fuzzy matching techniques to identify and merge duplicate records.

Data Profiling and Quality Assessment: Periodically run data profiling and quality assessment processes. These tools can analyze the data to identify inconsistencies, outliers, and potential errors. Regular reports can be generated to highlight data quality issues for review and correction.

User Authentication and Verification: Strengthen user authentication and verification procedures. Implement multi-factor authentication (MFA) to ensure that users are who they claim to be. Additionally, consider incorporating identity verification methods, such as sending confirmation codes to registered email addresses or phone numbers.

Data Quality Dashboards: Create data quality dashboards or reports that provide an overview of data accuracy and integrity. This allows administrators and data stewards to monitor data quality in real time and take corrective actions as needed.

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 purpose is to provide one single consolidated location for federal recreation information and reservation services through Recreation.gov.

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

At a minimum; name, address, phone number(s), e-mail addresses, credit card number, expiration date, CCV code. Additional information is needed to enforce certain business rules and will be collected when applicable will include; driver's license number, license plate and state, vehicle identification number, and date of birth.

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

Follow the format below:

Privacy Risk:

Unauthorized Access: The collection of sensitive PII, including names, birthdates, addresses, and personal identification numbers, presents a risk of unauthorized access by malicious actors or individuals with malicious intent.

Data Breaches: Storing a substantial amount of personal data increases the risk of data breaches, which could lead to the exposure of sensitive information and potential harm to individuals.

Data Leakage: Inadvertent data leakage, whether due to system vulnerabilities or human error, is a significant privacy risk. Accidental exposure of PII can result in privacy violations.

Mitigation:

Access Logging: The logging of all access and actions performed in the database helps mitigate the risk of unauthorized access. This allows for monitoring and audit trails, enabling the detection of any suspicious activities.

Data Encryption: Database encryption is a crucial measure to protect against unauthorized backup and restoration. It ensures that even if unauthorized access occurs, the data remains unreadable and inaccessible without the encryption keys.

Access Controls: Implement robust access controls to restrict access to the database. Only authorized personnel should have access to sensitive PII. Role-based access controls and authentication mechanisms, like multi-factor authentication (MFA), can help enforce this.

Data Minimization: Collect and retain only the minimum necessary data required for the intended purposes. By minimizing data storage, you reduce the volume of sensitive information that could be at risk in the event of a breach.

Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the system's defenses. Proactively addressing vulnerabilities helps reduce the risk of data breaches.

Data Loss Prevention (DLP): Implementing DLP tools and policies to detect and prevent data leakage. DLP solutions can monitor data flows and enforce policies to prevent unauthorized data transfers or sharing.

Incident Response Plan: Develop a comprehensive incident response plan that outlines the steps to take in the event of a data breach. This includes notifying affected individuals and relevant authorities promptly

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?

Financial Transaction: The primary use of personally identifiable information (PII) entered into the system is for conducting financial transactions. This includes processing payments related to reservations, ticket purchases, or other financial activities. The system may collect information such as credit card numbers or payment authorization status to facilitate these transactions.

Reservation Maintenance: PII is utilized to maintain and honor reservations made by customers. This includes ensuring that individuals have access to the reserved services or facilities at the specified times and locations. Reservation details, including customer names and contact information, are used to manage and confirm bookings.

Enforcing Location-Specific Business Rules: PII may be used to enforce location-specific business rules. This can include verifying the eligibility of individuals for certain services or ensuring compliance with regulations related to federal recreation locations and activities. For example, the system may use PII to validate that visitors meet age or residency requirements.

Data Analysis and Metrics: Disassociated elements of PII, such as zip codes without specific names, street addresses, or phone numbers, may be used in aggregate or anonymized forms to develop relevant metrics. These metrics provide insights into user demographics, preferences, and behaviors without disclosing individual identities. Managers can use this information to make informed business decisions, optimize resource allocation, and improve visitor experiences.

While the system may collect certain financial data for transaction processing (e.g., credit card details), it does not retain this sensitive information beyond what is necessary for the immediate financial transaction.

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: The collection of sensitive PII, including names, birthdates, addresses, and personal identification numbers, presents a risk of unauthorized access by malicious actors or individuals with malicious intent.

Data Breaches: Storing a substantial amount of personal data increases the risk of data breaches, which could lead to the exposure of sensitive information and potential harm to individuals.

Data Leakage: Inadvertent data leakage, whether due to system vulnerabilities or human error, is a significant privacy risk. Accidental exposure of PII can result in privacy violations.

Mitigation:

Access Logging: The logging of all access and actions performed in the database helps mitigate the risk of unauthorized access. This allows for monitoring and audit trails, enabling the detection of any suspicious activities.

Data Encryption: Database encryption is a crucial measure to protect against unauthorized backup and restoration. It ensures that even if unauthorized access occurs, the data remains unreadable and inaccessible without the encryption keys.

Access Controls: Implement robust access controls to restrict access to the database. Only authorized personnel should have access to sensitive PII. Role-based access controls and authentication mechanisms, like multi-factor authentication (MFA), can help enforce this.

Data Minimization: Collect and retain only the minimum necessary data required for the intended purposes. By minimizing data storage, you reduce the volume of sensitive information that could be at risk in the event of a breach.

Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the system's defenses. Proactively addressing vulnerabilities helps reduce the risk of data breaches.

Data Loss Prevention (DLP): Implementing DLP tools and policies to detect and prevent data leakage. DLP solutions can monitor data flows and enforce policies to prevent unauthorized data transfers or sharing.

Incident Response Plan: Develop a comprehensive incident response plan that outlines the steps to take in the event of a data breach. This includes notifying affected individuals and relevant authorities promptly.

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?

The notice is provided at the time of collection.

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

Should the users decide to "opt out", they would still be able to utilize the baseline FS R1s services, however their user experience will not be customized to their preferences or prior activities on the site.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

<u>Privacy Risk</u>:

Users are responsible to maintain their own data.

<u>Mitigation</u>:

Privacy Statement/Notice: We will develop and maintain a clear and comprehensive privacy statement or notice as a fundamental step in mitigating the risks associated with individuals being unaware of information collection. This statement will explicitly explain the purpose of data collection, detail how the data will be used, and outline any potential consequences of not providing the information. Our commitment is to ensure that this statement is easily accessible to individuals.

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?

PII accessed through the BAH SaaS provider/contractor's system is retained for a specific period in accordance with our contractual agreements. This retention period is [Specify Retention Period, e.g., 3 years].

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.fed.us/cgi-bin/Directives/get_dirs/fsh?6209.11

NARA retention periods will be reviewed any time a new reservation type is added to the system.

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

Follow the format below:

Privacy Risk:

NARA retention periods will be reviewed any time a new reservation type is added to the system.

Mitigation:

Production data could be improperly disclosed, altered, or taken offline, and FS R1s has protections in place to minimize the likelihood of these outcomes and depending upon the data the time length for retention. The database has many layers of protection from users on the Internet: Content Delivery Network (CDN) with distributed Web-Application Firewall (WAF), local firewall including Intrusion Prevention Systems (IPS) and an additional WAF module, instance level firewalls and the application itself. The application follows strict coding guidelines to prevent dangerous attacks.
Internal users can only access the system after authenticating with multiple factors. Although a small number of administrators can access the database in the development and test environments, none have access to the production database. When a need arises to access the database, administrators must receive approval from management to access the database by updating firewall rules and checking out a set of credentials. The database is encrypted, so it cannot be inadvertently restored from a backup or snapshot. The 30-year retention period for the Christmas Tree permits does increase the risk as R1s could conceivably have user account PII information being held on to for up to 27 years longer than the remainder of the retention policies. However, the security layers on the data are sufficient to protect that data. Further, R1s only recently started selling Christmas Trees in November 2020. The only records available for the Christmas Tree Permits are dating back to November 2020. R1s will work collaboratively with Recreation.gov over the next 2 years to come up with a comprehensive retention plan for Timber related permits.

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?

N/A - Only the PII required to maintain and honor reservations is available to internal users. All PII information contained in the system is fully encrypted while at rest and only accessible by those select personnel with the required role-based permissions to do so. Internal users access the information via secure login to the internal user interface where they will be able to view the necessary information within the Casandra database.

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

Follow the format below:

Privacy Risk:

Production data could be improperly disclosed, altered, or taken offline, and FS R1s has protections in place to minimize the likelihood of these outcomes and depending upon the data the time length for retention

Mitigation:

The database has many layers of protection from users on the Internet: Content Delivery Network (CDN) with distributed Web-Application Firewall (WAF), local firewall including Intrusion Prevention Systems (IPS) and an additional WAF module, instance level firewalls and the application itself. The application follows strict coding guidelines to prevent dangerous attacks.

Internal users can only access the system after authenticating with multiple factors. Although a small number of administrators can access the database in the development and test environments, none have access to the production database. When a need arises to access the database, administrators must receive approval from management to access the database by updating firewall rules and checking out a set of credentials. The database is encrypted, so it cannot be inadvertently restored from a backup or snapshot.

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?

N/A

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

Follow the format below:

Privacy Risk: N/A

Mitigation: 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?

Users are able to update their information by logging into their FS R1s user accounts utilizing the established secure username and password process.

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

N/A. Users are responsible to maintain their own data.

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

N/A. Users are responsible to maintain their own data.

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

Users are able to update their PII anytime at their discretion.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk: Users are responsible for the accuracy of their data.

Mitigation: Users are responsible to maintain their own data.

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?

User access control is provided by means of role-based permissions.

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

External users (such as a public user making reservations) are able to create and maintain their own accounts, but have no access to any PII other than their own.
Internal users, government employees, contractors (BAH) and concessionaires have access to only that PII as required to perform their daily duties. Role-based permissions are hierarchical and managed, assigned and revoked at level(s) above the individual user.

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

N/A – No PII is shared with external organizations.

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

The PII collected by the R1s system does not differ from that collected over the previous 12-years utilizing the outdated legacy National Recreation Reservation Service System (NRRS) system. Simply updating the system is no reason to alter the pre-existing federally mandated employee training requirements associated with the performance of their daily duties. Employees are required to accomplish all required PII training as dictated by their duties and job descriptions:
Booz Allen Hamilton employees; BAH mandates all privileged users to complete PII handling training during the onboarding process and the annual Security training which includes privacy training.

Concessionaire personnel; concessionaire users must acknowledge the FS R1s Rules of Behavior prior to gaining access to the system. Their specific PII training requirements are not within the purview of the FS R1s program, rather those requirements are documented and enforced through their concessionaire contracts / agreements with the relevant agency.

Federal employees and federal contractors complete a FS R1s Rules of Behavior prior and PII training during the onboarding process and the annual Security training which includes privacy training.

Responsible Official

ELLEN SHAW Digitally signed by ELLEN SHAW Date: 2023.06.09 11:44:57 -04'00'

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

Approval Signature

CYNTHIA TOWERS Digitally signed by CYNTHIA TOWERS Date: 2023.06.12 11:15:40 -05'00'

Cynthia Ebersohn
Privacy Officer (PO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

BENJAMIN MOREAU Digitally signed by BENJAMIN MOREAU Date: 2023.06.27 16:16:53 -04'00'

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