



DEPARTMENT OF THE INTERIOR

National Park Service

[DOI-2022-0006; PWOVPADW0 PPMRLE1Y.Y00000]

Privacy Act of 1974; System of Records

AGENCY: National Park Service, Interior.

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of the Interior (DOI) is issuing a public notice of its intent to create the National Park Service (NPS) Privacy Act system of records, INTERIOR/NPS-34, Backcountry and Wilderness Use Permit System. The system processes applications for permits from individual members of the public, organizations, and other business entities interested in obtaining permits authorizing access to and use of backcountry and wilderness areas within the National Park System. This new system will be included in DOI's inventory of record systems.

DATES: This new system will be effective upon publication. New routine uses will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. Submit comments on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may send comments identified by docket number [DOI-2022-0006] by any of the following methods:

- Federal eRulemaking Portal: <https://www.regulations.gov>. Follow the instructions for sending comments.
- Email: DOI_Privacy@ios.doi.gov. Include docket number [DOI-2022-0006] in the subject line of the message.
- U.S. mail or hand-delivery: Teri Barnett, Departmental Privacy Officer, U.S.

Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC
20240.

Instructions: All submissions received must include the agency name and docket number [DOI-2022-0006]. All comments received will be posted without change to <https://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <https://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: Felix Uribe, Associate Privacy Officer, National Park Service, 12201 Sunrise Valley Drive, Reston, VA 20192, nps_privacy@nps.gov or (202) 354-6925.

SUPPLEMENTARY INFORMATION:

I. Background

NPS is establishing the system of records for the INTERIOR/NPS-34, Backcountry and Wilderness Use Permit System. The system processes applications for permits from members of the public, organizations, and other business entities interested in obtaining permits authorizing access to and use of backcountry and wilderness areas within the National Park System. The system also assists park staff with visitors' education, trip planning, fee collection, resource management and protection, wilderness stewardship, outdoor ethics, recreational use planning, law enforcement activities, and public safety, including preventative search and rescue; provides permit holders and participants with information about parks and their partners; identifies permitted trip itineraries; and provides reports of activities conducted under an issued permit.

In accordance with its legal authorities, NPS may share information with Federal, state, local, and Tribal agencies for search and rescue and law enforcement activities, and status of permits to ensure compliance with all applicable permitting requirements and terms of other official agreements. To the extent permitted by law, information may be

shared with other agencies and organizations as authorized and compatible with the purpose of this system, or when proper and necessary, consistent with the routine uses set forth in this system of records notice (SORN).

II. Privacy Act

The Privacy Act of 1974, as amended, embodies fair information practice principles in a statutory framework governing the means by which Federal agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to records about individuals that are maintained in a "system of records." A system of records is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particulars assigned to the individual. The Privacy Act defines an individual as a United States citizen or lawful permanent resident. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOI by complying with DOI Privacy Act regulations at 43 CFR Part 2, Subpart K, and following the procedures outlined in the Records Access, Contesting Record, and Notification Procedures sections of this notice.

The Privacy Act requires each agency to publish in the *Federal Register* a description denoting the existence and character of each system of records that the agency maintains and the routine uses of each system. The INTERIOR/NPS-34, Backcountry and Wilderness Use Permit System, SORN is published in its entirety below. In accordance with 5 U.S.C. 552a(r), DOI has provided a report of this system of records to the Office of Management and Budget and to Congress.

III. Public Participation

You should be aware your entire comment including your personally identifiable information, such as your address, phone number, email address, or any other personal information in your comment, may be made publicly available at any time. While you

may request to withhold your personally identifiable information from public review, we cannot guarantee we will be able to do so.

SYSTEM NAME AND NUMBER: INTERIOR/NPS-34, Backcountry and Wilderness Use Permit System.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Visitor Resource and Protection Directorate, National Park Service, 1849 C Street NW, Room 2462, Washington, DC 20040. Records are also located at the parks responsible for issuing backcountry and wilderness use permits. A current listing of park offices may be obtained by visiting the NPS website at <https://www.nps.gov> or by contacting the System Manager below.

SYSTEM MANAGER(S): Chief of Wilderness Stewardship, Visitor and Resource Protection Directorate, National Park Service, 1849 C Street NW, Room 2462, Washington, DC 20240.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 54 U.S.C. Subtitle 1, National Park System; 16 U.S.C 1131-1136, Wilderness Act; 16 U.S.C 6801- 6814, Federal Lands Recreation Enhancement Act; 36 CFR Part 71, Recreation Fees; 36 CFR 1.6, Permits; 36 CFR 2.10, Camping; 36 CFR 2.23, Recreation Fees; and 36 CFR Part 13, NPS Units in Alaska.

PURPOSE(S) OF THE SYSTEM: The purposes of the system are to:

(1) Assist park staff with visitors' education, trip planning, fee collection, resource management and protection, wilderness stewardship, outdoor ethics, recreational use planning, trip itineraries, and law enforcement and public safety activities, including preventative search and rescue;

(2) Establish and verify applicants' eligibility and process applications from members of the public and organizations interested in obtaining a permit for authorized activities within the NPS;

(3) Provide permit holders, participants and members of the public with permit-related information and information about parks and partners;

(4) Monitor activities conducted under a permit and analyze data, produce reports to manage the use of park resources, generate budget estimates and track performance, and evaluate the effectiveness of the permit programs to meet reporting requirements of the DOI and NPS; and

(5) Assess the impact of permitted activities on the conservation and management natural and cultural resources, including protected species and their habitats and preservation of wilderness character.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals covered by the system include members of the public and organizations submitting a permit application, and NPS employees responsible for processing applications for permits, applicants of permits, and holders of permits. This system contains records concerning corporations and other business entities, which are not subject to the Privacy Act. However, records pertaining to individuals acting on behalf of corporations and other business entities may reflect personal information.

CATEGORIES OF RECORDS IN THE SYSTEM: The system contains backcountry and wilderness permit applications and permits for authorized activities in national parks and may include applicant information such as name, address and country, email, home phone number, personal mobile number, work phone number, park pass number, group/organization type, permit request number, permit number; type and location of backcountry and wilderness use requested; method of travel; mode of transportation such as vehicle, aircraft, watercraft, snowmobile, and off-road vehicle information including make, model, and color, state of issuance and license plate number; parking and launch locations; aircraft Registration N-number and watercraft Hull Registration number; equipment information; itinerary details such as dates, use area or location, trailhead

and/or campground/trail name or code, number of campsites, trip length, and group size; payment information such as credit card number, credit card expiration date, and amount authorized. Other records also include information pertaining to general administrative processing and review of an application, and the monitoring of activities under the issued permit.

RECORD SOURCE CATEGORIES: Records in the system are obtained from applicants and permit holders of backcountry and wilderness permits.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

(1) DOI or any component of DOI;

(2) Any other Federal agency appearing before the Office of Hearings and Appeals;

(3) Any DOI employee or former employee acting in his or her official capacity;

(4) Any DOI employee or former employee acting in his or her individual capacity when DOI or DOJ has agreed to represent that employee or pay for private representation of the employee; or

(5) The United States Government or any agency thereof, when DOJ determines that DOI is likely to be affected by the proceeding.

B. To a congressional office when requesting information on behalf of, and at the

request of, the individual who is the subject of the record.

C. To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible with the reason for which the records are collected or maintained.

D. To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

E. To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

F. To Federal, state, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

G. To representatives of the National Archives and Records Administration (NARA) to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

H. To state, territorial and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

I. To an expert, consultant, grantee, shared service provider, or contractor

(including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

J. To appropriate agencies, entities, and persons when:

(1) DOI suspects or has confirmed that there has been a breach of the system of records;

(2) DOI has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOI (including its information systems, programs, and operations), the Federal Government, or national security; and

(3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DOI's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

K. To another Federal agency or Federal entity, when DOI determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(1) responding to a suspected or confirmed breach; or

(2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

L. To the Office of Management and Budget (OMB) during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

M. To the Department of the Treasury to recover debts owed to the United States.

N. 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.

O. To Federal, state, local, and tribal jurisdictions and agencies for the purpose of disclosing emergency contact information related to search and rescue efforts and coordinated law enforcement activities.

P. To Federal, state, local and tribal natural resource, recreation and land management jurisdictions, agencies, and organizations for the purpose of monitoring backcountry and wilderness visitor use activities, locations, and statistics, and disclosing information on permits granted in compliance with all applicable permitting requirements.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Paper records are stored in file folders stored within filing cabinets. Electronic records are maintained in computers, computer databases, email, and electronic media such as removable hard drives, magnetic disks, compact discs, and computer tapes.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records in this system are retrieved by various fields including the first name, last name, permit request number, permit number, email address, phone number, license plate number, use area and date, organization, and zip code.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records in this system are retained in accordance with the NPS Records Schedule Resource Management and Lands (Item 1), which has been approved by NARA (Job No. N1-79-08-1). The disposition for routine visitor use, resource management and land records are temporary and are destroyed or deleted 3 years after closure. Approved destruction methods for temporary records that have met their retention period include shredding or pulping paper records and erasing or degaussing electronic records in accordance with NARA guidelines and Departmental policy.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security and privacy rules and policies. During normal hours of operation, paper records are maintained in locked file cabinets under the control of authorized personnel. Computer servers on which electronic records are stored and located in secured DOI controlled facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI network and information assets. Access granted to authorized personnel is password-protected, and each person granted access to the system must be individually authorized to use the system. A Privacy Act Warning Notice appears on computer monitor screens when records containing information on individuals are first displayed. Data exchanged between the servers and the system is encrypted. Backup tapes are encrypted and stored in a locked and controlled room in a secure, off-site location.

Computerized records systems follow the National Institute of Standards and Technology privacy and security standards as developed to comply with the Privacy Act of 1974, as amended, 5 U.S.C. 552a; Paperwork Reduction Act of 1995, 44 U.S.C. 3501 et seq.; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 et seq.; and the Federal Information Processing Standards 199: Standards for Security Categorization of Federal Information and Information Systems. Security controls include user identification, passwords, database permissions, encryption, firewalls, audit logs, and network system security monitoring, and software controls.

Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their official duties, and each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and

records management training and sign the DOI Rules of Behavior. Privacy Impact Assessments were conducted to ensure that Privacy Act requirements are met and appropriate privacy controls were implemented to safeguard the personally identifiable information contained in the system.

RECORD ACCESS PROCEDURES: An individual requesting access to their records should send a written inquiry to the applicable System Manager identified above. DOI forms and instructions for submitting a Privacy Act request may be obtained from the DOI Privacy Act Requests website at <https://www.doi.gov/privacy/privacy-act-requests>. The request must include a general description of the records sought and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked "PRIVACY ACT REQUEST FOR ACCESS" on both the envelope and letter. A request for access must meet the requirements of 43 CFR 2.238.

CONTESTING RECORD PROCEDURES: An individual requesting amendment of their records should send a written request to the applicable System Manager as identified above. DOI instructions for submitting a request for amendment of records are available on the DOI Privacy Act Requests website at <https://www.doi.gov/privacy/privacy-act-requests>. The request must clearly identify the records for which amendment is being sought, the reasons for requesting the amendment, and the proposed amendment to the record. The request must include the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked "PRIVACY ACT REQUEST FOR

AMENDMENT” on both the envelope and letter. A request for amendment must meet the requirements of 43 CFR 2.246.

NOTIFICATION PROCEDURES: An individual requesting notification of the existence of records about them should send a written inquiry to the applicable System Manager as identified above. DOI instructions for submitting a request for notification are available on the DOI Privacy Act Requests website at <https://www.doi.gov/privacy/privacy-act-requests>. The request must include a general description of the records and the requester’s full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor’s identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked “PRIVACY ACT INQUIRY” on both the envelope and letter. A request for notification must meet the requirements of 43 CFR 2.235.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

Signed:

Teri Barnett,
Departmental Privacy Officer,
Department of the Interior.