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: Every Kid in a Park Initiative

Date: August 28, 2015

Bureau/Office: Office of the Chief Information Officer

Bureau/Office Contact Title: Departmental Privacy Officer

Point of Contact Email: Teri_Barnett@ios.doi.gov

First Name: Teri

M.I.:

Last Name: Barnett

Phone: (202) 208-1605

Address Line 1: 1849 C Street, NW

Address Line 2: Mail Stop 5547 MIB

City: Washington

State/Territory: District of Columbia

Zip: 20240

Section 1. General System Information

A. Is a full PIA required?

Yes

Yes, information is collected from or maintained on

Members of the general public

B. What is the purpose of the system?

The Every Kid in a Park initiative is an interagency effort between the Department of the Interior (DOI) National Park Service, Bureau of Land Management, U.S. Fish and Wildlife Service, Bureau of Reclamation, U.S. Forest Service, Department of Education, U.S. Army Corps of Engineers, and the National Oceanic and Atmospheric Administration to provide free entrance and standard amenity fees to U.S. students during their 4th grade year and following summer.

Beginning in September 2015, a 4th grader (including home schooled and free choice learners age 9-11 years old) can obtain his or her fee-free access by visiting the Every Kid in a Park website to participate in an educational activity and generate a paper voucher for use at federal public lands and waters. If desired, the paper voucher can be exchanged for an Interagency Annual 4th grade pass at a Federal recreation site location. These locations will only issue a pass with the exchange of a valid paper voucher and when the 4th grader (the pass owner) is present. Federal recreation site locations can be found at https://store.usgs.gov/pass/PassIssuanceList.pdf. The 4th grader can use either the paper voucher or the pass for fee-free entry. The voucher and pass will be valid from September 1st through August 31st.

Educators can also obtain fee-free access by visiting the Every Kid in a Park website and participating in educational activities. Educators include teachers, youth group leaders, religious group leaders, camp directors, afterschool programs, leaders of homeschoolers, etc. and any adult comfortable preparing, leading and completing the educational activity associated with accessing the vouchers. Educators can gain fee-free access for their students by visiting the Every Kid in a Park website and entering the “Educators” section, where they can download the personalized paper vouchers for each of their students. Each voucher contains a unique voucher number to ensure duplicates or photocopies are not used, but will not contain information that identifies the student. Educators will also find downloadable learning activities, aligned with standards that can be used to introduce 4th graders to topics surrounding federal lands and waters.

C. What is the legal authority?

Federal Lands Recreation Enhancement Act of 2004 (REA), 16 U.S.C. 6804

D. Why is this PIA being completed or modified?

Other

Describe

This privacy impact assessment analyzes the privacy implications for the official Every Kid in a Park website and the collection of information for the Every Kid in a Park initiative.

E. Is this information system registered in CSAM?

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	Describe
Fee Collector Web Page and Database	Provides a mechanism to allow fee collectors in the field to record the use of a voucher in exchange for a durable pass. The web page records the public lands site where the voucher was collected, and the voucher unique identifier.	No	

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)

DOI-06, America the Beautiful--The National Parks and Federal Recreational Lands Pass System, 72 FR 30817, June 4, 2007

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

No

Section 2. Summary of System Data

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

☒ Name
☐ Citizenship
☐ Gender
☐ Birth Date
☐ Group Affiliation
☐ Marital Status
☐ Biometrics
☐ Other Names Used
☐ Truncated SSN
☐ Legal Status
☐ Place of Birth
☒ Other
☐ Religious Preference
☐ Security Clearance
☐ Spouse Information
☐ Financial Information
☐ Medical Information
☐ Disability Information
☐ Credit Card Number
☐ Law Enforcement
☐ Education Information
☐ Emergency Contact
☐ Driver's License
☐ Race/Ethnicity
☐ Social Security Number (SSN)
☐ Personal Cell Telephone Number
☐ Tribal or Other ID Number
☒ Personal Email Address
☐ Mother's Maiden Name
☐ Home Telephone Number
☐ Child or Dependent Information
☒ Employment Information
☐ Military Status/Service
☐ Mailing/Home Address

Specify the PII collected.

Information about educators, individuals or special groups participating in Every Kid in a Park online program activities may include name, school or organization name, address, zip code, email address, and number of passes requested, which is collected for the purpose of establishing eligibility, eliminating duplication, preventing fraud and abuse, developing metrics, and analyzing success of the Every Kid in a Park initiative, and to increase participation in targeted localities. Information collected from 4th graders includes zip code, which is collected to inform the development of metrics and the success of the initiative, and increase participation in targeted areas. This information is not associated with the 4th grader and will not be used to identify individual students. Voucher numbers are system-generated and are linked to the zip code provided at the time the voucher was created, the date the voucher was created, the location the voucher was redeemed, and the date the voucher was redeemed. The voucher information is used to develop metrics to improve the success of the program.

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

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

☐ Paper Format
☐ Email
☐ Face-to-Face Contact
☒ Web Site
☐ Fax
☐ Other
☐ Telephone Interview
☐ Information Shared Between Systems

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

Information is collected from schools, educators, individuals, or organizations in order to establish eligibility and issue fee-free passes, develop metrics to analyze the success of outreach programs, encourage participation, and target localities. The information is needed in order to eliminate duplication, prevent fraud and abuse, and identify areas of success and challenges within the program. Locality information, such as zip codes, will be used in an aggregated form to identify where the initiative is being adopted, and will not identify specific individuals. Program managers will consider potential best practices where there is high performance. Where there are anomalies in the data collected from educators, such as the number of passes far exceeding the number of 4th graders in a school or locality, program managers will consider further investigation to prevent fraud or abuse.

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

☐ Within the Bureau/Office

☒ Other Bureaus/Offices

Describe the bureau or office and how the data will be used.

Program partners include the DOI Bureau of Land Management, Bureau of Reclamation, Fish and Wildlife Service, and National Park Service. Data in the system may be shared within DOI among program leads for program assessment and analysis. No personally identifiable information will be collected or shared about children. Locality information, such as zip codes, will be shared in an aggregated form to identify where the initiative is being adopted and where program managers should focus outreach activities. Program managers will consider potential best practices where there is high performance. Where there are anomalies in the data collected from educators, such as the number of passes far exceeding the number of 4th graders in a school or locality, program managers will consider further investigation to prevent fraud or abuse. Personally identifiable information of educators may be shared with appropriate organizations if fraud or abuse is suspected. In the case of suspected fraud, a school or educational institution may be contacted to verify the existence and / or eligibility of an identified educator.

☒ Other Federal Agencies

Describe the federal agency and how the data will be used.

Federal agency partners include the U.S. Army Corps of Engineers, Department of Education, U.S. Forest Service, National Oceanic and Atmospheric Administration, and the General Services Administration. Statistical or aggregate data may be shared among the interagency partner leads for program assessment and analysis to identify the success of the initiative and areas where further outreach is necessary. No personally identifiable information for children will be collected or shared. Zip codes where vouchers are generated may be shared among agency leads in an aggregated form to identify where the initiative is being adopted. Program managers will consider potential best practices where there is high performance. Where there are anomalies in the data collected from educators, such as the number of passes far exceeding the number of 4th graders in a school or locality, program managers will consider further investigation to prevent fraud or abuse. Personally identifiable information of educators may be shared if fraud or abuse is suspected. In the case of suspected fraud, a school or educational institution may be contacted to verify the existence and/or eligibility of an identified educator.

The Every Kid in a Park website is hosted by the General Services Administration (GSA) under an interagency agreement with DOI. GSA hosts and manages the website and database, implements and monitors appropriate security controls to protect information against unauthorized access, use or disclosure, provides reports for metrics and program management, and supports the online functions of the Every Kid in a Park initiative.

☐ Tribal, State or Local Agencies

☐ Contractor

☐ Other Third Party Sources

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.

A Privacy Act Statement is posted on the Every Kid in a Park website to inform individuals about the purpose of the information requested, how it is used, what organizations it might be shared with, and any effects on the individual for not providing the requested information. Individuals may decline to provide information by not participating in the Every Kid in a Park program to obtain fee-free access vouchers. Students and other individuals may choose to interact on the website without providing personal information, and educators can find downloadable learning activities, aligned with standards that can be used to introduce 4th graders to topics surrounding federal lands and waters. The website contains a link to the DOI Privacy Policy and the Children's Privacy Policy, which provides notice to the public on how information is handled at DOI: http://www.doi.gov/privacy.cfm.

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

☒ Privacy Act Statement ☒ Privacy Notice ☐ Other ☐ None

Describe each applicable format.

Privacy Act Statement for Educators:
On this site, we ask you to give us some basic information. You're not required to provide it to us, but it's necessary to get a pass. We collect this information to give free passes to fourth graders and educators. We use it to make sure you're eligible for a free pass and to promote Every Kid in a Park. These passes allow free access to public lands and waters.

We may share the information with other agency groups or organizations. This helps us measure and improve the program. It also helps us stop fraud and abuse.

We do all this under the authority of the Federal Lands Recreation Enhancement Act of 2004 (REA), 16 U.S.C. 6804.

The Every Kid in a Park initiative and the passes issued are covered under the DOI system of records notice for national park and recreational lands, DOI-06, America the Beautiful--The National Parks and Federal Recreational Lands Pass System, last published in the Federal Register on June 4, 2007 at 72 FR 30817. The DOI-06 system notice and this privacy impact assessment provides information to the public on what information is collected and where it is maintained, how the information is used and safeguarded, who it is shared with, and how individuals can obtain access to their records. The DOI-06 notice is being updated and an amended notice will be published in the Federal Register.

The following notice is posted on the page where 4th graders interact with DOI:
We don't collect any information that could personally identify you. We do ask you to tell us the general area where you live. Knowing this helps us analyze who is using the program. It also helps us make your paper pass and protect against misuse.

We collect general information about our visitors so we can improve our website. If you want more information, see the Department of Interior Privacy Policy. See also the Children's Privacy Policy.

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

Data is retrieved by voucher number, date the voucher was created, date voucher is redeemed, location of voucher redeemed, or zip code where the voucher was created. The unique voucher number will be the identifier for printable paper vouchers. Data can be retrieved manually, but for evaluation purposes automatic reports will be developed such as the Duplicate Voucher Number Report. This report will allow the user to report when a voucher number is entered into the database more than one time. With regard to eligibility verification or suspected fraud or abuse, information may be retrieved by name of educator, individual, or organization requesting the fee-free pass.

I. Will reports be produced on individuals?

Yes

What will be the use of these reports? Who will have access to them?

Educator-based reports can be developed on-demand to better understand redemption strategies, detect fraud or abuse, and examine utilization amongst schools. No reports with personally identifiable information on children will be produced.

Section 3. Attributes of System Data

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

The sources of information are the educators, individuals and organizations participating in the Every Kid in a Park initiative. In most cases, educator information and will not be verified for accuracy. In cases of suspected fraud or abuse, a school or educational institution may be contacted to verify the eligibility of an educator requesting fee-free passes through the Every Kid in a Park website.

B. How will data be checked for completeness?

The sources of information are the educators, individuals and organizations participating in the Every Kid in a Park initiative, and it is expected that the name and contact information provided by the individual is complete at the time of submission. Data is not otherwise checked for completeness except in cases where fraud or abuse are suspected, then program officials may verify the accuracy or completeness of information with appropriate organizations.

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

The sources of information are the educators, individuals and organizations participating in the Every Kid in a Park initiative, and it is expected that the information provided by the individual is current at the time of submission. Data is not otherwise checked for currency.

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 maintained under the National Park Service Records Schedule Interpretation and Education (Item 6), Retention plan C - Routine and Supporting Documentation(N1-079-08-5), and Departmental Records Schedule 1 - Administrative Records (DAA-0048-2013-0001), which have been approved by the National Archives and Records

Administration. The interpretation and education records have a temporary disposition and will be retained 3 years from the end of the fiscal year in which the transaction was completed. The records maintained under the Departmental Records Schedule include general administrative records, including routine correspondence, administrative copy files, budget files, and duplicate copies, which have different disposition based on the subject matter, function, and the needs of the agency. Temporary records are cut off when superseded or obsolete, and destroyed after the required retention period for the specific record type. In some cases, records may be maintained under DOI bureau and office records retention schedules and disposed of in accordance with the applicable retention schedule.

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

Approved disposition methods for temporary records include shredding or pulping paper records, and erasing or degaussing electronic records in accordance with 384 Departmental Manual 1 and NARA guidelines.

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 minimal risk to the privacy of individuals associated with use of the Every Kid in a Park website to obtain fee-free passes. The risk is mitigated by the security and privacy controls implemented to safeguard privacy and the limited collection of personally identifiable information from individuals. The purpose of the initiative is to provide free entrance and standard amenity fees to U.S. students during their fourth grade year and following summer. The website does not collect names or other personally identifiable information that uniquely identifies these 4th grade students. In order to obtain a fee-free access or pass, the student must acknowledge they are a 4th grader, provide a zip code, and participate in an educational activity to generate a paper voucher for use at federal public lands and waters. If desired, the paper voucher can be exchanged for an Interagency Annual 4th grade pass at a Federal recreation site location; however, the identity of the student is not collected or verified during this exchange and the student can use either the paper voucher or the pass for fee-free entry. Vouchers contain a unique voucher number to ensure duplicates or photocopies are not used, but will not contain information that identifies the student.

Educators or other individuals who participate on the website to obtain fee-free access include teachers, youth group leaders, religious group leaders, camp directors, afterschool programs, leaders of homeschoolers, and any adult comfortable preparing, leading and completing the educational activity associated with accessing the vouchers. These individuals are required to provide a minimum amount of personally identifiable information, such as name, school or organization name, address, email address, and number of passes requested, in order to establish eligibility and obtain the fee-free access or personalized paper vouchers for their students. In some cases, individual participants may provide personal contact information or home address instead of school address. This may pose a risk to the privacy of the individual, which is mitigated by the strict controls in place to prevent unauthorized access, use or disclosure of this information.

Access to data collected, stored and utilized is limited to system developers and administrators, and authorized program officials. Data shared outside of the system will be limited to derived summary reports that do not contain personally identifiable information. Aggregated locality information is shared with interagency partners in order to facilitate program management and identify areas of participation, develop metrics, and analyze success of this initiative. Where there are anomalies in the data collected from educators, such as the number of passes far exceeding the number of 4th graders in a school or locality, program managers will consider further investigation into fraud or abuse, and may contact a school or organization to verify eligibility.

The website is hosted by the GSA under an interagency agreement with DOI. GSA manages the website and database, implements and monitors security controls, provides reports for metrics, and supports the online functions of the Every Kid in a Park initiative. Data is housed in a public cloud for Federal Government customers, the Amazon US East/West Public Cloud through Amazon Web Services, and is designed to meet a wide range of regulatory requirements, including government compliance and security requirements. Amazon Web Services - East/West US Public Cloud is FedRAMP compliant. FedRAMP requires cloud service providers and contractors to implement the controls within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system as defined in Federal Information Processing Standards (FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. The FedRAMP baseline controls are based on National Institute of Standards and Technology Special Publication 800-53, and this system meets the FedRAMP FISMA Moderate Impact baseline - see https://www.fedramp.gov/marketplace/compliant-systems/amazon-web-services-aws-eastwest-us-public-cloud/.

The physical, administrative and technical controls and appropriate safeguards implemented to mitigate privacy risks are outlined below in section 4. Records are destroyed in accordance with approved methods as outlined in DOI policy and the applicable records schedule. Data retention and destruction requirements are described above in section 3.D., and in the applicable records management schedules.

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

The data collected is necessary to carry out the purpose of the Every Kid in a Park initiative, to provide annual passes to 4th graders while limiting duplication, fraud and abuse. Collecting locality information is necessary in order to provide a basic level of program management and to identify areas of participation and areas that need additional outreach. Information on educators is relevant and necessary to establish eligibility, develop metrics, and analyze success of this initiative. Where there are anomalies in the data collected from educators, such as the number of passes far exceeding the number of 4th graders in a school or locality, program managers will consider further investigation to prevent duplication, fraud or abuse.

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

No

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

No

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

No

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

The website does not create new data about an individual therefore new data is not verified for relevance or accuracy.

F. Are the data or the processes being consolidated?

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 ☒ Developers ☒ System Administrator

☒ Contractors ☒ Other

Describe

Access to data is limited to Developers, System Administrators and other program officials on an official need to know basis. Access is restricted to the greatest extent possible and is based on the least privilege security principle, such that the least amount of access is given to a user to complete the required business activity. All access is controlled by authentication methods to validate the authorized user. Program managers only receive derived electronic reports when necessary via email. Only the System Administrator or select Developers who are involved in the generating of derived reports has access to the electronic collection. As a cloud-hosted application, all access to the system is remote, and a number of security controls have been implemented to secure the transmission and storage of data, including the controls listed in section N below.

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

Access to data is limited to Developers, System Administrators and other authorized individuals on an official need to know basis. Access is restricted to the greatest extent possible and is based on the least privilege security principle, such that the least amount of access is given to a user to complete the required business activity. All access is controlled by authentication methods to validate the authorized user. Program managers only receive derived electronic reports. Only the system administrator or select developers who are involved in the generating of derived reports has access to the electronic collection.

The data is housed in a public cloud for Federal Government customers, the Amazon US East/West Public Cloud through Amazon Web Services. It is designed to meet a wide range of regulatory requirements, including government compliance and security requirements. Amazon Web Services – AWS East/West US Public Cloud is FedRAMP compliant. FedRAMP requires cloud service providers and contractors to implement the controls within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. The FedRAMP baseline controls are based on National Institute of Standards and Technology Special Publication 800-53. This system meets the meet the FedRAMP FISMA Moderate Impact baseline - see https://www.fedramp.gov/marketplace/compliant-systems/amazon-web-services-aws-eastwest-us-public-cloud/.

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?

As part of the FedRAMP compliance process, the contractor is responsible for properly protecting all information used, gathered, or developed as a result of work under the contract. The contractor protects all Government data, equipment, etc. by treating the information as sensitive. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

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

No

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

No

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

The Every Kid in a Park website does not monitor individuals. The website is used to provide annual passes to 4th graders to access federal public lands and waters.

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

The Every Kid in a Park website does not monitor individuals. The website is used to provide annual passes to 4th graders to access federal public lands and waters.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Cards
☐ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Other
☐ Combination Locks
☒ Locked Offices

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Other
☒ Intrusion Detection System (IDS)
☐ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card

Describe

Two-factor authentication, Transport Layer Security (TLS) standard, penetration testing, vulnerability scanning

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☐ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☐ Other
☒ 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

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 Every Kid in a Park Program Manager is responsible for protecting the privacy of individuals for this website and for addressing Privacy Act requests or complaints in consultation with the DOI Privacy Officer. Procedures for submitting Privacy Act requests or complaints are outlined in DOI Privacy Act Regulations at 43 CFR Part 2, Subpart K, and in the DOI-06 system of records notice.

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 Every Kid in a Park Program Manager, System Owner, and Information System Security Officer are responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information. This responsibility is described in the Federal Information Security Modernization Act of 2014, Office of Management and Budget policy, as well as DOI security and privacy policies, mandatory IT security and privacy training, and DOI Rules of Behavior. The Every Kid in a Park Program Manager is responsible for ensuring the Privacy Act records are maintained in accordance with the provisions of the Privacy Act and the published DOI-06 system of records notice, and reporting any suspected or confirmed compromise of privacy information.