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 Backcountry Permit System - Web
Bureau/Office: National Park Service Grand Canyon National Park
Date: 8/5/19
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?

Grand Canyon National Park's backcountry program is managed according to the 1988 Backcountry Management Plan. The Backcountry Management Plan defines the primary

policies which manage visitor use and resource protection for the undeveloped areas of Grand Canyon National Park. The plan applies to lands within the park. Of the 1,215,735 acres contained within the park, approximately 1,179,700 acres are considered backcountry.

The purpose of the system is twofold: (1) to process applications for backcountry permits for individual members of the public and organizations interested in obtaining a backcountry permit allowing overnight access to backcountry use areas within Grand Canyon National Park; 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 backcountry users. This system is replacing an existing internal (not web based) backcountry permitting system.

Information is collected from backcountry users through a secure online website (https://grcabackcountrypermits.nps.gov) accessed via the internet using a web browser.

The system does not collect or store financial information. Monetary costs related to obtaining a backcountry permit are collected via pay.gov. Pay.gov is an offering 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. Additional information regarding pay.gov can be found at https://pay.gov/public/home/forAgencies

Trip participant information for guided overnight backcountry trips is provided to the Grand Canyon National Park Backcountry Information Center by the commercial company hired by the participant to guide their hike. Only those companies issued a Grand Canyon Backpacking Commercial Use Authorization by the National Park Service are allowed to obtain Grand Canyon backcountry permits to guide overnight hikes. A condition of the commercial use backcountry permit is a verified trip participant list. The Personally Identifiable Information (PII) provided is legal name and contact information for all trip participants.

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?
The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

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

Grand Canyon National Park Backcountry Permit System - Web (GRCA BC Permit).

☐ 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	None	No	N/A

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, National Park Service, Expiration Date: 08/31/2020. Note: NPS Form 10-404 (OMB Control No. 1024-0022) is an NPS-wide form and contains optional fields. The use of the optional fields is determined by the National Park Service unit collecting the information. A copy of the original form showing 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
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Emergency Contact
☒ Mailing/Home Address

☒ Other: *Specify the PII collected.*

Users requesting a backcountry permit: permittee name, address, travel-in date, travel-out date, group size, vehicle plate information, permit request ID.

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 guided overnight backcountry trips is provided to the Grand Canyon National Park Backcountry Information Center by the commercial company hired by the participant to guide their hike. Only those companies issued a

Grand Canyon Backpacking Commercial Use Authorization by the National Park Service are allowed to obtain Grand Canyon backcountry permits to guide overnight hikes. A condition of the commercial use backcountry permit is a verified trip participant list. The PII provided is legal name and contact information for all trip participants.

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?

In order to issue a backcountry permit, legal name and contact information are needed for the permit holder. Depending on the itinerary chosen, for safety reasons, emergency contact information may also be needed. To meet the requirements of a Guided Backpacking Commercial Use Authorization, names and contact information for each trip participant is needed for commercial use.

Once all pertinent backcountry forms are finalized, and the requested itinerary is available, the trip leader pays permit costs. If needed for safety reasons, information is reviewed by the Grand Canyon National Park Backcountry Information Center. Lastly, a backcountry permit is issued. The trip leader/permit holder accesses the issued backcountry permit online.

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 Backcountry Information Center for the purpose of issuing a backcountry 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, or for the purpose of conducting search and rescue activities. PII shared could include backcountry trip participant information (name, address, phone number, and email address) and emergency contact information (emergency contact name and phone number).

☐ 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 upon request with Federal, state, local, tribal organizations upon request for the purpose of emergency contact and/or conducting search and rescue activities. PII shared could include backcountry trip participant information (name, address, phone number, and email address) and emergency contact information (emergency contact name and phone number).

To subject matter experts, including but not limited to experts in State, Federal, local, and foreign agencies, for the purpose of obtaining scientific, management, and legal advice relevant to making a decision on an application for a permit.

To Federal, State, and 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 backcountry trip participant information (name, address, phone number, and email address) and emergency contact information (emergency contact name and phone number).

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

Access to one of the hiking areas, known as Pasture Wash, is via a road which passes through Havasupai tribal lands. The Havasupai Tribe requires non-tribal members to obtain authorization prior to crossing tribal lands. Limited information will be shared with the Havasupai Tribe for backcountry permits going to or beyond this area. The individual, when requesting a backcountry permit for the Pasture Wash area, is notified that information will be shared with the Havasupai Tribe for backcountry permits going to or beyond this area.

☐ 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.

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 apply for a backcountry permit and provide information, or decline to apply for a permit and provide no information.

In order to issue a backcountry permit, legal name and contact information is needed for the permit holder. Depending on the itinerary chosen, for safety reasons, emergency contact information might also be needed. To meet the requirements of a Guided Backpacking Commercial Use Authorization, names and contact information for each trip participant is needed for commercial use.

☐ 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 whenever information is collected on the website (https://grcabackcountrypermits.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.

☒ Other: *Describe each applicable format.*

A link to the Backcountry Information Center Privacy Policy is provided to the user on the website. It is located at https://grcabackcountrypermits.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.).

Members of the public can retrieve data related to a single backcountry permit request by providing the email address used when requesting the permit and the permit request ID. (Note: a permit request ID is created by the system and given to the user after the initial, successful submittal.) Members of the public can view an automated calendar which retrieves data on the availability status for groups of geographically adjacent backcountry use areas/locations.

Users with administrative access can retrieve data using specific search options or by bulk retrieval of requests requiring staff attention.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

The data will be used to issue a backcountry permit to an individual trip leader. The trip leader will only have access to their own permit information. Grand Canyon National Park Backcountry Information Center staff and National Park Service law enforcement will have access to all permits. Information will be shared with law enforcement for any authorized investigations. The printed backcountry permit contains permit holder name and address, hike start date, number of hikers, number of equines (horses, mules, and/or burros), and the use area for each night.

The following backcountry statistical information will be shared with the public: numbers of backcountry permit applications received, issued, or cancelled; countries or US states trip leaders come from; seasonal user-day, participant, and trip totals; trip sizes and trip lengths; common itineraries; use trends; use by zone, use area, month, and year; backcountry use by commercial guiding companies. All information is aggregated and does not allow identification of any one individual.

☐ 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 requesting the backcountry permit and is only as accurate as what they provide. PII is not verified for accuracy by the Grand Canyon National Park Backcountry Permit System. Participant lists for commercially

guided backcountry trips are provided by the company approved to guide the trip. Commercial Use Authorization documents specify reporting requirements and methods for verifying accuracy of data.

B. How will data be checked for completeness?

All required data must be provided prior to a backcountry permit request being saved. The system performs security and validation checks to ensure the data provided is what is expected 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).

The data is provided by the individual or organization and is only as current as what they provide. Members of the public who use the system are expected to enter accurate information online.

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 I), which has been approved by the National Archives and Records Administration (Job No. Nl-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) Backcountry Permits System due to the amount and nature of the data collected, processed, and stored. The GRCA Backcountry Permits System has undergone a formal Assessment and Authorization and has been granted 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. All communication via the internet is encrypted in compliance with government encryption standards.

There is a risk that individuals may gain unauthorized access to the information in the system. Members of the public only have access to their own record. A member of the public with multiple backcountry permit requests in their name is only able to access one record at a time using the email and request ID unique to that record. Users granted administrative accounts, who can access multiple records, are limited to authorized National Park Service personnel with valid DOI credentials. There are several levels of administrative access, the level assigned depends on the specific employee's need when performing their job. 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. Users with administrative access who wish to use the system for personal use (i.e. request a backcountry permit) may not do so using an administrative account. Additionally, users with administrative access who acquire a backcountry permit for personal use are not permitted to verify or issue their own 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 backcountry 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 backcountry within Grand Canyon National Park meets the guidelines and requirements specified in the Grand Canyon National Park Backcountry Management Plan. Records are maintained in accordance with Department Records Schedules that were approved by NARA. 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 individuals may not have noticed that their PII will be collected or how it will be used. This risk is mitigated by the Privacy Act Statement posted at https://grcabackcountrypermits.nps.gov/privacy.cfm and this Privacy Impact Assessment. Additionally, a Privacy Act Statement is presented to the user whenever information is collected on the website.

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 backcountry within Grand Canyon National Park meets the guidelines and requirements specified in the Grand Canyon National Park Backcountry Management Plan, information needs to be collected from backcountry users.

☐ 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*

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 record. 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)) or information related to their backcountry itinerary (for example, hike start date, number of hikers, number of stock, nightly use areas). A record is created only when all required backcountry permit information has been submitted. Members of the public access existing saved backcountry permit information using email address and request ID. Email address is provided by the individual when the permit request is submitted. Request ID is created by the system when the permit request is saved. The combination of both items allows access to one record only.

Users with administrative access can view/edit records other than their own and issue/approve backcountry permits. Only a limited number of National Park Service employees have administrative access. There are several levels of administrative access, the level assigned depends on the specific employee's need when performing their job.

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.

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*

Access to data located online is restricted to the individual submitting the permit request or to administrative users. Individual users are identifiable via permit request number and email address.

☐ No

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

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 and be on a National Park Service network.

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. National Park Service employees with the highest level of administrative access to either the online backcountry permit system and/or its database are required to complete Role Based Privacy Training.

Administrative users who wish to use the system for personal use (i.e. request a backcountry permit), may not do so using an administrative account. Additionally, users with administrative access who acquire a backcountry permit for personal use are not permitted to verify or issue their own permit.

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*

Data backups are encrypted.

(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.

Privacy rights of the public and employees will be protected by the Grand Canyon National Park Permits Program Manager and the Permits Office Web Developer. Privacy Act complaints and requests for redress or amendment of records will be addressed by Grand Canyon National Park Backcountry Information Center staff. All Privacy Act complaints will be forward to 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 the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information.