Privacy Impact Assessment

for

Forest Service Recreation One Stop (FS R1s)

Policy, E-Government and Fair Information Practices

Version: 1.1

Date: April 28, 2020

Prepared for: USDA NRE Forest Service Privacy Office

United States Department
of Agriculture

Contact Point

Michiko Martin

System Owner

USDA NRE Forest Service

360-891-5223

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

Abstract

The Forest Service Recreation One Stop (FS R1S) system represents an evolutionary leap forward in the recreation reservation services utilized by more than 10 participating federal agencies. FS R1S provides a full suite of reservation and business management tools to manage more than 90,000 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 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 providing a full suite of recreation reservation and business management tools to be employed by over 3,300 federal recreation facilities to manage more than 92,000 recreation locations and activities across more than 10 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 federal Government is simply procuring the services provided by this SaaS solution. 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. There are several types of data to be stored within FS R1s as follows:

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 PI 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 to manage 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). PII is also accessible through the US Treasury as it is associated with the secure processing of credit card payments.

In addition to the public facing aspect of the services, there is an internal component accessible by federal recreation managers and authorized concessionaires offering 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 Characterization of the Information

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

1.1 Identification

What information is collected, used, disseminated, or maintained in the system?

> At a minimum; name, address, phone number(s), e-mail addresses. Additional information is needed to enforce certain business rules are collected when applicable and include; driver's license number, license plate and state, vehicle identification number, and date of birth. Other non PII information may also be collected includes RV length, tent size, etc.

1.2 Source

What is the source(s) of the information in the system?

> The general public will input this information into the system.

1.3 Justification

Why is the information being collected, used, disseminated, or maintained?

> This information is necessary to create and manage reservations for the public.

1.4 Collection

How is the information collected?

> Direct input into the system by the public on-line, entered by federal personnel upon arrival at a reservable facility, and through call center agents when using the toll-free contact center.

1.5 Validation

How will the information be checked for accuracy?

The PII information entered by customers is not checked for accuracy beyond the verifications accomplished during the payment process to protect against fraudulent transactions. All PII entered into the system is entered by the customers and it is their individual responsibility to ensure the accuracy of the information entered into the FS R1s system.

1.6 Authority

What specific legal authorities, arrangements, and/or agreements defined the collection of information?

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.

1.7 Risk Mitigation

Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

All access and actions performed in the FS R1s production database is logged. The database is encrypted to prevent unauthorized backup and restoration.

In addition, all team members are required to acknowledge the rules of behavior form prior to gaining access. Recreation.gov Information Security Policies and Procedures document including access control and acceptable usage policies is also distributed to all Recreation.gov personnel.

Section 2.0 Uses of the Information

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

2.1 Usage

Describe all the uses of information.

> The PII information entered into the system is utilized strictly for the purposes of conducting the financial transaction, maintaining and honoring the reservation and enforcing location-specific business rules.
>
> Dissociated elements of the PII, such as a listing of zip codes without names, street addresses, phone numbers, etc., is used where appropriate to develop relevant metrics to help mangers make informed business decisions.

2.2 Analysis and Production

What types of tools are used to analyze data and what type of data may be produced?

> PII data is used for transactions using credit card transaction processing systems. In addition, PII data is available to authorized government users to pull specific reports, such as ‘campers who are arriving today’, as well as aggregate reports like ‘campsite utilization by week’. Reports are generated using a combination of custom software as well as a Business Intelligence (BI) tool.

2.3 Commercial/Public Use

If the system uses commercial or publicly available data, please explain why and how it is used

> The system does not use any external sources of PII.

2.4 Risk Mitigation

Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

All access and actions performed in the FS R1s production database is logged. The database is encrypted to prevent unauthorized backup and restoration.

In addition, all team members are required to acknowledge the rules of behavior form prior to gaining access. Rec.gov Information Security Policies and Procedures document including access control and acceptable usage policies is also distributed to all Recraetion.gov personnel.

Section 3.0 Retention

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

3.1 Time Period

How long is information retained?

FS R1s maintains active customer profiles as long as they remain active. A profile is considered inactive after a period of 3 years of inactivity (i.e., the customer has not logged into his/her profile for 3 years). These profiles will be purged from the system.

Active profiles may be retained in the system indefinitely as there are many individuals who will use this system for to make reservations for many years to come.

PII associated with specific reservations is fully encrypted and retained for a period of no less than 5 years.

3.2 Approval

Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Review and approval pending.

3.3 Risk Mitigation

Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Production data could be improperly disclosed, altered, or taken offline, and FS R1s has protections in place to minimize the likelihood of these outcomes. The database has many layers of protection from users on the Internet: CDN with distributed 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. All builds are tested before they are deployed to production, and PII data is not loaded into the test environment.

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 database is resistant to denial of service attacks because there are so many levels of defense from a networking perspective, and because the database was built with availability in mind. Cassandra is the primary database, and it's distributed across a number of virtual machines and geographies. The current plan is to deploy it across 6 data centers; three on the west coast and 3 on the east coast. Data is continuously replicated between data centers and is engineered to withstand multi node outages.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 Identification and Purpose

With which organization(s) outside of the Forest Service, but still within the Department of Agriculture is the information shared? What information is shared and for what purpose?

> Only that 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.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

> 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.

4.3 Risk Mitigation

Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

> 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. Changes are validated by the SME’s and security engineers and must comply with the applicable FEDRAMP controls.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 Identification and Purpose

With which external organization(s), outside of both the Forest Service and the Department of Agriculture, is the information shared? What information is shared, and for what purpose?

No PII is shared with external organizations.

5.2 Compatibility

Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

N/A.

5.3 Delivery and Security Measures

How is the information shared outside the Department and what security measures safeguard its transmission?

N/A.

5.4 Risk Mitigation

Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

N/A.

Section 6.0 System of Records Notice (SORN)

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

6.1 Requirement and Identification

Does this system require a SORN and if so, please provide SORN name and URL?

(Note: If a SORN is not required, answer “No” to this question, and “N/A” for questions 6.2 through 6.5.)

> No. System does not collect, store or retrieve PII based on an individual’s name or other personal identifier. All individual account records created and maintained in the use of this system are assigned a unique identifier independent from the individual.

6.2 Individual Notification

Was notice provided to the individual prior to collection of information?

> N/A.

6.3 Right to Decline

Do individuals have the opportunity and/or right to decline to provide information?

> N/A.

6.4 Right of Consent

Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

> N/A.

6.5 Risk Mitigation

Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

N/A.

Section 7.0 Access, Redress and Correction

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

7.1 Access

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 Correction

What are the procedures for correcting inaccurate or erroneous information?

> The PII in the FS R1s system is user-provided and therefore is user-maintained as well. Neither the Government nor the service provider (BAH) are checking the PII for errors outside of the financial transaction processing workflow so users are 100% responsible for maintaining their data.

7.3 Notification

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

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

7.4 Redress Alternatives

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

> N/A. Users are able to update their PII anytime at their discretion.

7.5 Risk Mitigation

Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

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

Section 8.0 Technical Access and Security

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

8.1 Procedures

What procedures are in place to determine which users may access the system and are they documented?

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

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.

8.2 Contractor Access

Will Department contractors have access to the system?

The service provider (BAH) has access to the SaaS solution in order to maintain and operate the system.

Concessionaires operating recreation facilities in the field have access to the system in order to operate and manage their facilities as well as to maintain and honor reservations made in the system.

8.3 Privacy Training

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

The PII collected by the R1s system does not differ from that collected over the previous 12-years utilizing the outdated legacy 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.

Specific to 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.

Specific to 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.

8.4 System Authority to Operate

Has Assessment & Authorization been completed for the system(s) supporting the program? If so, answer "Yes" and provide ATO expiration date(s).

Yes. ATO expiration date is June 28, 2022.

8.5 Audit and Technical Safeguards

What auditing measures and technical safeguards are in place to prevent misuse of data?

Access to the system requires users to authenticate and be authorized to access the respective system. Operating system as well as application logs are collected and streamed to a log aggregation server where they can be reviewed at a later time.

8.6 Risk Mitigation

Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Production data could be improperly disclosed, altered, or taken offline, and FS R1s has protections in place to minimize the likelihood of these outcomes. The database has many layers of protection from users on the Internet: CDN with distributed 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. All builds are tested before they are deployed to production, and PII data is not loaded in to the test environment.

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 database is resistant to denial of service attacks because there are so many levels of defense from a networking perspective, and because the database was built with availability in mind. Cassandra is the primary database, and it’s distributed across a number of virtual machines and geographies. The current plan is to deploy it across 6 data centers; three on the west coast and 3 on the east coast. Data is continuously replicated between data centers and is engineered to withstand multi node outages.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 Description

What type of project is the program or system?

> The system consists of Government data, which is hosted on a web-based SaaS application.

9.2 Privacy Concerns

Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

> The ability to secure customer data is a critical criterion in the service provider’s technology selection process. If the service provider is not confident that a given technology can be secured, it is not utilized as part of the service.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Review

Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

Yes.

10.2 Purpose

What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

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

10.3 PII Availability

What Personally Identifiable Information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

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. Other non PII information may also be collected includes RV length, tent size, etc.

10.4 PII Usage

How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

This information is necessary to create and manage reservations for the public.

10.5 PII Maintenance and Security

How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

> The information is available to the agency via controlled access to the contractor's system, it is never transferred to, or stored on, any agency-owned IT system(s). The security and controls defined earlier for the contractor owned system remain in effect at all times.

10.6 PII Purging

Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically? If so, is it done automatically? If so, is it done on a recurring basis?

> The information is available to the agency via controlled access to the BAH SaaS provider/contractor's system, it is never transferred to, or stored on, any agency- owned IT system(s). The security, controls and data retention policies defined earlier for the contractor owned system remain in effect at all times.
>
> The information is available to the agency via controlled access to the contractor's system, it is never transferred to, or stored on, any agency-owned IT system(s). The security, controls and data retention policies defined earlier for the contractor owned system remain in effect at all times
>
> The information is available to the agency via controlled access to the contractor's system, it is never transferred to, or stored on, any agency-owned IT system(s). The security, controls and data retention policies defined earlier for the contractor owned system remain in effect at all times

10.7 PII Access

Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

> The information is available to the agency via controlled access to the BAH SaaS Provider/contractor's system, it is never transferred to, or stored on, any agency- owned IT system(s). The users and related access controls defined earlier for the contractor owned system remain in effect at all times.

10.8 PII Sharing

With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared—either internally or externally?

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.

10.9 SORN Requirement

Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

No. FS R1s does not require a SORN .

10.10 Web Measurement and Customization

Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Yes. The FS R1s service utilizes "Tier 3 Multi-Session with PII" technology to deliver a customer experience akin to what users experience on the top commercial travel and e-commerce websites, such as Amazon, Airbnb and TripAdvisor.

Consistent with the requirements and prohibitions established by OMB M-10-22, all users are required to "opt in" before their PII may be utilized in this fashion. Should the users decide to "opt out", they would still be able to utilize the baseline R1s services, however their user experience will not be customized to their preferences or prior activities on the site.

System and procedures are reviewed annually.

10.11 Web Measurement and Customization Opt-In/Opt-Out

Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology? If so, does the agency provide the public with alternatives for acquiring comparable information and services?

Consistent with OMB M-10-22; users are required to “opt in”.

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.

10.12 Risk Mitigation

Given the amount and type of PII that becomes available through the agency’s use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Production data could be improperly disclosed to external attackers or internal administrators, and R1s has protections in place to minimize the likelihood of these outcomes. The database has many layers of protection from users on the Internet: CDN with distributed 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. All builds are tested before they are deployed to production, and PII data is not loaded into the test environment.

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.

Responsible Official

JEFFREY MARSOLAIS Digitally signed by JEFFREY MARSOLAIS
Date: 2020.05.15 16:36:03 -04'00'

Michiko Martin
System Owner (SO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

Approval Signature

CYNTHIA TOWERS Digitally signed by CYNTHIA TOWERS
Date: 2020.05.19 14:00:32 -05'00'

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

ROBERT CHADDERDON Digitally signed by ROBERT CHADDERDON
Date: 2020.05.26 07:02:55 -06'00'

Laura Hill
Information System Security Program Manager (ISSPM)
Natural Resources and Environment, Forest Service
United States Department of Agriculture