U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Grand Canyon National Park Noncommercial River Permit System
Bureau/Office: National Park Service, Grand Canyon National Park
Date: 6/3/2020
Point of Contact
Name: Felix Uribe
Title: NPS Associate Privacy Officer
Email: nps_privacy@nps.gov
Phone: 202-354-6925
Address: 12201 Sunrise Valley Drive, Reston VA 20192

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Colorado River through Grand Canyon National Park is managed according to the 2006 Colorado River Management Plan. The Colorado River Management Plan is a visitor use management plan that specifies actions to conserve park resources and visitor experiences while enhancing river running recreational opportunities on the Colorado River through Grand Canyon National Park. The Colorado River Management Plan sets overall use limits. Individuals are limited to a maximum of one recreational river trip through the Grand Canyon (between Lees Ferry and Diamond Creek) per calendar year. Launches from Diamond Creek are limited to two trips per day.

There are two types of recreational river trips possible on the Colorado River through Grand Canyon National Park. Commercial River trips are concessioner-guided river trips, often reserved a year or two in advance. Noncommercial river trips are self-guided river trips for individuals who have previously acquired the river skills to coordinate and safely lead their own trips through technical, world-class rapids.

The purpose of the system is twofold: (1) to process applications for noncommercial river trip permits for individual members of the public interested in obtaining or who have already obtained a noncommercial river trip launch date for the Colorado River between the Lees Ferry, Diamond Creek, and Pearce Ferry locations in Grand Canyon National Park, Arizona; and (2) to assist Grand Canyon National Park staff with visitor education, resource management and protection, recreational use planning, law enforcement, public safety (such as search and rescue efforts), fee collection, and providing information about the park and the park's partners to river users.

Noncommercial river launch dates are awarded via a weighted lottery system. The Main Lottery is held once a year, in February, to assign launch dates for river trips occurring the following calendar year. Follow-up lotteries are held as needed throughout the year to reassign cancelled and/or left-over river launch dates. Lottery applications are only accepted through the noncommercial river website when a lottery is open. If a user wins a noncommercial launch date in a lottery, they complete an online river permit application and an online river trip participant list. Once all pertinent river forms are finalized and costs paid, information is reviewed by the Grand Canyon National Park Permits Office. If all requirements listed in the Grand Canyon National Park Noncommercial River Trip Regulations are met, a noncommercial river permit is issued. The user (trip leader/permit holder) accesses the issued river permit online.

Information is collected from noncommercial river users through an online website (https://grcariverpermits.nps.gov) accessed via the internet using a web browser. All communication via the internet is encrypted in compliance with government encryption standards.

The system does not collect or store financial information. Monetary costs related to obtaining a noncommercial river permit are collected via pay.gov. Pay.gov is a program of the U.S. Department of the Treasury, Bureau of the Fiscal Service that provides U.S. federal agencies with a secure government-wide portal for collection of funds electronically. Financial information is collected and stored via the pay.gov infrastructure. Pay.gov processes ACH (Automated Clearing House) debits and plastic card collections, and allows payments using alternative payment services. Payment is made using a web-based interface. The pay.gov system provides agencies with a payment verification code allowing a payment to be marked as successful or failed. Additional information regarding privacy and security for pay.gov can be found at https://www.pay.gov/public/home/privacy

Trip participant information for commercial river trips is provided to the Grand Canyon National Park Permits Office by Grand Canyon National Park river concessioners. The PII provided is necessary to help ensure compliance with the one recreational river trip per year limit for all river users. Commercial river trip participants do not use the online system to obtain or arrange their river trips.

C. What is the legal authority?

54 U.S.C. 100101(a), National Park Service Organic Act; 54 U.S.C. 100751, Regulations; 54 U.S.C. 102712, Aid to visitors, grantees, permittees, or licensees in emergencies; 54 U.S.C. 103104, Recovery of costs associated with special use permits; and, 54 U.S.C. 320302, Permits. 36 CFR 1.5 - Closures and public use limits. 36 CFR 1.6 - Permits.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*,

System Security and Privacy Plan for Grand Canyon National Park Noncommercial River Permit System. UII Code: 000001896.

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None			

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

Special Use Permits--Interior, NPS-1 - February 18, 2014, 79 FR 9272

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*

OMB Control No. 1024-0022, Backcountry/Wilderness Use Permit (36 CFR 1.5, 1.6, and 2.10), Expiration Date 08/31/2020.

The Grand Canyon National Park Noncommercial River Permit System uses a series of web-based forms to collect information from the public. Information fields used by the system have been approved in OMB Control No. 1024-0022. A paper copy of the form is not used.

Note: NPS Form 10-404 (OMB Control No. 1024-0022) is a NPS-wide form and contains a combination of required and optional fields. The use of the optional fields is determined by the National Park Service unit collecting the information. The original form with all fields can be found at https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201704-1024-002

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Birth Date
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Other: *Specify the PII collected.*
All users: Password, username.

☒ Mailing/Home Address
☒ Credit Card Number
☒ Driver's License

Users with administrative access: government email address, government mailing address.

Users assigned a launch date: river trip permittee name, address, launch date, takeout date, takeout location, starting number of trip participants from Lees Ferry, number of participants hiking out, number of participants hiking in, number of children under 16.

River trip participants age 16 and older: government-issued photo identification is shown to a National Park Service River Ranger at Lees Ferry.

Monetary costs related to obtaining a noncommercial river permit are collected via pay.gov. Pay.gov is a program of the U.S. Department of the Treasury, Bureau of the Fiscal Service that provides U.S. federal agencies with a secure government-wide portal for collection of funds electronically. Financial information is collected and stored via the pay.gov infrastructure. Pay.gov processes ACH (Automated Clearing House) debits and plastic card collections.

Date of birth is collected for security purposes and to ensure an individual is uniquely identified. This information provides an additional layer of security to protect the user and participant data maintained in each account and is also necessary to help ensure compliance with the one recreational river trip per year limit for all river users and to ensure each user only has one account in the river system.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☐ DOI records

☐ Third party source
☐ State agency
☒ Other: *Describe*

Trip participant information for commercial river trips is provided to the Grand Canyon National Park Permits Office by Grand Canyon National Park river concessioners. This information is necessary to help ensure compliance with the one recreational river trip per year limit for river users. Commercial river trip participants do not use the online system to obtain or arrange their river trips, they directly contact the company they wish to hire. Commercial river use at Grand Canyon National Park is regulated by a concession contract between the business entity issued the contract and the National Park Service.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Web site
☒ Fax
☒ Telephone Interview
☐ Information Shared Between Systems
☐ Other: *Describe*

D. What is the intended use of the PII collected?

PII collected is used to issue a noncommercial river permit, to enforce the one recreational river trip per person per calendar year limit for the section of the Colorado River between Lees Ferry and Diamond Creek, and to ensure that individuals can be uniquely identified. Specifically, the data will be used to issue a noncommercial river trip permit to an individual trip leader and to create a river trip participant list for that individual's river trip. The trip leader will only have access to their own permit information and trip participant list. Grand Canyon National Park Permits Office staff and National Park Service law enforcement will have access to all permits and trip participant lists. Information will be shared with law enforcement for any authorized investigations and/or search and rescue operations.

When logging in, PII is collected from the user to identify a unique user profile. The login method has two steps. First, a user logs into the system with username and password. Second, if username and password pass validation, the user is sent to a new webpage where they enter date of birth as an additional layer of security to protect user and participant data in the accounts. Level of access granted after a successful login depends on type of user account.

Date of birth is collected when the user first creates the account and upon each subsequent login for security purposes. This information provides an additional layer of security to protect the user and participant data maintained in each account and is also necessary to help ensure compliance with the one recreational river trip per year limit for all river users and to ensure each user only has one account in the river system.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Information is shared internally within the Grand Canyon National Park Permits Office for the purpose of issuing a noncommercial river permit. Information is shared internally within the National Park Service at Grand Canyon National Park for resource protection, visitor education, law enforcement, to protect public safety, for the purpose of conducting search and rescue activities, or for any authorized investigations. PII shared could include river trip participant names, addresses, dates of birth, phone numbers, and email addresses.

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Information is shared with Federal agencies for the purpose of emergency contact and/or conducting search and rescue activities. Information is shared with Federal law enforcement for any authorized investigations. PII shared could include river trip participant names, addresses, dates of birth, phone numbers, and email addresses.

To subject matter experts in Federal agencies, for the purpose of obtaining scientific, management, and legal advice relevant to making a decision on an application for a permit.

To Federal natural resource and land management agencies for the exchange of information on permits granted or denied to assure compliance with all applicable permitting requirements.

In addition, information would be shared as needed to recover debts owed to the United States, in response to court order and/or discovery purposes related to litigation, or other authorized routine use when the disclosure is compatible with the purpose for which the records were compiled. PII shared could include river trip participant names, addresses, dates of birth, phone numbers, and email addresses.

Monetary costs related to obtaining a noncommercial river permit are collected via pay.gov. Pay.gov is a program of the U.S. Department of the Treasury, Bureau of the

Fiscal Service that provides U.S. federal agencies with a secure government-wide portal for collection of funds electronically. Financial information is collected and stored via the pay.gov infrastructure. Pay.gov processes ACH (Automated Clearing House) debits and plastic card collections, and allows payments using alternative payment services.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Information is shared with Tribal, state, or local agencies for the purpose of emergency contact and/or conducting search and rescue activities. Information is shared with Tribal, state, or local law enforcement for any authorized investigations. PII shared could include river trip participant names, addresses, dates of birth, phone numbers, and email addresses.

To subject matter experts in Tribal, state, local, or foreign agencies, for the purpose of obtaining scientific, management, and legal advice relevant to making a decision on an application for a permit.

To Tribal, state, or local natural resource and land management agencies for the exchange of information on permits granted or denied to assure compliance with all applicable permitting requirements.

In addition, information would be shared as needed to recover debts owed to the United States, in response to court order and/or discovery purposes related to litigation, or other authorized routine use when the disclosure is compatible with the purpose for which the records were compiled. PII shared could include river trip participant names, addresses, dates of birth, phone numbers, and email addresses.

Access to one of the river trip launch/takeout areas, known as Diamond Creek, is via Diamond Creek Road which passes through Hualapai tribal lands. The Hualapai Tribe requires non-tribal members to obtain authorization prior to crossing tribal lands. Limited information will be shared with the Hualapai Tribe for those noncommercial river trips whose permit indicates that trip participants would be joining or leaving the trip at Diamond Creek, requiring trip participant access to tribal lands via the Diamond Creek Road.

The data fields disclosed are limited in scope and will only include river trip permittee name, Diamond Creek date, number of participants joining the trip at Diamond Creek, number of participants leaving the trip at Diamond Creek. This information is faxed to the Hualapai Tribe.

☐ Contractor: *Describe the contractor and how the data will be used.*

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Records or information contained in this system may be disclosed to the news media and the public, with the approval of the Public Affairs Officer in consultation with counsel and the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy. Information might be released to the media when it pertains to a river-related death or to a missing person report.

The following statistical river information will be shared with the public: number of river lottery applications submitted; total points of all river lottery applications submitted; number of points held by a winning lottery application; number of river permits issued or cancelled; countries or US states applicants come from; user days by season, participant and trip totals; trip sizes and trip lengths; number of launches by date. PII is removed and information is aggregated prior to statistical information being shared.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

The individual can choose to enter a river lottery and apply for a noncommercial river launch date and provide information or decline to enter a river lottery and provide no information. Users are notified that by submitting information they are giving consent to the use of that information. This notification is given when creating a user profile, when submitting a lottery application, and when submitting a river permit application. Due to the information requirements of the system, lack of consent will prevent the permitting process from completing.

In order to issue a noncommercial river permit, legal name and contact information is needed for the permit holder. In order to enforce the one recreational river trip per person per calendar year limit for the section of the Colorado River between Lees Ferry and Diamond Creek, legal name, date of birth, and contact information are needed from each river trip participant to ensure they can be uniquely identified.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is presented to the user when information is collected on the website (https://grcariverpermits.nps.gov).

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this privacy impact assessment and the current publication of the Special Use Permits--Interior, NPS-1 system of records notice in the Federal Register.

Users may also view the pay.gov privacy policy at https://www.pay.gov/public/home/privacy and the U.S. Department of the Treasury, Bureau of the Fiscal Service, pay.gov privacy impact assessment at https://www.fiscal.treasury.gov/pia.html.

☒ Other: *Describe each applicable format.*

A link to the River Permits Office Privacy Policy is provided to the user on the website. It is located at https://grcariverpermits.nps.gov/privacy.cfm.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Users with administrative access can retrieve data using specific search options (last name, username, email address, or launch date) or by bulk retrieval of requests requiring staff attention (for example, permit applications ready for staff review, permit applications pending payment). Additionally, users with administrative access can retrieve data on groups of river permits via automated reports within the system.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*
Limited information will be shared with the Hualapai Tribe about noncommercial river trips whose permit indicates that trip participants would be joining or leaving the trip at Diamond Creek, requiring trip participant access to tribal lands via the Diamond Creek Road. The information is faxed to the Hualapai Tribe and is used by them to make decisions regarding authorization to cross tribal lands.

A monthly trip participant report is shared with National Park Service employees of the Grand Canyon National Park Science and Resource Management Division. This report is

used to contact trip participants and educate them about resource issues on the river. For example, how to prevent the spread of invasive species such as quagga mussels.

During a search and rescue incident or for law enforcement purposes, a report may be produced containing information regarding one or more specific river trips and their trip participants. The information would be made available to the officials authorized to oversee the incident and/or investigation.

Reports may be created to confirm only one user profile exists per individual. Reports may be created to verify the accuracy of last recreational river trip date as listed in a user profile. These reports will be for internal administrative use of National Park Service employees of the Grand Canyon National Park Permit Office.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data is collected directly from the individual who created the river user account and is only as accurate as what they provide. For those individuals awarded a noncommercial river trip launch date, the information provided in the river permit application is verified by a National Park Service River Ranger before the river trip launches from Lees Ferry. The River Ranger verifies river trip participant information (legal name, date of birth, contact information) and river trip details. All river trip participants age 16 and older must carry government-issued photo identification and present it to the River Ranger prior to trip launch.

Participant lists for commercial river trips are provided by Grand Canyon National Park river concessioners. River concession contracts specify reporting requirements and methods for verifying accuracy of data.

B. How will data be checked for completeness?

Data is collected directly from the individual who created the river user account and is only as accurate as what they provide. All required data must be provided before a user account can be created, a lottery application can be submitted, or a river permit application can be saved. The system performs security and validation checks to ensure the data provided is what is expected (for example, length and type of data) prior to accepting and storing the information. Users are warned of errors and given an opportunity to correct any issues found by the system.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Data is collected directly from the individual who created the river user account and is only as accurate as what they provide. Members of the public who use the system are expected to enter accurate information online. With certain restrictions, a user may edit their own information (including PII) at any time. A user may not edit either their legal name or their date of birth after a profile has been created. For existing user profiles, legal name and date of birth can only be changed by an administrative user with the correct level of access. River trip information for completed trips may be viewed by the trip leader, but it can only be edited by a user with administrative access. Edits/changes to user information in the system is instantaneous and the updated information is available to all who have online access to that record.

To change their date of birth after a profile has been created, the user must request the change via fax. The fax machine is in a locked room in a government building. Faxes containing date of birth are shredded after the information has been updated in the system. This is the only incoming noncommercial river information collected from a user via fax.

For noncommercial river trips launching from Lees Ferry, a National Park Service River Ranger verifies river trip participant information (legal name, date of birth, contact information) and river trip details with the trip leader. During the check-in process, all trip participants 16 years of age and older must show government-issued photo identification to the River Ranger. At the end of the check-in process, the trip leader signs a paper check-out sheet acknowledging all information is correct. Information verified by the River Ranger is used to update system data.

When members of the public contact the Grand Canyon National Park Permits Office, online information is verified. Email addresses that fail delivery are flagged in the system.

Multiple user profiles per individual are not permitted in the online system. Regular checks are performed to catch extra profiles. When multiple profiles are found per individual, information is verified, and extra profiles are disabled.

The river system does not collect, validate, or store financial information. Monetary costs related to obtaining a noncommercial river permit are collected via pay.gov. Pay.gov is a program of the U.S. Department of the Treasury, Bureau of the Fiscal Service that provides U.S. federal agencies with a secure government-wide portal for collection of funds electronically. Financial information is collected, validated, and stored via the pay.gov infrastructure. The pay.gov system provides agencies with a payment verification code allowing a payment to be marked as successful or failed.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Records in this system are retained in accordance with the National Park Service Records Schedule Resource Management and Lands (Item 1), which has been approved by the National Archives and Records Administration (Job No. N1-79-08-1). The disposition for short-term resource management and land records is temporary and records are destroy/delete 15 years after closure. The disposition for routine resource management and land records is temporary and records are destroyed/deleted 3 years after closure.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

The approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with National Archives and Records Administration Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to individual privacy in the Grand Canyon National Park (GRCA) Noncommercial River Permits System due to the amount and nature of the data collected, processed, and stored. The GRCA Noncommercial River Permits System has undergone a formal Assessment and Authorization and is working towards obtaining an Authority to Operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology standards. The system is rated as FISMA moderate based upon the type of data and has had defined and implemented a series of administrative, technical and physical mitigation measures to mitigate risks. Electronic data is protected through user identification, passwords, database permissions, and software controls. Database access is controlled by system user authentication, database access (table and row level) via grants, and specific database-table access by user account restrictions. All communication via the internet is encrypted in compliance with government encryption standards. All users of the system must log in and user sessions are automatically voided after 30 minutes of inactivity. Inactivity is defined as the user not interacting with the river system via a web browser.

There is a risk that individuals may gain unauthorized access to the information in the system. Users access data by logging in with username, password, and date of birth. The login method has two steps. First, a user logs into the system with username and password. Second, if username and password pass validation, the user is sent to a new webpage where they enter date of birth. Level of access granted after a successful login depends on type of user account. Members of the public only have access to their own data. Users granted administrative accounts, who can access multiple records, are limited

to authorized National Park Service personnel with valid DOI Active Directory credentials. Administrative level webpages check for a DOI-Net IP address prior to loading. There are several levels of administrative access, the level assigned depends on the specific employee's need when performing their job. The GRCA Permits Office Manager determines (1) who receives administrative access, and (2) the level of administrative access assigned. To obtain administrative access, the employee and their supervisor complete the "Request Administrative Access" form and submit it to the GRCA Permits Program Manager. The GRCA Permits Program Manager verifies the list of users with administrative access several times a year. When deemed no longer needed, administrative accounts are disabled and left in the database. Temporary or emergency administrative accounts are not created. Administrative accounts are automatically disabled by the system after 45 days of inactivity. Disabled administrator accounts can only be re-enabled by an administrative user with the correct level of access. The database is on a separate server from the online system. Direct access to the database is limited to database administrators and is only possible via DOI-Net. Changes made to system data are tracked and stored. Edits/deletions to the PII contained in a user record can only be made by either the owner of the record or specific administrative users, and such changes are logged into a database by UTC date/time and name of the individual who initiated the edit/deletion. Administrative users may not use the system for personal use (i.e. apply in a noncommercial river trip lottery to win a river launch date). Only user accounts with basic access may apply in a noncommercial river lottery. Users with administrative access who win a launch date in a lottery (using their “regular” account) are not permitted to verify or issue their own river permit.

There is a risk that information may be used outside the scope of the purpose for which it was collected. This risk is mitigated by restricting administrative access to the system to only those National Park Service personnel who need such access to perform their official job duties and have DOI credentials. Additionally, the level of administrative access provided starts at the lowest level. The U.S. Department of the Interior requires all National Park Service employees to complete annual training in Federal Information Systems Security Awareness, Privacy Awareness, Records Management and Section 508 Compliance, and Controlled Unclassified Information. National Park Service employees are required by the U.S. Department of the Interior to sign form DI-4002: Rules of Behavior for Computer Network Users stating they will neither misuse government computers nor the information contained therein. National Park Service employees with the highest level of administrative access to either the online river system and/or its database are required to complete Role Based Privacy Training. These trainings will ensure that throughout the life cycle of the information system and data management, the privacy and security controls and protections can be executed and maintained by meeting sufficient level of performance requirement.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored has intentionally been limited to only the minimal amount of

data needed to ensure management of the river corridor within Grand Canyon National Park meets the guidelines and requirements specified in the Grand Canyon National Park Colorado River Management Plan. Records in this system are retained in accordance with the National Park Service Records Schedule Resource Management and Lands (Item 1), which has been approved by the National Archives and Records Administration (Job No. N1-79-08-1). System records will be disposed of through standard procedures, which further mitigates any potential risk. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

There is a risk that an individual's date of birth submitted via fax may be accessed by unauthorized individuals, however, there are controls in place to protect the PII in the faxed documents. The fax machine is located in a locked room in a government building. Faxes containing date of birth are shredded after the information has been updated in the system.

There is a risk that individuals may not have noticed that their PII will be collected or how it will be used. This risk is mitigated by this Privacy Impact Assessment, by the system's privacy policy posted at https://grcariverpermits.nps.gov/privacy.cfm, and by the System of Records Notice, Special Use Permits--Interior, NPS-1 - February 18, 2014, 79 FR 9272. A Privacy Act Statement is presented to the user when information is collected on the website. Users are notified that by submitting information they are giving consent to the use of that information. This notification is given when creating a user profile, when submitting a lottery application, and when submitting a river permit application. Users whose river permit indicates access to Diamond Creek Road will be needed are notified that limited information will be shared with the Hualapai Tribe.

Users are directed to the U.S. Department of the Treasury, Bureau of the Fiscal Service, pay.gov site to process electronic payments and may view the pay.gov privacy policy for privacy practices. Users may also view the pay.gov privacy impact assessment published on the Bureau of Fiscal Service website at https://www.fiscal.treasury.gov/pia.html.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

Yes, use of the data is both relevant and necessary. To ensure management of the Colorado River corridor within Grand Canyon National Park meets the guidelines and requirements specified in the Grand Canyon National Park Colorado River Management Plan, information needs to be collected from recreational river users (both noncommercial and commercial).

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

No new data on individuals is created.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users

☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe*

Data collected is stored in a database. The database is automatically backed up daily. Data backups are compressed and then encrypted. The database is on a separate server from the online system. Access to the server the database is limited to the individuals specified in the National Park Service NISC Service Level Agreement.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Members of the public only have access to their own data. Members of the public can create new records containing their own information, or for existing records may edit their contact information (address, phone number(s), email address(es)). With certain restrictions, a user may edit their own information (including PII) at any time. A user may not edit either their legal name or their date of birth after a profile has been created. For existing user profiles, legal name and date of birth can only be changed by an administrative user with the correct level of access. To change a date of birth the user must request the change via fax. River trip information for completed trips may be viewed by the trip leader, but it can only be edited by a user with administrative access. Edits/changes to user information in the system is instantaneous and the updated information is available to all who have online access to that record.

Users with administrative access can view/edit records other than their own and issue/approve river permits. Only National Park Service employees have administrative access. Administrative level webpages check for a DOI-Net IP address prior to loading. There are several levels of administrative access, the level assigned depends on the specific employee's need when performing their job. The GRCA Permits Office Manager determines (1) who receives administrative access, and (2) the level of administrative access assigned. The GRCA Permits Program Manager verifies the list of users with administrative access several times a year.

Electronic data is protected through user identification, passwords, database permissions, encryption, and software controls. Database access is controlled by system user authentication, database access (table and row level) via grants, and specific database-table access by user account restrictions. Direct access to the database is limited to database administrators and is only possible by logging into the server hosting the database via the NPS network using a government issued Personal Identity Verification Card.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy Act contract clauses were included in their contracts and other regulatory measures addressed.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The login method has two steps. First, a user logs into the system with username and password. Second, if username and password pass validation, the user is sent to a new webpage where they enter date of birth. Level of access granted after a successful login depends on type of user account. The system tracks last successful login date and time for each user. For administrative accounts, the system additionally tracks date of last password change. When data is changed, the system logs both the changes and the user responsible.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The login method has two steps. First, a user logs into the system with username and password. Three incorrect entries and the username is logged into a login security table and the associated account is locked for 24 hours. Second, after a correct username and password combination, the user enters date of birth. Three incorrect date of birth entries and the username is logged into a login security table and the associated account is locked and can only be unlocked by an administrative user with the correct level of access upon request by the user.

Changes made to system data is tracked and stored. The user who made the change is logged. Administrative users write detailed notes when making changes to information in a user's account.

M. What controls will be used to prevent unauthorized monitoring?

Only users with administrative privileges have access to records other than their own. There are several levels of administrative access. The administrative access level assigned is dependent on the employee's need when performing their job. All users with administrative access must use government equipment, be on a National Park Service network, and change their passwords every 60 days. If a user with administrative access goes on furlough or changes jobs, their account is disabled.

Administrative users are educated on safeguards to be employed while utilizing the network/internet prior to accessing the information in the system. All National Park Service employees with access to the records are required to complete training in Federal Information Systems Security Awareness, Privacy Awareness, Records Management and Section 508 Compliance, and Controlled Unclassified Information (CUI) prior to being given access to the system, and on an annual basis, thereafter. National Park Service employees sign security forms stating they will neither misuse government computers nor the information contained therein. All National Park Service employees with the highest level of administrative access to either the online noncommercial river system and/or its database are required to complete Role Based Privacy Training.

Administrative users may not use the system for personal use (i.e. apply in a noncommercial river trip lottery to win a river launch date). Only user accounts with basic access may apply in a noncommercial river trip lottery. This restriction is to ensure a clear separation between user account types. Administrative users are the only users permitted duplicate accounts.

Note: PII (legal name, date of birth, contact information) is not changed or modified as a result of a noncommercial river lottery. Any edits/deletions to the PII contained in a user account can only be made by either the owner of the account or specific administrative users, and such changes are logged by date/time and name of the individual who initiated the edit/deletion. These logs cannot be accessed via the online river system. Direct access to the database containing these logs is limited to database administrators and is only possible by logging into the server hosting the database via the NPS network using a government issued Personal Identity Verification Card.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards

☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. *Describe* Only approved personnel are allowed access.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. *Describe* Personal information on the river trip participant lists (first name, middle initial, last name, date of birth, mailing address, telephone number(s), and email address(es)) is encrypted twice (using two different keys) before being stored in the database. Encryption algorithm is AES CBC using 256-bit keys.

Data collected is stored in a database. The database is automatically backed up daily. Data backups are compressed and then encrypted. The database is on a separate server from the online system and does not have access to the trip participant encryption keys.

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII

☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Grand Canyon National Park Permits Program Manager serves as the Grand Canyon National Park Noncommercial River Permit System Information System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in the system. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within the Grand Canyon National Park Noncommercial River Permit System, in consultation with NPS and DOI Privacy Officials. All Privacy Act complaints will be addressed by the NPS Associate Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The Grand Canyon National Park Permits Program Manager and the Grand Canyon National Park Permits Office Web Developer are responsible for assuring proper use of the data and for reporting any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with NPS Associate Privacy Officer. Physical security of the servers containing the data is the responsibility of the National Park Service NISC.